Sumário

TERMO DE REFERÊNCIA

1. DESCRIÇÃO OBJETO

1.1. Contratação de empresa especializada para prestação de serviço de redes *Multi Protocol Label Switching* (MPLS) e circuitos de acesso à Internet com LINK DEDICADO, SDWAN, gerenciamento proativo contra falhas e incidentes de segurança cibernética com a utilização de solução de *Next Generation Firewall* - NGFW nas atividades operacionais, atuando como camada protetiva para o tráfego de dados e informações críticas, nas condições e quantitativos propostos, nas localidades de interesse da Procuradoria Geral do Estado do Rio de Janeiro (PGE/RJ). O atendimento desses serviços deverá ser realizado em conformidade com as condições e especificações constantes no presente Termo de Referência.

2. DA JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO

2.1. Os serviços eletrônicos da PGE/RJ utilizam atualmente a Internet e a Rede de Dados (WAN) que conecta o ambiente computacional do Edifício-Sede às Secretarias de Estado, Procuradorias Regionais, à Especializada de Brasília/DF e ao TJ-RJ. Esta rede possui seus circuitos de comunicação de dados MPLS e de acesso à internet, com período próximo para expirar, sem possibilidade de renovação. Além disso, há a expectativa de aumento da demanda por novos serviços, como VOIP, o que acarretará maior necessidade de recursos de conectividade.

2.2. Esta rede de dados (WAN) é parte integrante da rede CONNECTA RJ (REDE GOV), que permite acessar diversos sistemas eletrônicos estaduais e, principalmente, o Sistema da Dívida Ativa, hospedado no PRODERJ – Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro.

2.3. A não conclusão, em tempo hábil, do procedimento licitatório da nova Rede de Dados (WAN) do Governo do Estado do Rio de Janeiro, por parte do PRODERJ, pode resultar na indisponibilidade de serviços, uma vez que não haverá cobertura contratual para garantir a continuidade de serviços essenciais desta instituição.

2.4. O serviço de acesso à internet é indispensável para o desempenho das atribuições da PGE-RJ, sendo que sua interrupção pode comprometer a continuidade das atividades institucionais. Além disso, a evolução tecnológica e o crescimento da

demanda por serviços online reforçam a necessidade de uma infraestrutura de conectividade robusta e contínua.

2.5. Sendo assim, os serviços ora pretendidos configuram-se como uma solução de TI composta por múltiplos itens, organizados em dois lotes distintos. A combinação de SD-WAN, MPLS, Link Dedicado e Proteção Integrada visa manter e aprimorar o atendimento aos requisitos de qualidade, segurança e tecnologia na infraestrutura de TI da PGE-RJ.

2.6. A nova infraestrutura de rede a ser contratada tem como objetivo a aquisição de links de internet com velocidade adequada para atender à demanda atual, bem como possibilitar a expansão futura do tráfego da Sede e das unidades remotas. Além disso, deverá suprir as necessidades institucionais da organização, mantendo um elevado padrão de qualidade na comunicação e no acesso a novas tecnologias, de modo a sustentar a infraestrutura tecnológica existente. A solução também deverá ser capaz de atender, de forma estratégica, às novas demandas de serviços e aplicações, como o PGE Digital, Portal PGE, videoconferências, VoIP, entre outros. Por fim, a arquitetura da rede deverá assegurar o nível de segurança necessário, visto que esses serviços requerem uma infraestrutura de alta disponibilidade e desempenho, resultando em maior eficiência e proteção para a administração.

2.7. **Da Fundamentação Legal:**

2.7.1. É importante ressaltar que essa modalidade de contratação encontra respaldo na Lei nº 14.133/2021, especificamente em seu artigo 6º, XLI, por se enquadrar nos casos de licitação, na modalidade Pregão, sob a forma ELETRÔNICA, no âmbito da administração pública. Além disso, a contratação se justifica pela necessidade de garantir a atualização contínua em áreas estratégicas essenciais para o desempenho e desenvolvimento da instituição.

2.7.2. O presente Termo de Referência contém um "conjunto de elementos necessários e suficientes, com nível de precisão adequado, para caracterizar o serviço ou complexo de serviços objeto da licitação (...)", assegurando que, nos procedimentos licitatórios, a demanda da Administração seja claramente apresentada. Dessa forma, o potencial contratado poderá estruturar sua proposta de maneira adequada, demonstrando sua capacidade de atender integralmente aos requisitos previamente estabelecidos.

2.7.3. Adicionalmente, o objeto da contratação possui padrões de desempenho e qualidade que podem ser objetivamente definidos no edital, por meio de especificações usuais de mercado. Isso garante maior transparência, previsibilidade e equidade no

processo licitatório, permitindo que a Administração selecione a proposta mais vantajosa com base em critérios técnicos e objetivos.

2.7.4. Ademais, o presente TR é decorrente do Estudo Técnico Preliminar que se baseou na Instrução Normativa SGD/ME nº 94/2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal. juntamente com o Decreto Estadual nº 48.816/2023.

3. DO DETALHAMENTO DO OBJETO

O objeto a ser contratado abrangerá os serviços de:

3.1 Elaboração de Plano de Projeto (Modelo Anexo) de fornecimento e implantação dos serviços descritos no objeto e gerenciá-lo até o aceite final da CONTRATANTE.

3.2 Tendo em vista o incentivo à competitividade, optou-se por separá-los em dois lotes, adicionando a cada um seus respectivos itens agregados e opcionais, de forma a garantir que as soluções constituintes de cada lote sejam implementadas com eficiência, alinhadas aos requisitos técnicos e promovendo a interoperabilidade necessária entre os sistemas.

3.3 Fornecimento, implantação, manutenção e operação da infraestrutura de comunicação de dados de alto desempenho fim a fim com serviço Anti-DDOS (DoS – *Denial of Service*), alta qualidade, baixa latência em circuitos de dados 100% em fibra óptica, síncrona, e serviços acessórios, visando o transporte de dados, vídeo e imagem sobre TCP/IP – Rede *Multi Protocol Label Switching* (MPLS) com QoS e capaz de transportar de forma coordenada e não competitiva os mais variados tipos de tráfego, inclusive voz sobre IP (VoIP). Este serviço deve ser instalado diretamente no datacenter localizado no edifício Sede da PGE e nos centros de redes das unidades administrativas remotas, localizadas no território fluminense e em Brasília/DF, discriminados na Tabela 1 - Tabela de Endereços das Localidades.

3.4 Fornecimento, implantação, manutenção e operação da tecnologia SD-WAN (*Software-Defined WAN*) centralizada, gerenciando a rede em uma console única, proporcionando as vantagens, tais como: configuração de recursos de qualidade de serviço QoS inteligente para priorizar tráfego sensível (VoIP, videoconferência,

backup, entre outros), DPI (*Deep Packet Inspection*) nativamente incorporada, permitindo a identificação, classificação e controle do tráfego de rede com base em aplicações, protocolos e conteúdos, para identificar e bloquear tráfego não autorizado ou malicioso sem necessidade de passar pelo NGFW.

3.5 Flexibilidade na definição de topologia lógica, simplificação de roteamento, menor custo, implantação de parâmetros de segurança da informação, mantendo a disponibilidade (contingência da Rede MPLS) e desempenho da Rede PGE-RJ, através de túneis IPSec entre os equipamentos SD-WAN das localidades remotas e o edifício-Sede.

3.6 Fornecimento de Serviço de Segurança Gerenciada, monitoração proativa do(s) dispositivo(s) de segurança ofertados pela CONTRATADA. A solução de segurança deverá estar em conformidade com as boas práticas recomendadas pelas normas NIST e ISO 27001 e seu fabricante avaliado pelo Gartner Group, mencionado em seu quadrante mágico dentro nos últimos 2 anos.

3.7 Todos os equipamentos devem, ser dimensionados para suportar os requisitos mínimos informados nesta especificação técnica;

3.8 Os equipamentos fornecidos deverão ser novos (sem uso), estar em perfeito estado de conservação e de funcionamento.

3.9 Compatibilidade nativa a IPv6 em todos os links e dispositivos (roteadores, firewalls, SD-WAN).

3.10 Nenhum dos equipamentos fornecidos podem estar em modo *End of Life, End of Sale e End of Support* no dia da entrega do equipamento, após assinatura do contrato;

3.11 Os switches de cada localidade será de responsabilidade da PGERJ;

3.12 Todos os equipamentos, a serem disponibilizados em cada lote, que apresentarem alta utilização de recursos, deverão ser substituídos por outros de maior capacidade. Sem custos para a CONTRATANTE.

3.12.1 Por alta utilização de recursos entende-se qualquer uma das situações descritas abaixo:

a. Quando o equipamento permanecer com a utilização da CPU (ou média da utilização das CPUs) acima de 60% (setenta por cento) por mais de 8 (oito) horas, contínuas ou não, em um mês específico;

b. Quando o equipamento permanecer com a utilização da memória

RAM acima de 60% (setenta por cento) por mais de 16 (dezesseis) horas, contínuas ou não, em um mês específico.

c. Quando o disco local de cada equipamentos atingir 80% ou mais de utilização podendo causar prejuízo no esgotamento de recursos.

3.12.2 O prazo para substituir os equipamentos será de 60 (sessenta) dias, a partir do fechamento do mês específico em que houve a constatação de alta utilização dos recursos do equipamento, sem prejuízos das eventuais glosas e multas decorrentes dos esgotamentos dos recursos computacionais.

A. Nem o perfil de tráfego da PGE e nem a utilização de recursos que não fazem parte da especificação poderá ser utilizada como argumento para a alta utilização dos recursos e não será permitido que recursos técnicos sejam desabilitados para reduzir o consumo computacional dos dispositivos.

3.13 A LICITANTE não poderá participar do certame concorrendo simultaneamente aos Lotes 1 e 2, tampouco ser adjudicatária de ambos, vedada a concentração do objeto em um único fornecedor.

A limitação da participação e adjudicação se justifica por razões técnicas e operacionais, visando:

I – mitigar riscos de indisponibilidade sistêmica decorrentes da concentração da prestação dos serviços em um único fornecedor;
II – garantir a redundância lógica e física entre os links contratados, com utilização de caminhos distintos, não compartilhados;
III – assegurar que a infraestrutura, inclusive na última milha, não possua pontos de falha em comum entre os lotes;
IV – preservar a continuidade e a alta disponibilidade dos serviços essenciais de comunicação de dados da PGE-RJ em todos os pontos de atendimento;
V – evitar dependência tecnológica e operacional de único provedor (vendor lock-in).

A medida visa, ainda, ampliar a resiliência da rede corporativa, garantindo a adequada estratégia de contingência e alta disponibilidade dos serviços críticos.

3.14 Última milha caracteriza-se como o meio de comunicação utilizado para interligar cada unidade da CONTRATANTE ao *Backbone* da CONTRATADA.

3.15 Por ponto de falha comum, entende-se:

3.15.1 Utilização compartilhada dos mesmos equipamentos no ambiente da

CONTRATADA ou em ambientes públicos: roteadores, multiplexadores, *switches*, conversores ópticos e outros. Será permitido o compartilhamento de equipamentos somente dentro das instalações da PGE-RJ.

3.15.2 Utilização compartilhada no ambiente da CONTRATADA entende-se que: no ambiente público, como: utilização dos mesmos dutos, caixas de passagem, DIOs da caixa de passagem (na calçada do prédio da CONTRATANTE) e dos dutos da caixa de passagem até o rack dentro das instalações da CONTRATANTE **apenas.**

3.15.3 Deverão ser utilizados links de comunicação terrestre confeccionados com fibra óptica. Apenas será permitida a conversão do meio óptico para UTP para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou *appliances* SD-WAN.

3.15.4 Considerando os requisitos de qualidade, rendimento, compatibilidade, durabilidade e segurança que envolvem a prestação dos descritos neste objeto, todas as exigências técnicas foram definidas com base em critérios estritamente necessários à continuidade das operações da PGE-RJ, à estabilidade da rede e à proteção do ambiente institucional. Tais critérios visam garantir o atendimento aos mais elevados padrões de desempenho e estejam em conformidade com as normas técnicas vigentes, evitando soluções inadequadas ou obsoletas que possam comprometer a eficiência, a interoperabilidade entre sistemas, a sustentabilidade do investimento público e a segurança da informação.

4. DO QUANTITATIVO DOS SERVIÇOS

4.1 A contratação deverá ser realizada em lotes.

4.2 O **LOTE 1** constitui a rede principal da Sede e das Unidades Remotas da PGE, localizadas no território fluminense, conforme discriminado na Tabela 3 — Tabela de Endereços das Localidades.

4.2.1 As soluções de SD-WAN e MSS devem atender às boas práticas recomendadas pelo NIST e ISO 27001;

4.2.2 A solução de segurança deverá contemplar o serviço de Gerenciamento de Segurança (MSS), interligado a um SNOC *(Security and Network Operation Center*), o qual deverá dispor das ferramentas de hardware e software necessárias para o adequado monitoramento, detecção e tratamento de incidentes de forma remota;

4.2.3 Serviço de MSS monitoramento, detecção e tratamento dos incidentes e segurança e solução de NGFW *Firewall* a ser entregue pelo serviço de MSS com alta

disponibilidade;

4.2.4 Solução de SD-WAN em alta disponibilidade ativo/ativo;

4.2.5 Proteção Anti-DDOS

4.2.6 1 (um) *link* IP DEDICADO de acesso à internet com 12 IPS fixo;

4.2.7 1 *link* Concentrador MPLS;

4.2.8 16 (dezesseis) *links* MPLS.

4.3 O **LOTE 2** contempla o acesso, formando a rede redundante que deverá interligar a rede local do Edifício-Sede da PGE/RJ às Unidades Remotas, localizadas no território fluminense, em Brasília/DF e ao TJ-RJ, conforme discriminado na Tabela 1 — Tabela de Endereços das Localidades, garantindo o acesso aos sistemas corporativos do Estado e da própria PGE-RJ.

4.3.1 Proteção Anti-DDOS

4.3.2 1 (um) link IP DEDICADO de acesso à internet na Sede com 12 IPS fixo;

4.3.3 1 (um) link Concentrador MPLS

4.3.4 15 (quinze) links MPLS das Unidades Remotas

4.3.5 1 (um) link MPLS interligação com o TJ-RJ

Tabela 2 LOTE 1 – Tabela lotes, localidades, serviço e velocidades

LOTE 1- <u>Nucleo Central</u> – SEDE PGE/RJ - Rua do Carmo, 27 - Centro - Rio de Janeiro, RJ			
Item	**SERVIÇO**	**Métrica Quantidade/Velocidade**	
01	LINK IP Dedicado (Acesso Dedicado à internet com fornecimento de 12 endereços IP validos (1- rede; 1 broadcasting e 10 hosts)	**1 Gbps**	
02	Serviço SDWAN(NGFW + Licenciamento) SEDE em Alta Disponibilidade HA	**UN 02**	
03	LINK MPLS SDWAN Concentrador Rede Principal_ interligação com a Rede Externa em Alta Disponibilidade HA	**UN 1**	**2 Gbps**
04	Serviço Gerenciado de Segurança MSS (Managed Security Services)	**UN 01**	
05	Serviço de Projeto da implantação completa da solução	**UN**	**01**
06	Console de gerenciamento. logs e relatórios centralizado para SDWAN Concentradora Principal e o NGFW FIREWALL 1 com garantia de 60 meses	**UN**	**01**
07	Serviço de treinamento *hands-on* operacional para a solução do lote 1	**Aluno**	**03**

Item	LOTE 1 - Rede Externa principal localidades serviço velocidade		Quantidade
08	**PR01 – NITERÓI** Rua Visconde de Sepetiba, 935 / 7° andar - Centro - Niterói, RJ	LINK MPLS 100 Mbps	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01
09	**PR02 - DUQUE DE CAXIAS** Avenida Brigadeiro Lima e Silva, 1939 / 6° e 7° andares - Vinte de Agosto - Duque de Caxias, RJ	LINK MPLS 100 Mbps	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01
10	**PR03 - NOVA IGUAÇU** Rua Comendador Soares, 194 / 2º andar - Ed. São Paulo Business Center - Centro - Nova Iguaçu, RJ	LINK MPLS 100 Mbps	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01
11	**PR04 - BARRA DO PIRAÍ** Rua Dona Guilhermina, 100 - Chácara Farani - Barra do Piraí, RJ	LINK MPLS 100 Mbps	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01
12	**PR05 - VOLTA REDONDA** Avenida Paulo de Frontin, 590 / Salas 1001 a 1013 - 10º andar - Aterrado - Volta Redonda, RJ	LINK MPLS 100 Mbps	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01
13	**PR06 - ANGRA DOS REIS** Rua do Comércio, 10 - Sobreloja - Centro - Angra dos Reis, RJ	LINK MPLS 100 Mbps	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01
14	**PR07 – PETRÓPOLIS** Rua do Imperador, 288 / Salas 30 a 35 - Shopping Dom Pedro II - Centro - Petrópolis, RJ	LINK MPLS 100 Mbps	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01
15	**PR08 - NOVA FRIBURGO** Rua Dante Laginestra, 49 - Centro - Nova Friburgo, RJ	LINK MPLS 100 Mbps	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01

16	**PR09 – MACAÉ** Avenida Nossa Senhora da Glória, 999 / 1º andar - Cavaleiros - Macaé, RJ	LINK MPLS 100 Mbps	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01
17	**PR10 – CAMPOS** Rua Gastão Machado, 66 - Parque Tomás Coelho - Campos dos Goytacazes, RJ	LINK MPLS 100 Mbps	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01
18	**PA- ITAPERUNA** Avenida Zulamith Bittencourt, 300 / Sala 104 - 4º andar - Ed. Residencial Ajala - Centro - Itaperuna, RJ	LINK MPLS 100 Mbps	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01
19	**PR12 - CABO FRIO** Local temporario:Rua Raul Veiga, 153,sala 102 - Centro Local Principal: Rua Domingos Ribeiro, 62 – Passagem Cabo Frio, RJ	LINK MPLS 100 Mbps	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01
20	**PA - SÃO GONÇALO** Rua Coronel Serra, 1000 / 7º andar - Zé Garoto - São Gonçalo, RJ	LINK MPLS 100 Mbps	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01
21	**PG-13 - BRASÍLIA** SAF/S, Quadra 02, Lote 04, Sala 304 - Cond. Via Esplanada - Brasília, DF	**LINK MPLS 300 Mbps**	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01
22	**CONVENTO** DO CARMO Praça XV de Novembro, 101 (Antigo Convento do Carmo), Centro, Rio de Janeiro/RJ – CEP: 20010-010	**LINK MPLS 300 Mbps**	UN 01
		APPLIANCE NGFW FIREWALL SDWAN, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN 01

Item	LOTE 2 - Rede Redundante – LINK DEDICADO - MPLS		Métrica Quantidade/Velocidade	
01	Link IP Dedicado (Acesso Dedicado à internet com fornecimento de 12 endereços IP validos (1- rede; 1 broadcasting e 10 hosts) Acesso a Internet Rede Redundante (SEDE)		**1 Gbps**	
02	Concentradora Rede Redundante MPLS com a Rede Externa	SEDE PGE/RJ - Rua do Carmo, 27 - Centro - Rio de Janeiro, RJ	**UN 01**	**1 Gbps**
03	Serviço de Projeto da implantação completa da solução		**UN 01**	**01**
04	**PR01 – NITERÓI**	Rua Visconde de Sepetiba, 935 / 7° andar - Centro - Niterói, RJ	**UN 01**	**100 Mbps**
05	**PR02 - DUQUE DE CAXIAS**	Avenida Brigadeiro Lima e Silva, 1939 / 6° e 7° andares - Vinte de Agosto - Duque de Caxias, RJ	**UN 01**	**100 Mbps**
06	**PR03 - NOVA IGUAÇU**	Rua Comendador Soares, 194 / 2º andar - Ed. São Paulo Business Center - Centro - Nova Iguaçu, RJ	**UN 01**	**100 Mbps**
07	**PR04 - BARRA DO PIRAÍ**	Rua Dona Guilhermina, 100 - Chácara Farani - Barra do Piraí, RJ	**UN 01**	**100 Mbps**
08	**PR05 - VOLTA REDONDA**	Avenida Paulo de Frontin, 590 / Salas 1001 a 1013 - 10º andar - Aterrado - Volta Redonda, RJ	**UN 01**	**100 Mbps**
09	**PR06 - ANGRA DOS REIS**	Rua do Comércio, 10 - Sobreloja - Centro - Angra dos Reis, RJ	**UN 01**	**100 Mbps**
10	**PR07 - PETRÓPOLIS**	Rua do Imperador, 288 / Salas 30 a 35 - Shopping Dom Pedro II - Centro - Petrópolis, RJ	**UN 01**	**100 Mbps**
11	**PR08 - NOVA FRIBURGO**	Rua Dante Laginestra, 49 - Centro - Nova Friburgo, RJ	**UN 01**	**100 Mbps**
12	**PR09 – MACAÉ**	Avenida Nossa Senhora da Glória, 999 / 1º andar - Cavaleiros - Macaé, RJ	**UN 01**	**100 Mbps**
13	**PR10 – CAMPOS**	Rua Gastão Machado, 66 - Parque Tomás Coelho - Campos dos Goytacazes, RJ	**UN 01**	**100 Mbps**
14	**PA- ITAPERUNA**	Avenida Zulamith Bittencourt, 300 / Sala 104 - 4º andar - Ed. Residencial Ajala - Centro - Itaperuna, RJ	**UN 01**	**100 Mbps**
15	**PR12 - CABO FRIO**	Local ATUAL *temporário*: Rua Raul Veiga, 153,sala 102 - Centro Local Principal:*em obras* Rua Domingos Ribeiro, 62 – Passagem - Cabo Frio, RJ	**UN 01**	**100 Mbps**
16	**PA - SÃO GONÇALO**	Rua Coronel Serra, 1000 / 7º andar - Zé Garoto - São Gonçalo, RJ	**UN 01**	**100 Mbps**
17	**PG-13 - BRASÍLIA**	SAF/S, Quadra 02, Lote 04, Sala 304 - Cond. Via Esplanada - Brasília, DF	**UN 01**	**100 Mbps**

18	**CONVENTO DO CARMO**	Praça XV de Novembro, 101 (Antigo Convento do Carmo), Centro, Rio de Janeiro/RJ – CEP: 20010-010	**UN 01**	**100 Mbps**
19	**TJ-RJ**	Endereço: Av. Erasmo Braga, n° 115 Centro, Rio de Janeiro/RJ – CEP 20020-903	**UN 01**	**20 Mbps**

Tabela 3 LOTE 2 – Tabela lotes, localidades, serviço

4.4 A Rede Externa é formada por pontos de acesso das unidades remotas, que interligará ao Núcleo Central supramencionado através de **duas abordagens**, sendo a **principal através da rede MPLS LOTE 1 com SDWAN** e a da **redundante através da rede MPLS LOTE 2**.

4.4.1.1 Unidades remotas:

4.4.1.1.1 Procuradorias Regionais;

4.4.1.1.2 Convento;

4.4.1.1.3 Procuradoria Especializada de Brasília/DF.

4.4.1.1.4 TJ-RJ

4.4.2 **Redes MPLS para interligar as unidades remotas:**

4.4.2.1 Os pontos de acesso remoto de ambas redes MPLS terão velocidades mínimas de 100 Mbps dedicados e devem suportar o protocolo IP, que serão interligados ao Núcleo Central através de IPSEC com QoS as concentradoras MPLS, proteção e diferenciação dos tipos de tráfegos, dando prioridades às aplicações mais sensíveis (rede escalonável), com baixa oscilação, conexão simétrica sem IP Fixo, para acessar aplicações e serviços de rede do datacenter da PGE/RJ;

4.4.2.2 A operação de ambas as redes funcionará no regime **ativo/ativo**, 24x7;

4.4.2.3 Ambas as redes devem ter baixo tempo de latência, entre a rede de dados da unidade administrativa remota e a Sede da PGE/RJ.

4.5 Serviços, equipamentos e materiais para implantação:

4.5.1 A CONTRATADA deverá realizar todos os serviços necessários de instalação, configuração e infraestrutura básica, para prover os acessos físico e lógico nos endereços indicados pela CONTRATANTE. Deve, ainda, fornecer todos os equipamentos, conectores, cabos, materiais diversos necessários para implantar os circuitos de redes fim-a-fim;

4.5.2 Nestes serviços estão incluídas as configurações de rede, testes de conectividade e roteamento, VPN, segurança de conectividade, túneis IPSEC, segmentação lógica via VLANs, como por exemplo : https, ipsec, acls, entre outros, que

permitam a conexão dos serviços de rede instalados no Datacenter ou Endpoints instalados na rede local do Edifício-Sede da PGE/RJ, que possam se conectar com outros serviços de rede locais das unidades remotas ou no acesso à Internet.

4.6 O aceite da instalação de cada localidade do Núcleo Central e da Rede Externa será dado após a confirmação de operação estável por 30 dias.

4.7 Consideramos operação estável, a visualização pela equipe técnica da CONTRATANTE de "status" normal na ferramenta de gerenciamento no Portal de Acompanhamento de Serviços e Monitoramento disponibilizada pela CONTRATADA.

4.8 Neste objeto, estão inclusos equipamentos de NFGW C/ SDWAN , que serão fornecidos pela CONTRATADA DO LOTE 1.

4.9 Requisitos Exigidos pela Rede MPLS e IP Dedicado

4.9.1 Cada porta de acesso à rede da CONTRATADA deverá ter acesso dedicado com as velocidades descritas na Tabela 2 (LOTE 1– Localidades, Serviço e Velocidades) e Tabela 3 (LOTE 2 – Tabela lotes, localidades, serviço) não podendo ser compartilhada com nenhum outro cliente da CONTRATADA.

4.9.2 Os acessos deverão absorver 100% (cem por cento) do tráfego referente às velocidades contratadas, garantindo o não descarte de pacotes.

4.9.3 Os equipamentos CPE, necessários à interligação das localidades à rede da CONTRATADA, serão de propriedade da mesma e por ela fornecidos, instalados, configurados e monitorados, em conjunto com a PGE/RJ.

5. DOS LOCAIS PARA A PRESTAÇÃO DOS SERVIÇOS

5.1 Os serviços – pontos de acesso – serão prestados nos endereços abaixo descritos:

Ite m	Unidades PGE (Lote 1 e 2)	Endereços
01	SEDE	Rua do Carmo, 27 - Centro - Rio de Janeiro, RJ
02	PR01 – NITEROI	Rua Visconde de Sepetiba, 935 / 7° andar - Centro - Niterói, RJ
03	PR02 - DUQUE DE CAXIAS	Avenida Brigadeiro Lima e Silva, 1939 / 6° e 7° andares - Vinte de Agosto - Duque de Caxias, RJ
04	PR03 - NOVA IGUAÇU	Rua Comendador Soares, 194 / 2º andar - Ed. São Paulo Business Center - Centro - Nova Iguaçu, RJ
05	PR04 - BARRA DO PIRAÍ	Rua Dona Guilhermina, 100 - Chácara Farani - Barra do Piraí, RJ
06	PR05 - VOLTA REDONDA	Avenida Paulo de Frontin, 590 / Salas 1001 a 1013 - 10º andar - Aterrado - Volta Redonda, RJ
07	PR06 - ANGRA DOS REIS	Rua do Comércio, 10 - Sobreloja - Centro - Angra dos Reis, RJ
08	PR07 - PETRÓPOLIS	Rua do Imperador, 288 / Salas 30 a 35 - Shopping Dom Pedro II - Centro - Petrópolis, RJ

09	**PR08 - NOVA FRIBURGO**	Rua Dante Laginestra, 49 - Centro - Nova Friburgo, RJ
10	**PR09 – MACAÉ**	Avenida Nossa Senhora da Glória, 999 / 1º andar - Cavaleiros - Macaé, RJ
11	**PR10 – CAMPOS**	Rua Gastão Machado, 66 - Parque Tomás Coelho - Campos dos Goytacazes, RJ
12	**PR11- ITAPERUNA**	Avenida Zulamith Bittencourt, 300 / Sala 104 - 4º andar - Ed. Residencial Ajala - Centro - Itaperuna, RJ
13	**PR12 - CABO FRIO**	Rua Domingos Ribeiro, 62 - Passagem - Cabo Frio, RJ
14	**PR13 - SAO GONÇALO**	Rua Coronel Serra, 1000 / 7º andar - Zé Garoto - São Gonçalo, RJ
15	**PG-13 - BRASÍLIA**	SAF/S, Quadra 02, Lote 04, Sala 304 - Cond. Via Esplanada - Brasília, DF
16	**CONVENTO DO CARMO**	Praça XV de Novembro, 101 (Antigo Convento do Carmo), Centro, Rio de Janeiro/RJ – CEP: 20010-010
17	**TJ-RJ**	Endereço: Av. Erasmo Braga, n° 115 Centro, Rio de Janeiro/RJ – CEP 20020-903

Tabela 1 - Tabela de Endereços das Localidades

O local de prestação dos serviços poderá sofrer alterações no decorrer da execução do Contrato, conforme solicitação da CONTRATANTE, nos termos do art. 124 da Lei nº 14.133/2021, desde que devidamente justificado por motivo de interesse público, necessidade técnica ou operacional, e sem que isso implique, por si só, a descaracterização do objeto contratado.

5.2 Ocorrendo a necessidade de alteração do local de instalação de qualquer equipamento, a CONTRATADA deverá providenciar o desligamento, desinstalação, transporte e reinstalação no local indicado pela PGE/RJ, no prazo denifido teste, a contar da abertura de chamado, sem ônus para a CONTRATANTE.

5.3 A interligação entre a Procuradoria Geral do Estado do Rio de Janeiro (PGE-RJ) e a REDE GOV CONNECTA será realizada por meio de link MPLS fornecido pelo PRODERJ, sendo este o único órgão autorizado a prover tal serviço.

6. DO PRAZO DE VIGÊNCIA DO CONTRATO

6.1 O prazo de vigência do Contrato é de 60 (sessenta) meses, contado da data indicada na Ordem de Serviço, desde que previamente divulgado no Portal Nacional de Contratações Públicas.

6.2 O prazo de vigência do Contrato poderá ser prorrogado, sucessivamente, até o máximo de 10 (dez) anos, na forma dos arts. 106 e 107 da Lei n° 14.133/2021, desde que observadas as condições previstas no Contrato, e mediante a celebração de termo aditivo.

7. DO CRITÉRIO DE JULGAMENTO

7.1 A nova contratação será realizada por procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO GLOBAL POR LOTE.

7.2 **Do modo de Disputa**

7.2.1 O modo de disputa será aberto, hipótese em que os licitantes apresentarão suas propostas por meio de lances públicos e sucessivos, com prorrogações.

7.3 **Justificativa da adequação e da eficiência**

7.3.1 A combinação dos parâmetros Pregão e Menor Preço é adequada e eficiente para contratação de empresa especializada para prestação de serviço de redes *Multi Protocol Label Switching* (MPLS) e circuitos de acesso à Internet com LINK DEDICADO, SDWAN, gerenciamento proativo contra falhas e incidentes de segurança cibernética com a utilização de solução de Next Generation Firewall - NGFW nas atividades operacionais, conforme os seguintes pontos:

a) Adequação

- O pregão mostra-se apropriado para a presente contratação, uma vez que os serviços de comunicação de dados, incluindo conectividade entre a Sede e as Procuradorias Regionais, bem como acesso à internet, no âmbito da Procuradoria Geral do Estado, possuem padrões de desempenho e de qualidade que podem ser descritos de forma objetiva no edital, por meio de especificações usuais de mercado, atendendo, assim, ao disposto no art. 29 da Lei nº 14.133/21
- Simplificação do Processo: O Pregão Eletrônico facilita a condução rápida e competitiva, atendendo à necessidade de eficiência e prazos curtos.

b) Eficiência

- Menor Preço garante a contratação mais econômica, promovendo a obtenção da proposta mais vantajosa para a administração.
- Redução de Custos: O Pregão fomenta a concorrência, resultando em preços mais vantajosos e redução de custos operacionais.
- Objetividade: A escolha do fornecedor é clara e sem subjetividade,

baseada exclusivamente no menor preço ofertado, respeitando as condições técnicas exigidas.

7.4 Essa combinação assegura a competitividade e a vantajosidade econômica, alinhando-se aos princípios da Lei nº 14.133/2021.

8. RESULTADOS ESPERADOS

8.1 Manutenção do funcionamento de acesso a rede corporativa com no mínimo os atuais níveis de serviços prestados

8.2 Maior nível de informações, sobre o tráfego e da segurança no acesso à rede e à Internet.

8.3 Maior eficiência na proteção de acessos remotos, por meio da adoção de recursos de MFA (Autenticação Multifator), que exigem duas ou mais formas de verificação, e de ZTNA (*Zero Trust Network Access*), que restringe o acesso a aplicações com base em identidade, dispositivo, contexto e políticas definidas. Permite a substituição gradual da VPN tradicional, proporcionando maior controle, segurança e flexibilidade no acesso remoto.

8.4 Fornecimento centralizado de conectividade à Internet para as unidades que compõem a Rede Governo, permitindo uma melhor gestão do serviço.

8.5 Possuir Plano de *Disaster Recovery* (DR) funcional e validado, em caso de perda total do Datacenter da SEDE;

8.6 Tráfego de dados estável e seguro entre as localidades;

8.7 Permitir o acesso aos sistemas de informação hospedados pela REDE-GOV e demais órgãos da administração pública direta e indireta aos servidores públicos e cidadãos;

8.8 Melhorar o aproveitamento de recursos e serviços de tecnológicos;

8.9 Manter e melhorar o nível de eficiência e segurança da rede com os serviços especializados de monitoramento de rede e de segurança cibernética, bem como permitir que a rede possa ser utilizada para os novos serviços de tecnologia, como por exemplo IA e voz sobre IP (VoIP).

9. DAS ESPECIFICAÇÕES TÉCNICAS DO OBJETO

LOTES 1 E 2:

9.1. Todos os equipamentos deverão ser fornecidos com bandeja, cabos ou suporte para montagem em rack 19";

9.1.1. Deverá possuir LEDs de diagnóstico que forneçam informações de alimentação e atividade do equipamento;

9.1.2. Deverá possuir console com porta USB

9.1.3. O equipamento deve possuir fontes de energia interna, bivolt automatico e capacidade de operação em 100V à 240V (50/60Hz);

9.2. **Os roteadores**

9.2.1. Devem possuir memória com capacidade suficiente para armazenar, no mínimo, duas novas versões de sistema operacional que tenha o tamanho de duas vezes o sistema operacional na versão atual.

9.2.2. Os equipamentos fornecidos pela CONTRATADA lotes (1 e 2) deverão ser dimensionados de forma a garantir o desempenho e os níveis de serviço requeridos para os serviços fornecidos descritos neste documento.

9.2.3. A CONTRATADA lotes (1 e 2) deverá fornecer e gerenciar os equipamentos CPE, necessários a interligação de novas localidades à rede.

9.2.4. Deve possuir a quantidade mínima necessária de memória RAM e memória auxiliar que atenda a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do Fabricante.

9.2.5. Deve possuir uma porta de console para o gerenciamento e configuração do equipamento, no padrão RS-232, com conector RJ-45 ou DB-9

9.2.6. Deve permitir auto-negociação de modo de transmissão *half / full-duplex* para as interfaces Ethernet.

9.2.7. Os roteadores instalados deverão permitir a configuração de parâmetros de Qualidade de Serviço (QoS).

9.2.8. Os roteadores instalados deverão suportar o padrão IEEE 802.1Q, permitindo assim a configuração de VLANs.

9.2.9. Deve possuir LEDs de diagnóstico que forneçam informações de alimentação e atividade do equipamento

9.2.10. Deve possuir LEDs de diagnósticos que forneçam informações e status das portas;

9.2.11. Caso o Fabricante possua mais de uma versão de uma mesma placa para atendimento a esta especificação, deverá ser fornecida a versão mais recente e estável da mesma;

9.2.12. Deve possuir suporte à tradução de endereços de rede (*Network Address Translation* – NAT) em conformidade com a RFC 1631 e RFC 3022;

9.2.13. Deve possuir suporte à tradução de endereços de porta (*Port Address Translation* – PAT);

9.2.14. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interface Ethernet;

9.2.15. Possuir ferramentas para depuração e gerenciamento em primeiro nível para IPv4 e IPv6, implementando ao menos, testes ICMP, debug, trace e log de eventos;

9.2.16. Deve suportar a implementação da funcionalidade de DHCP Relay e DHCP Server;

9.2.17. A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo IPFIX padronizado, para no mínimo: Net Flow ou Sflow ou JFlow ou Hflow ou Cflowd;

9.2.18. Deve implementar o protocolo VRRP (*Virtual Router Redundancy Protocol*), em conformidade com o padrão RFC 2338;

9.2.19. Deve possibilitar a implementação de Lan Virtual (VLAN) por porta e compatíveis com o padrão IEEE 802.1Q e IEEE 802.1Q-in-Q;

9.2.20. Deve implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseado em um servidor de autenticação e autorização do tipo TACACS+;

9.2.21. Deve implementar mecanismos de AAA (*Authentication, Authorization e Accounting*) com garantia de entrega;

9.2.22. Deve implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP;

9.2.23. Deve implementar filtragem de pacotes (listas de controle de acesso) para IPv4 e IPv6;

9.2.24. Deve suportar serviços de *Virtual Private Network* (VPN) baseados no padrão IKE (*Internet Key Exchange*);

9.2.25. Deve suportar a criação de VPN baseado no padrão IPSEC, suportar algoritmos de criptografia 56-bit DES, 168-bit 3DES, 128-bit AES e 256-bit AES para conexões VPN com IPSEC

9.2.26. Deve permitir a criação de VPNs IPSec baseada em politícas de segurança;

9.2.27. Deve reagrupar pacotes de sessão de VPN fragmentados para análise e entrega no destino;

9.2.28. Os equipamentos instalados deverão possuir o protocolo de gerenciamento NETCONF e/ou SNMP (versão 3 ou mais atual) e suportar a especificação MIB-II, implementados em conformidade com as RFCs 1157, 1213 e 2570, respectivamente.

9.2.29. É de responsabilidade da CONTRATADA informar à PGE/RJ sobre novas versões de sistemas operacionais e/ou "*firmware*", bem como correções de vulnerabilidades;

9.2.30. Sempre que houver lançamento de uma nova versão de sistema operacional e/ou "*firmware*" que faça correções de segurança ou dos serviços prestados, deverá ser agendada formalmente juntamente com a PGE/RJ pela CONTRATADA a atualização do sistema e/ou "*firmware*" dos equipamentos instalados. Neste caso, a CONTRATADA realizará as atualizações sem nenhum ônus à PGE/RJ.

9.2.31. Quando uma solicitação de alteração da taxa de transmissão ou a implementação de protocolos e serviços de QoS implicar na violação dos percentuais máximos de utilização da CPU e memória, os roteadores que não atenderem a estes parâmetros de desempenho deverão ser trocados, sem nenhum tipo de ônus para a PGE/RJ, no prazo máximo de 60 (sessenta) dias corridos.

9.3. **Projeto de rede**

9.3.1. A CONTRATADA do lote 1 e 2, deverá elaborar e apresentar Projeto de rede detalhado a CONTRATANTE para análise e aprovação;

9.4. A CONTRATADA deverá fornecer como parte integrante da solução todos os serviços, equipamentos, cabos, conectores, *softwares* entre outros, necessários para garantir a completeza e a funcionalidade integral dos serviços contratados.

9.5A CONTRATADA deverá realizar *hands-on* e contemplar todos os recursos e configurações existentes na solução ofertada do LOTE;

9.5.1 O hands-on será direcionado aos técnicos da CONTRATANTE, focado na operacionalização, conhecimento das configurações existentes, sua utilização, monitoramento dos equipamentos e relatórios para até três servidores

9.5.1.1 Carga horária mínima de 24 (vinte e quatro) horas;

9.5.1.2 Deverá iniciar no prazo máximo de até 10 dias úteis contados da formalização da entrega de toda a solução do LOTE 1;

9.5.1.3 O *hands-on* será em português e diretamente nos equipamentos, softwares, consoles, de toda a solução do LOTE 1

9.5.1.4 A Contratante reserva-se o direito de solicitar pelo menos 2 novos hands-on, ao longo do contrato;

9.5.1.5 Poderá ser gravado para fins de documentação, caso seja de interesse da CONTRATANTE;

9.6 É de responsabilidade da CONTRATADA a instalação de todo o cabeamento necessário até o quadro de distribuição interno e CPE. A CONTRATADA deverá identificar todos os equipamentos e o cabo lógico utilizado para a conexão ao CPE.

9.7 A CONTRATANTE informará à CONTRATADA a localização exata (sala e móvel) da instalação do CPE na localidade, após a assinatura do Contrato.

9.8 A CONTRATADA poderá realizar visita prévia de vistoria a fim de verificar as condições de instalação do serviço de acesso das localidades situadas no edifício Sede da PGE e nos centros de redes das unidades administrativas remotas, localizadas no território fluminense e em Brasília/DF, discriminados na Tabela 1 - Tabela de Endereços das Localidades.

9.9 As incorreções, como falta de ponto de força, aterramento inadequado e fios de energia internos necessários para a instalação do CPE da localidade, deverão ser corrigidos e/ou providenciados pela CONTRATANTE.

9.10 É de responsabilidade da CONTRATADA lotes (1 e 2) verificar se as instalações elétricas internas das localidades estão de acordo com as normas da ABNT 5410/19, para que a CONTRATANTE possa promover as devidas correções, se assim for necessário.

9.11 Em ambos os lotes (1 e 2) é obrigatoria a utlização de criptografia *end-to-end* para todos os túneis IPSEC das rede MPLS, além do QoS, segmentação lógica via VLANs para proteção de serviços sensíveis (VoIP, videoconferência, sistemas judiciais).

9.12 Em ambos os lotes (1 e 2) a CONTRATADA se responsabilizará pela implantação nas unidades da CONTRATANTE (item 5 – Dos Locais Para A Prestação Dos Serviços) e de toda a infraestrutura necessária à configuração dos canais de comunicação. Dentre os itens de infraestrutura a serem fornecidos pela CONTRATADA, caso seja necessário, estão: abertura, construção/reforma de caixas de passagem, instalação de dutos entre a caixa de passagem e a unidade, lançamento de cabos e recomposição de calçada, parede, gesso, quando for necessário.

9.13 Em ambos os lotes (1 e 2) a CONTRATADA deverá disponibilizar em seu *backbone* proteção contra ataques de negação de serviços, evitando assim a saturação

da banda da Internet e a indisponibilidade dos serviços em momentos de ataques DOS (DoS – Denial of Service) e DDOS Distributed Denial of Service).

9.13.1 A análise deverá ser passiva, sem utilização de elementos probes para coleta dos dados a serem analisados;

9.13.2 A Solução deverá prover o serviço de mitigação de ataques de negação de serviço distribuídos (DDoS – *Distributed Denial of Service*) ou não (DoS – *Denial of Service*) para o circuito de conectividade IP dedicada à Internet.

9.13.3 O ataque deve ser mitigado na estrutura da CONTRATADA, separando o tráfego legítimo do malicioso, de modo que os serviços de Internet providos continuem disponíveis.

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

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

9.13.6 Tomar todas as providências necessárias para recompor a disponibilidade do *link* em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo pela contratada.

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

9.13.7 Para a mitigação dos ataques, não deverá ser encaminhado o tráfego para limpeza fora do território brasileiro.

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

9.13.9 A mitigação de ataques deve ser baseada em uma arquitetura na qual há o desvio de tráfego suspeito, comandado pelo equipamento de monitoramento, por meio de alterações no plano de roteamento.

9.13.10 A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pela CONTRATANTE.

9.13.11 A solução deve suportar a mitigação automática de ataques, utilizando

múltiplas técnicas como *White Lists, Black Lists,* limitação de taxa, técnicas desafio-resposta, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP.

9.13.12 A solução deve implementar mecanismos capazes de detectar e mitigar todos os ataques que utilizem recursos de rede de forma não autorizada, incluindo, mas não se restringindo aos seguintes:

9.13.12.1 Ataques de inundação (*Bandwidth Flood*), incluindo *Flood* de UDP e ICMP.

9.13.12.2 Ataques à pilha TCP, incluindo mau uso das Flags TCP, ataques de RST e FIN, SYN *Flood* e TCP *Idle Resets*.

9.13.12.3 Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP.

9.13.12.4 Ataques de *Botnets, Worms* e ataques que utilizam falsificação de endereços IP origem (*IP Spoofing*).

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

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

9.13.15 Realizar a comunicação da ocorrência do ataque ao órgão do Governo CONTRATANTE imediatamente após a detecção;

9.13.16 Disponibilizar relatórios mensais de mitigação de ataques;

9.13.17 Disponibilizar um Centro Operacional de Segurança no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

9.13.18 A proteção deverá operar sem exigir o desligamento de qualquer outro circuito de acesso do Órgão, independente de quantos ou quais sejam os demais fornecedores;

9.13.19 A solução ofertada não poderá afetar a visibilidade do endereço de origem das requisições, mantendo o tráfego legítimo livre de qualquer modificação;

9.13.20 A CONTRATADA deverá disponibilizar acesso a sistema de monitoramento que permita a visualização do tráfego, emissão de relatórios,

visualização de alertas e informações da conta associada aos serviços de proteção;

9.13.21 Uma vez que o ataque é detectado pela solução, o equipamento instalado no *backbone* da operadora, responsável pela mitigação do trafego de ataque, deverá ser alertado e então todo o trafego do cliente deverá ser direcionado imediatamente, sem impactos e/ou interrupção do serviço;

9.13.22 A CONTRATADA deverá comunicar via *WhatsApp*, com a equipe de TI responsável da PGE-RJ do início à mitigação do tráfego;

9.13.23 Caso a CONTRATADA por qualquer razão não consiga contato com a equipe responsável da PGE-RJ, esta poderá implementar as ações de mitigação do ataque que julgar necessárias, comunicando assim que possível a CONTRATANTE.

9.14 A solução de gerência LOTE 1 tem por objetivo ofertar uma camada de segurança essencial para a Rede e todos os pontos de presença contratados e de acordo com as especificações do Termo de Referência e este Encarte Técnico.

9.15 A solução de segurança e do tráfego LOTE 1 deverá conter as ferramentas de *hardware* e *software* necessárias ao devido monitoramento, detecção e tratamento dos incidentes, operadas por equipe com os perfis especificados neste termo, não restringindo quanto à existência de outra estrutura adicional.

9.16 A solução de segurança NGFW a ser fornecida pelo MSS no LOTE 1, não fará parte da solução de SD-WAN (concentradora rede principal que interligará com rede EXTERNA), SD-WAN somente para os links de INTERNET bem como recursos de segurança necessários, especificados neste termo.

9.17 O equipamento de SD-WAN concentrador que interligará a rede externa, deverá ser HA ativo/ativo em alta disponibilidade;

9.18 As soluções SD-WAN e MSS devem atender às boas práticas recomendadas pelo NIST e ISO 27001.

9.19 A solução de segurança deverá contemplar o serviço de Gerenciamento de Segurança (MSS), interligado a um SNOC (*Security and Network Operation Center*), o qual deverá dispor das ferramentas de *hardware* e *software* necessárias para o adequado monitoramento, detecção e tratamento de incidentes de forma remota. As atividades deverão ser executadas por equipe especializada, em regime de atendimento 24x7, sendo essa estrutura localizada nas dependências da CONTRATADA.

9.20 Em casos de incidentes graves (parada total), deverá ser providenciado o deslocamento de um analista de segurança da informação LOTE 1 para a PGERJ no prazo máximo de 1 (uma) hora.

9.21 A solução de proteção NGFW fornecida pelo MSS deverá possuir a funcionalidade de SD-WAN e deverá ser capa de realizar o balanceamento de carga e agregação de banda melhorando a capacidades comunicação para o tráfego de acesso a INTERNET dos Lotes 1 e 2 de forma que se permita realizar a gestão integrada dos serviços, processos e infraestruturas disponibilizadas.

9.22 A solução de SD-WAN deve possuir os recursos de:

9.22.1 Failover automático e dinâmico e com medição de (latência, perda de pacotes, *jitter*)

9.22.2 Roteamento baseado em aplicação.

9.22.3 Monitoramento ativo de *links*

9.22.4 *Link health monitoring*.

9.22.5 Otimização por IA/ML (em soluções como Mist, Prisma SD-WAN)

9.22.6 Orquestração centralizada com templates e políticas unificadas

9.22.7 Integração com NGFW e políticas de segurança

9.23 A solução de SD-WAN da CONCENTRADORA PRINCIPAL com a rede externa, deverá ser uma soluçao em *appliances* físico, *on-primes,* ativo/ativo, em HA alta disponibilidade, fornecer o recurso de balanceamento de carga e agregação de banda melhorando a capacidades destes enlaces de comunicação para o tráfego de dados e integrar física e logicamente os serviços de MPLS dos Lotes 1 e 2 de forma que se permita realizar a gestão integrada dos serviços, processos e infraestruturas disponibilizadas.

9.24 A Solução de Gerência do lote 1 deverá disponibilizar a visualização de informações *on-line* (de forma gráfica) da rede para o acompanhamento e monitoração do estado global e detalhado do ambiente;

9.25 Deverá ser possível criar políticas para a modelagem do tráfego definindo pelo menos os seguintes parâmetros:

A. IP de origem;
B. IP de destino;
C. Porta TCP/UDP de destino;
D. URL de destino.

9.26 Deve ser possível definir qual *link* será utilizado em situação normal por determinada aplicação.

9.27 Deve ser possível definir qual *link* será utilizado em caso de falha do(s) *link(s)* primário(s).

9.28 Deve possuir solução de gerenciamento que permita realizar configurações em todos os *applicances* SD-WAN da rede de forma centralizada e ou individualizado;

9.29 A configuração de todos os equipamentos envolvidos na solução será efetuada pela CONTRATADA com base em informações fornecidas pela CONTRATANTE.

9.30 Após a conclusão da etapa de instalação dos serviços (lote 1 e 2), a CONTRATADA deverá apresentar documentação técnica da solução (*As Built*), contendo:

A. Topologia física e lógica da rede; (desenho, detalhamento dos ips, vlans de cada ponto e interligações)
B. Descrição de equipamentos e circuitos de comunicação de dados;
C. Descrição dos níveis mínimos de serviços contratados;
D. Dados para acesso ao portal de monitoramento dos serviços;
E. Dados para abertura de chamados de suporte técnico;

9.30.1 O aceite da instalação do serviço será dado após 30 dias da disponibilidade do serviço na Rede PGE/RJ.

9.30.2 A estrutura tecnológica deverá ser implantada em camada para melhor gestão e controle, conforme descrito abaixo:

9.30.3 O Núcleo Central, situado no Edifício-Sede da PGE/RJ, tem a finalidade de interligar as unidades remotas ao datacenter da PGE, através de um segmento de rede de alta velocidade que permite a conexão da rede de dados à concentradora MPLS à internet, com níveis de serviço e segurança diferenciados de acordo com a finalidade e o tipo de tráfego. Na **tabela 2 LOTE 1– Localidades, Serviço e Velocidades** e **Tabela 3 LOTE 2 – Tabela lotes, localidades, serviço** a seguir, estão indicadas as localidades, seus endereços e respectivas velocidades de acesso:

9.31 **IP Dedicado – Ambos os lotes** deverão fornecer 1 link de internet dedicado com velocidade de 1 Gbps com IP fixo, ambos disponibilizaram 12 endereços IP validos (1- rede; 1 *broadcasting* e 10-*hosts*) (não necessáriamente em sequência), a CONTRATADA do LOTE 1 será responsável pelo balanceamento da internet entre os links de Internet (do Lote 1 e 2);

9.31.1 Todos os equipamentos de acesso e acessórios, que serão instalados no edifício Sede deverão possuir interface de rede *Ethernet* com velocidade mínima de 1 Gbps, preferêncialmente com portas SPF/SFP+ (roteadores dos *links* e *appliances Firewall*, SD-WAN), necessários às conexões da Rede LAN e WAN da PGE/RJ, permitindo acesso à CONTRATANTE de monitoramento de acesso real.

9.31.2 Para garantir a padronização dos equipamentos de rede, todos os equipamentos fornecidos pela CONTRATADA do **LOTE 1** deverão ser do mesmo fabricante.

9.31.3 Para garantir a padronização dos equipamentos de rede, todos os equipamentos fornecidos pela CONTRATADA do **LOTE 2** deverão ser do mesmo fabricante.

9.31.4 A implantação de um sistema de gerenciamento centralizado de infraestrutura de rede e segurança pressupõe a existência de padrões compatíveis de integração, visibilidade e controle entre os equipamentos e sistemas envolvidos. Entretanto, em ambientes compostos por soluções de múltiplos fabricantes (*multi-vendor*), surgem limitações técnicas que inviabilizam, ou ao menos comprometem significativamente, essa centralização, tais como:

a) Protocolos e APIs proprietários;

Cada fabricante utiliza padrões próprios de comunicação, dificultando ou impedindo a integração nativa com painéis unificados de gerenciamento.

b) Falta de interoperabilidade plena;

Funcionalidades avançadas (como SD-WAN, IPS, DLP, ZTNA, automação e resposta a incidentes) muitas vezes não são suportadas de forma uniforme entre marcas, criando inconsistências no controle.

c) Fragmentação na gestão de políticas e atualizações;

Políticas de segurança, regras de *firewall* e atualizações de *firmware* precisam ser gerenciadas individualmente em cada solução, o que aumenta o risco de erro humano e dificulta a governança.

d) Limitações de visibilidade e correlação de eventos;

Sistemas de fabricantes distintos dificultam a correlação centralizada de *logs* e eventos, prejudicando a eficácia de soluções SIEM/SOAR e da resposta a incidentes.

e) Complexidade operacional e aumento de custos;

A gestão *multi-vendor* exige múltiplas ferramentas, múltiplas competências técnicas e processos duplicados, tornando a operação mais complexa, cara e sujeita a falhas.

9.31.5 Portanto, não é tecnicamente viável assegurar um gerenciamento centralizado eficaz em um ambiente composto por múltiplos fabricantes, sem o uso de soluções

intermediárias complexas, caras e com limitações técnicas. A padronização de fabricantes e plataformas é recomendada para garantir visibilidade, segurança, automação e gestão unificada, conforme as melhores práticas de mercado.

9.31.6 O serviço contratado deverá permitir modificações ou ampliações sem que estas impliquem na interrupção do restante das conexões da rede.

9.31.7 Poderão ser solicitadas durante a vigência do Contrato, mudanças de endereço, sem custos para a CONTRATANTE, mantendo o acesso antigo em funcionamento até 4 (quatro) horas antes da ativação do novo acesso, no novo endereço e deverão respeitar o seguintes prazos após a solicitação:

9.31.7.1 Uma semana (7 dias corridos) para vistoria no novo endereço a ser implementado;

9.31.7.2 Caso o local já tenha viabilidade técnica, 1semana (7 dias corridos) para implementar no novo endereço.

9.31.7.3 Caso não tenha viabilidade técnica e seja preciso somente passagem de fibra, 15 dias (corridos) para implementação;

9.31.7.4 Caso não tenha viabilidade técnica e precise de contrução até o novo local, 45 dias (corridos).

9.31.8 Quaisquer alterações relativas aos serviços de acesso serão informadas pela CONTRATANTE, através de *e-mail* e/ou documento próprio a ser definido após a assinatura do Contrato.

9.31.9 Lotes (1 e 2) sempre que for solicitada pela equipe técnica da PGE/RJ a alteração na configuração ou reconfiguração do *FIREWALL* e/ou roteador de acesso à PGE/RJ ou do gerenciador de tráfego SD-WAN, a CONTRATADA realizará, por meio de chamado, sem nenhum ônus para a PGE/RJ. Caberá a CONTRATADA fazer análise de risco e comunicar a CONTRATANTE, que deverá autorizar formalmente a implementação. Toda e quaisquer configurações e reconfigurações, ficará a cargo da CONTRATADA e a realização de *backups* para possível *downgrade* da configuração ou reconfiguração malsucedida.

9.31.10 Lotes (1 e 2) a CONTRATADA deverá fornecer à PGE/RJ as senhas de acesso, via portas de console e remota, para cada um dos ECDs (Equipamentos de Comunicação de Dados) instalados nas dependências desta, com privilégios para operações de leitura.

9.31.11 Também deverá ser fornecido acesso de leitura às estatísticas de SNMP (comunidade de leitura ou usuário/senha), além de configurar os ECDs

para gerar logs (Syslog – RFC 3164) ou traps SNMP para todos os circuitos e endereços IPs disponibilizados para a PGE/RJ.

9.31.12 A configuração inicial dos equipamentos para ativação dos serviços, incluindo parâmetros e ajustes relativos à solução de gerenciamento do tráfego, será sempre de responsabilidade da CONTRATADA, observadas as diretrizes do Plano de Segurança a ser repassado pela PGE/RJ.

9.31.13 As senhas de leitura serão compartilhadas entre a PGE/RJ e a CONTRATADA conforme o disposto no Acordo Operacional.

9.31.14 Os ECDs instalados na PGE/RJ deverão estar configurados para permitir acesso remoto somente através de SSH v2 e WEB HTTPS, ficando por conta da CONTRATADA o fornecimento de todos os recursos necessários à configuração remota, sempre sem nenhum ônus à PGE/RJ.

9.31.15 As manutenções programadas deverão ser limitadas a 04 (quatro) eventos por ano. Acima de 4 manutenções programadas será considerado como uma paralisação da rede e com as penalidades previstas no Acordo de Nível de Serviço (ANS).

9.31.16 As manutenções programadas deverão ser comunicadas à CONTRATANTE com, no mínimo, 05 (cinco) dias utéis de antecedência e deverão ocorrer no período de 00:00hs até as 06:00hs, durante o final de semana ou acordado com a CONTRATANTE.

9.32 Gerenciamento da Rede (de cada LOTE)

9.32.1 Configuração da Rede

9.32.1.1 A CONTRATADA deverá monitorar e supervisionar (gerenciamento proativo) a sua rede de transporte da Rede Externa e do Núcleo Central, diagnosticando e solucionando de imediato as falhas, mesmo antes do desencadeamento da notificação pelo cliente

9.32.1.2 A responsabilidade pelo monitoramento proativo da Rede do Lote II é atribuição da CONTRATADA do Lote I, responsável pelo fornecimento dos enlaces principais com solução de SD-WAN embarcada.

9.32.1.3 Constatada a falha, interrupção ou qualquer anormalidade nos enlaces redundantes do Lote II, a CONTRATADA do Lote I deverá notificar formalmente, de forma imediata e automatizada, a CONTRATADA do Lote II para que sejam adotadas as providências corretivas cabíveis, conforme os prazos de resposta e solução definidos contratualmente.

9.32.1.4 A ferramenta ou portal de monitoramento de cada operadora deve ser capaz de possuir as seguintes informaçõs:

9.32.1.4.1Utilização de banda em cada *link* (MPLS／IP Dedicado);

9.32.1.4.2Latência ponta-a-ponta entre Sede e cada Regional;

9.32.1.4.3*Jitter* e perda de pacotes em tempo real;

9.32.1.4.4Alertas automáticos por *e-mail/SMS* para *thresholds* críticos.

9.32.1.5 A CONTRATADA ficará, também, encarregada de prestar esclarecimentos à CONTRATANTE, sobre eventuais falhas, sempre que este julgar necessário.

9.32.1.6 A CONTRATADA deverá informar a senha de acesso, com privilégios de leitura (*read-only*) de cada equipamento de acesso à rede de comunicação de dados, após o aceite da instalação.

9.32.1.7 A CONTRATADA deverá configurar os avisos de *trap* SNMP dos equipamentos de acesso (CPE), para serem enviados para o seu centro de gerência e para o centro de gerência da CONTRATANTE.

9.32.1.8 A CONTRATADA deverá informar à CONTRATANTE a "*string*" de leitura do parâmetro SNMP *Community (read-only)* dos equipamentos de acesso CPE.

9.32.2 Gerência Proativa (de cada LOTE)

9.32.2.1 A CONTRATADA deverá prover gerenciamento 24x7 (24 horas por 7 dias na semana) do acesso local e do equipamento de acesso (CPE), informando sobre possíveis falhas no circuito de ou no próprio CPE, com registros via e-mail, grupo do WhatsApp e através de um Portal de Acompanhamento de Serviços, que permita aos técnicos da CONTRATANTE (mediante identificação e senha) realizar consultas, emitir e visualizar relatórios.

9.32.2.2 Paralelamente, tomar as ações cabíveis para a resolução do problema, sem a necessidade do acionamento prévio pela CONTRATANTE

9.32.2.3 A CONTRATADA deverá permitir visualização, através de *web browser*, do acompanhamento dos registros de problemas e das ações executadas para a recuperação dos serviços, relativos pelo menos aos últimos 90 (noventa) dias, incluindo as seguintes informações:

A. Identificação do registro (número do chamado);
B. Data e hora da abertura do chamado (registro);
C. Descrição do problema;
D. Identificação do reclamante (nome e telefone);
E. Data e hora de conclusão do atendimento (fechamento do chamado);

F. Ações realizadas para a solução do problema;

G. Identificação do técnico responsável pelo atendimento.

9.33 Atendimento Técnico (de cada LOTE)

9.33.1 Cada chamada técnica deverá ser registrada pela CONTRATADA e possuir identificador (número) próprio repassado à CONTRATANTE, a fim de registro e acompanhamento das ocorrências. Uma vez registrada a ocorrência junto à CONTRATADA, ela deverá ser encaminhada para os procedimentos de atendimento e solução de problemas.

9.33.2 O serviço de Gerenciamento da Rede deverá dar suporte a chamados referentes à recuperação de falhas de circuitos e serviços.

9.33.2.1 Para configuração de equipamentos, endereçamentos, análise de desempenho, etc. deverá ser feito através de abertura de chamados pelos canais de comunicação disponibilizados pela CONTRATADA.

9.33.2.2 A abertura do chamado deverá ser realizada pela equipe do Serviço de Gerência PRO-ATIVA de Rede da CONTRATADA, imediatamente após a constatação de defeito ou falha em qualquer circuito ou serviço que esteja em funcionamento e seja da responsabilidade da operadora, com o atraso máximo de 1 minuto para links de Internet (lotes 1 e 2) e concentradores Sede (lotes 1 e 2) e 5 minutos para circuito mpls nas localidades.

9.33.2.3 Deverá ser disponibilizado um canal de comunicação via WhatsApp para agilidade para abertura, tratamento e encerramento dos chamados, bem como poder abrir via e-mail, além dos canais normais.

9.33.2.4 Após a abertura ou encerramento do chamado, a CONTRATADA deverá enviar à CONTRATANTE, no prazo máximo de 10 (dez) minutos, um e-mail contendo:

9.33.2.4.1 No caso de abertura do chamado: o número de protocolo, a descrição do incidente, as providências já adotadas e a estimativa de tempo para solução;

9.33.2.4.2 No caso de encerramento do chamado: o registro da solução aplicada e a confirmação do restabelecimento do serviço.

9.33.2.5 As informações dos chamados, deverão ser disponibilizada e visualizadas deverão conter:

A. Número do chamado;

B. Estimativa para solução do problema;

C. Data e hora da abertura e fechamento;

D. Status (aberto/fechado) informando as providências tomadas;

E. Localidade;
F. Responsável pela abertura (CONTRATADA e CONTRATANTE quando reativa);
G. Descrição do problema;
H. Histórico do problema (com os contatos mantidos);
I. Ocorrências;
J. Solução implementada (com a sequência cronológica das ações tomadas).

9.32.2.6 Os chamados técnicos só poderão ser considerados encerrados e solucionados, através de aceite da CONTRATANTE.

9.33 Portal de Gerência (de cada LOTE)

9.33.3 A visualização das informações deverá ser via *web*, por qualquer *browser*, através de login e senha no Portal de Gerência a ser disponibilizado pela CONTRATADA para a CONTRATANTE.

9.33.4 Deverá possuir interfaces para acesso, independente dos equipamentos ou tecnologias empregadas na prestação dos serviços.

9.33.5 O intervalo de coleta dos dados para exibição das informações deverá ser preferênciamente em tempo real e/ou pelo menos de 5 (cinco) minutos.

9.33.6 A visualização das informações, apresentando todas as funcionalidades listadas nos itens abaixo:

9.33.6.1 Alertas em caso de falhas e anormalidades dos circuitos, com grau de criticidade;

9.33.6.2 Topologia da rede ou Mapa da rede, incluindo roteadores e circuitos, com a visualização do status em tempo real de todos os elementos. O agrupamento dos elementos que compõem a topologia da rede (roteadores e circuitos) será definido pela CONTRATANTE;

9.33.6.3 Visualização da utilização de banda dos circuitos, em tempo real, diário, semanal e mensal, com a opção de consulta de dados históricos;

9.33.6.4 Visualização do consumo de CPU e memória dos roteadores em tempo real e, com a opção de consulta de dados históricos;

9.33.6.5 Visualização do tempo de resposta dos circuitos, em tempo real, com a opção de consulta de dados históricos;

9.33.6.6 Visualização de tráfego de vídeo e banda em uso, conforme solicitação;

9.33.6.7 Possuir gráficos em tempo real, a cada 5 minutos, 1h, 24h, 1 mês, 3 mês,

6 meses, 12 meses e customizáveis até 1 ano. A partir de qualquer estação de trabalho da rede da CONTRATANTE, por intermédio de navegador *web*, utilizando protocolo HTTPS;

9.33.6.8 A CONTRATADA deverá permitir a visualização da CONTRATANTE, através de *web browser*, da topologia da rede de CPE, com a possibilidade de verificar o status dos equipamentos (*up/down*), tráfego do link, disponibilidade por período, relatórios, tráfego detalhado (origem e destino), alarmes e eventos, relatórios mensais;

9.33.6.9 Tráfego dos *links*, cada *link*, de cada lote dever ser possivel que a CONTRATANTE tenha as seguintes informações detalhadas:

9.33.6.9.1 Volume de tráfego (download/upload) por intervalo de tempo, em tempo real, 5 minutos;

9.33.6.9.2 Protocolos e serviços detalhados (ex: HTTP, HTTPS, DNS, dropbox, youtube, etc.), com informação de origens (login de usario e ip) e destinos (ip, urls e/ou serviço);

9.33.6.10 Relatório de utilização de banda por período;

9.33.6.11 Taxa de descarte de pacotes, retransmissões ou erros por interface.

9.33.6.12 Latência e *jitte*r.

9.33.6.13 Eventuais alarmes e/ou falhas detectadas em períodos solicitados customizados (dd/mm/aaaa hh:mm] até [dd/mm/aaaa hh:mm);

9.33.6.14 Indicação de congestionamento nos circuitos, além dos valores de limiares excedidos e o enfileiramento e/ou descarte do tráfego nos roteadores;

9.33.6.15 Visualização dos chamados registrados, abertos e encerrados, dentro do prazo contratual, por data ou circuito, permitindo acesso ao detalhamento dos chamados;

9.33.6.16 Inventário dos roteadores contendo a configuração física de cada equipamento (interfaces, memória e CPU), modelo e fabricante, endereços IPs e máscaras;

9.33.6.17 Visualização do desempenho, por circuito, apresentando informações de taxa de erro, disponibilidade, latência, jitter e informações apuradas nos CPEs;

9.34 Relatórios (de cada LOTE)

9.34.1 O acompanhamento da qualidade dos serviços da rede, dos chamados e do Acordo de Nível de Serviços (ANS) pré-estabelecido, será feito através de relatórios disponibilizados pela CONTRATADA (operadora A e operadora B) no Portal de Gerência com periodicidade mensal ou sob demanda da CONTRATANTE.

9.34.2 A CONTRATADA deverá armazenar todos os dados e informações

coletadas durante a vigência do Contrato, tais como: dados brutos coletados nos elementos gerenciados, dados sumarizados para confecção de relatórios, acompanhamento dos chamados, acompanhamento da qualidade de serviço, de faturamento, dentre outros. Esses dados deverão ser disponibilizados à CONTRATANTE mensalmente durante a vigência do Contrato. Pode, ainda, ser solicitado pela CONTRATANTE, ao final do Contrato, um relatório completo com todos os dados coletados durante a vigência do contrato.

9.34.3 Todos os relatórios deverão permitir o uso de diversos filtros para visualizar as informações. Os filtros também deverão permitir a seleção de informações a serem impressas de um ou mais circuitos ou de toda rede, a critério da CONTRATANTE.

9.34.4 Todos os relatórios deverão possibilitar a seleção de datas de início e fim do período a que se referem os dados a serem exibidos.

9.34.5 O serviço de Gerência de Rede da CONTRATADA deverá permitir que todos os relatórios possam ser visualizados, armazenados em meios eletrônicos e impressos. Deverá ser implementada a funcionalidade de exportação dos relatórios em formatos compatíveis com MS Office e PDF.

9.34.6 Os relatórios abaixo deverão ser enviados até 5 (cinco) dias úteis, após o fechamento do mês. Após o aceite da CONTRATANTE, a CONTRATADA emitirá a fatura correspondente:

9.34.6.1 Relatórios de disponibilidade: devem ser emitidos mensalmente e apresentar informações com apuração diária, semanal e mensal.

9.34.6.2 Devem conter a análise de tendência quanto ao desempenho e à utilização dos recursos da rede;

9.34.6.3 Relatórios de tráfego: relatórios com apuração diária que apresentam o tráfego de todos os circuitos, com suas séries históricas, fornecendo subsídios para analisar o desempenho e as tendências de aproveitamento dos recursos da rede. Devem demonstrar informações da banda utilizada e do volume de tráfego;

9.34.6.4 Relatório de acompanhamento dos chamados: relatório com apuração diária com todas as informações relativas ao chamado como data, hora, identificação do elemento (circuito ou equipamento) e descrição detalhada do chamado;

9.34.6.5 Relatórios de chamados: relatório mensal de chamados abertos e encerrados, incluindo o índice de tempo médio de recuperação;

9.34.6.6 Relatórios de reincidência: relatórios que mostram problemas

reincidentes dos elementos (circuitos ou equipamentos) da rede;

9.34.6.7 Relatório de acompanhamento de ANS: descritivo de ANS, contendo para cada circuito as ocorrências de falhas, caso tenham existido e os valores mensais apurados para cada indicador (Parâmetros de Qualidade dos Circuitos e Serviços);

9.34.6.8 Relatório específico de ANS: relatório de acompanhamento de cada indicador a ser monitorado para o ANS. Estes relatórios devem ser emitidos mensalmente.

LOTE 1 e 2:

9.35 Rede MPLS:

9.35.1 Prestação de serviço de links de comunicação para implantação de uma rede de contigência contemplando o transporte de dados, voz e vídeo com a tecnologia MPLS;

9.35.2 Os enlaces físicos deverão ser providos por meio de roteadores fornecidos, instalados e configurados pela CONTRATADA, sendo instalados nas extremidades do enlace, conforme segue:

9.35.2.1 Um na extremidade da Sede da PGE/RJ, denominado de concentradora;

9.35.2.2 E outro, na extremidade individualizada localizada em cada uma das unidades individualizadas, incluindo todas as Procuradorias Regionais, a Procuradoria Especializada de Brasília/DF, a unidade do Convento e TJ-RJ.

9.35.2.3 Para o LOTE 1 o concentrador SDWAN deverá balancear o tráfego entre as concentradoras do LOTE 1 e 2, bem como o tráfego de origem e destino;

9.35.3 A taxa de transmissão está definida nas Tabelas 2 – Localidades, Serviço e Velocidades;

9.35.4 A CONTRATADA deverá ter viabilidade técnica imediata para atender as unidades administrativas descritas na Tabela 1 - Tabela de Endereços das Localidades. Ademais, a critério da CONTRATANTE, pode solicitar a mudança de localidade, assim como, aumentar a velocidade inicialmente definida, mediante acordo entre as partes;

9.35.5 Os enlaces deverão ser gerenciados de forma proativa, através de equipe da CONTRATADA dedicada a esta atividade;

9.35.6 A CONTRATADA deverá fornecer concentradoras suficientes para recebimento de toda a planta estimada nas Tabelas 2 – Localidades, Serviço e Velocidades, bem como os roteadores e demais equipamentos, e todos os custos deverão estar incluídos na precificação final a ser fornecida em cada item da Tabelas 2;

9.35.7 A automação e configuração do processo acima deverá ser executada pela CONTRATADA, utilizando as melhores práticas de mercado em ambas as extremidades dos *links*;

9.36 Qualidade de Serviço (QoS):

9.36.1 Os *links* de dados, objeto deste instrumento técnico, obrigatoriamente deverão suportar a implementação de mecanismos de garantia de banda e priorização de tráfego (QoS);

9.36.2 Além de priorizar aplicações críticas, o QoS deverá obrigatoriamente tratar o tráfego, de forma a otimizar o uso da rede, em casos de congestionamentos;

9.36.3 A PGE/RJ, através da Gerência de Tecnologia da Informação (GTI), irá definir em conjunto com a CONTRATADA as configurações de QoS, que deverão ser efetivamente implementadas para cada circuito, na ocasião da implantação dos *links* contratados ou sempre que se fizer necessária uma adequação;

9.36.4 Em situações normais, os tráfegos oriundo da rede externa, de sistemas e serviços corporativos, além dos tráfegos multimídia de telefonia IP e videoconferência deverão ser encaminhados pela rede MPLS do LOTE 1.

9.36.5 Em situações de falha ou de uso intenso da rede MPLS do LOTE 1, alternativamente o tráfego deverá ser encaminhados a rede MPLS do LOTE 2.

9.36.6 A rede MPLS deverão utilizar a topologia hub-and-spoke, com centralização nos equipamentos SD-WAN.

9.36.7 Deve possuir roteamento baseado em políticas e múltiplas saídas (e tipos de saídas) WANs.

9.36.8 Os serviços a serem prestados incluem, ainda, a elaboração prévia de um Projeto de rede, a ser analisado pela equipe técnica da PGE/RJ para aprovação, conforme especificações incluídas neste documento.

9.36.9 Este documento deverá possuir, no mínimo:

A. Definição de topologias físicas e lógicas;
B. Plano de endereçamento;
C. Plano de balanceamento do tráfego;
D. Parâmetros de qualidade de serviço;
E. Dimensionamento de enlaces e interfaces de comunicação;

9.36.10 A solução deverá ser capaz de fazer balanceamento de carga de enlaces para conexões de saída sem uso de equipamentos terceiros e de forma automática;

9.36.11 O balanceamento deverá ser capaz de selecionar o caminho para o destino usando pelo menos um dos seguintes métodos escolhidos pelo administrador:

A. RTT (*Round Trip Time*) ao destino através do uso do protocolo TCP, com enlace mais rápido ao destino encaminhando o tráfego para uma dada conexão;
B. Distribuição de tráfego em função da capacidade relativa entre os enlaces de comunicação;

9.36.12 A solução de gerência de tráfego SD-WAN deverá fornecer mecanismo de balanceamento de carga através dos enlaces para conexões VPN, sendo que as conexões poderão ser balanceadas aumentando a capacidade do túnel VPN IPSec;

9.36.13 Deverá implementar VPN IPSec com capacidade de implementar túneis site-to-site;

9.36.14 Deverá permitir o estabelecimento do túnel utilizando uma "chave secreta" ou certificados digitais;

9.36.15 Deverá implementar IKEv1 e IKEv2;

9.36.16 Deverá oferecer suporte pelo menos aos seguintes algoritmos de criptografia: 3DES, AES128, AES-256 e pelo menos aos seguintes algoritmos de autenticação: MD5, SHA1, SHA2-256 e SHA2-512;

9.36.17 O balanceamento de conexões VPN IP/IPSec deverá ser realizado através de túneis lógicos, não havendo necessidade de configuração de protocolo de roteamento adicional;

9.36.18 No caso de falha de um enlace, todas as conexões existentes deverão ser automaticamente transferidas (*statefully*) para o outro enlace que estiver ativo, sem a necessidade de intervenção do administrador;

9.36.19 Deverá ser possível acrescentar novos enlaces de comunicação sem que haja a necessidade de alterar enlaces existentes;

9.36.20 A configuração do encaminhamento do tráfego e da contingência em casos de falha deverá ser feita utilizando tecnologia SD-WAN em que o encaminhamento de tráfego é feito com base no perfil de tráfego em vez da utilização de rotas;

9.36.21 A CONTRATADA deverá realizar alterações nas configurações de QoS implementadas, a qualquer momento, mediante solicitação formal da PGE/RJ, devendo efetivá-las no prazo máximo de 15 (quinze) dias corridos;

9.36.22 Para garantir a implementação de QoS nos links contratados, a CONTRATADA deverá garantir que os roteadores MPLS estejam configurados para permitir que:

9.36.23 Todos os pacotes sejam marcados com um rótulo (MPLS Label) de 20 bits;

9.36.24 Todos os pacotes sejam marcados pelo MPLS na entrada da rede (MPLS Edge Routers);

9.36.25 Exista a possibilidade de reconhecer pacotes marcados na origem;

9.36.26 Todos os pacotes tenham os rótulos retirados na saída da rede (MPLS Edge Routers);

9.36.27 A garantia de Qualidade de Serviço (QoS) é fim-a-fim, envolve os equipamentos de rede (roteadores e *switches*) e, todos os equipamentos e tecnologias utilizados nas suas interconexões;

9.37 Classe de Serviço (CoS)

9.37.1 Com base nas RFC 2597 e 2598, diferentes Classes de Serviços (CoS) poderão ser definidas, possibilitando a diferenciação entre o tráfego, para a implementação de QoS. De acordo com as prioridades e níveis de serviços, os diferentes tipos de tráfego da rede PGE/RJ poderão, a critério da CONTRATANTE, a qualquer tempo, ser classificados nas seguintes classes de serviço, conforme a seguir:

9.37.2 Tempo real: aplicações sensíveis a retardo (*delay*) e variações de retardo (*jitter*), que exigem priorização de tráfego e reserva de banda;

9.37.3 Gerenciamento: aplicações de gerenciamento de rede e de sistemas, que necessitam de uma banda mínima para suporte técnico, mesmo em situações de congestionamento da rede, porém não ocupam banda suficiente para interferir nos demais tráfegos em condições normais de operação;

9.37.4 Dados prioritários: aplicações críticas para os negócios do Governo do Estado do Rio de Janeiro, que exigem entrega garantida, reserva de banda e tratamento prioritário;

9.37.5 Dados críticos: aplicações com grande volume de dados importantes, porém sem a necessidade de um tempo de resposta reduzido. Embora possam representar conteúdo importante, essas aplicações podem esperar por disponibilidade de recursos da rede, em horários com menor volume de transações, para serem efetuadas;

9.37.6 Melhor esforço: todo tráfego não atribuído às 3 classes acima, nem à classe Tempo Real. Sua finalidade é permitir uma alocação menor de recursos para os

tráfegos não previstos ou ainda não identificados como tráfegos prioritários ou críticos. É preciso garantir que tal tráfego possa fluir se houver recursos disponíveis na rede, sem afetar negativamente as demais classes.

9.37.7 Cabe ressaltar que em um primeiro momento, deverão ser utilizadas classes de serviços referentes aos dados, que são: Gerenciamento, Dados Prioritários e Dados Críticos. A classe Tempo Real, relacionada com os serviços de videoconferência e voz sobre IP (VoIP) só será utilizada quando solicitada pela CONTRATANTE.

9.37.8 Em situação de congestionamento, deverão ser assegurados, no mínimo, os tráfegos definidos para as classes Dados Prioritários e Dados Críticos, podendo todo tráfego restante ser classificado na classe Melhor Esforço.

9.37.9 As configurações referentes à probabilidade de descartes de pacotes, especificados na RFC 2597, deverão ser suportados pelo Backbone MPLS, porém não serão utilizadas num primeiro momento. No futuro, nos casos em que se observe congestionamento na rede, serão solicitadas para que seja possível a escolha de tráfegos específicos que terão pacotes descartados antes dos outros.

LOTE 1 e 2:

9.38 Redes IP:

9.38.1 Serviços de acesso dedicado à internet com fornecimento de infraestrutura para o ambiente computacional da PGE/RJ, com a finalidade de proporcionar escalabilidade, gerenciamento, performance, confiabilidade, continuidade e segurança no acesso e utilização das aplicações para os seus usuários externos e internos, para suportar o tráfego total de 1 Gbps, bidirecional *full-duplex* e transmissão síncrona.

9.38.2 Serviço de acesso dedicado à internet, com fornecimento de infraestrutura, responsáveis pela implantação, configuração e disponibilização de ferramentas de gerenciamento e manutenção de uma rede de serviços de dados para acesso IP, Dedicado e exclusivo, através de enlaces com larguras 1000 Mbits.

9.38.3 Além dos requisitos acima, os Equipamentos de Comunicação de Dados (ECDs) do tipo roteador fornecidos, deverão possuir também:

9.38.3.1 Porta LAN *Gigabit Ethernet* RJ-45 Cat6 preferencialmente SFP/SPF+;

9.38.3.2 Sistema operacional com suporte a:

a. Protocolos de roteamento, OSPF, RIP2, IGRP e EIGRP;
b. Roteamento estático e dinâmico;
c. Tunelamento (“*tunelling*”);

d. NAT – *Network Address Translation*, estático e dinâmico;
e. Gerenciamento via SNMP;
f. HSRP ou equivalente e demais recursos para operação redundante e balanceada;
g. Configuração residente em memória não volátil;
h. Interface para configuração local via console auxiliar, *remote login http* (via browser);
i. Recursos de segurança como filtros de protocolos, controle de tráfego e listas de acesso (baseados em endereços IPs, protocolos e portas, dentre outros);
j. Restrição e controle de acesso (*username* e *password*) para login remoto ou local;
k. Documentação completa em formato PDF, para instalação, configuração e determinação de problemas.

9.38.4 Cada porta de acesso à rede da CONTRATADA deverá ter acesso dedicado com as velocidades descritas nas Tabelas 2 Localidades, Serviço e Velocidades, não podendo ser compartilhada com nenhum outro cliente da CONTRATADA.

9.38.5 Os acessos deverão absorver 100% (cem por cento) do tráfego referente às velocidades contratadas, garantindo o não descarte de pacotes.

9.38.6 A CONTRATADA deve garantir acesso dedicado IP a *web*, de forma segura (considerando os recursos nativos, inerentes ao Serviço Contratado, como por exemplo: https, IPSEC, DNSSEC), estável e eficiente para suportar as mais diversas aplicações, *uploads* e *download*s de dados, além da realização de videoconferências de qualidade e outras trocas de informações.

9.38.7 Os servidores de DNS da CONTRATADA deverão dar suporte à tecnologia DNSSEC (Domain Name System Security Extensions) ou DNS over SSL (Security Socket Layer);

9.38.8 Os serviços descritos nesta parte se referem ao fornecimento de acessos destinados à conexão entre a CONTRATANTE e o *Backbon*e de internet da CONTRATADA. Deverá ser utilizada a tecnologia de fibra óptica, *Gigabit Ethernet*, para garantir a sua escalabilidade, até o limite do circuito adotado.

9.38.9 Os acessos de comunicação com à internet deverão ter as seguintes

características:

9.38.9.1 Fornecer um *range* de, no mínimo, 10 (dez) endereços IP válidos;

9.38.9.2 O *BACKBONE* IP da CONTRATADA deve possuir canais próprios e dedicados de acesso à internet:

9.38.9.2.1 Possuir, no mínimo, 5 (cinco) Gbps de conexão instalada com *Backbone* IP mundial, sem a utilização de redes intermediárias;

9.38.9.2.2 Possuir interligação direta, através de canais dedicados, a pelo menos 2 (dois) outros AS (*Autonomous System*) nacionais. Assim, o *Backbon*e deverá possuir, no mínimo, 2 (dois) PTTs com provedores nacionais e 1 (um) PTT (Ponto de Troca) internacional. As bandas de saída entre os AS (nacional e internacional) deverão somar pelo menos 5 (cinco) Gbps;

A. Sem franquia de tráfego;

B. Os *links* deverão ser simétricos no transporte de dados, permitindo a separação das bandas de *downloa*d e *upload*. Ou seja, os *links* terão respectivamente, 1000 Mbps disponíveis para *upload* e 1000 Mbps para *download*.

9.38.10 O aceite da instalação do serviço de acesso à internet será dado após 30 dias da disponibilidade do serviço para a rede local da CONTRATANTE / Sede PGE/RJ.

9.39 Solução segurança e de SDWAN características gerais do lote 1

9.39.1 A solução NGFW (*Next-Generation Firewall*) com IPS/IDS, **controle de aplicações**, **filtros de conteúdo** e **recursos avançados de segurança**, ***antimalware***, recursos de SD-WAN para os *links* de internet dos lotes 1 e 2, composto por 2 *appliance* físico *on-primess* e licenciamento, *software* para gerenciamento, *logs* e relatórios;

9.39.2 A solução SDWAN, que gerenciará os links de 2Gbps lote 1 e de 1Gbps do lote 2, ambos os concentradores dos lotes 1 e 2, deverá ser composto em alta disponibilidade em HA ativo/ativo por 2 (dois) *appliance* físico *on-primess* licenciamento

9.39.3 A solução SD-WAN gerenciado, especificado no Lote 1 para a REDE EXTERNA deve possuir licenciamento básico para prover, proteção e ser capaz de realizar o balancemanto via SDWAN automatico ou definidio por regras, juntamente com o *link* MPLS do lote 02 e encaminhar o tráfego aos concentradores do lote 1 ou lote 2 na SEDE;

Deverá ser capaz de fornecer à CONTRATANTE todas as informações necessárias

sobre o tráfego detalhado de ambos os links MPLS (Lote 1 e Lote 2), incluindo, no mínimo: gráficos de utilização de banda, detalhamento do tráfego por origem e destino, entre outras métricas relevantes, não se limitando exclusivamente a esses itens, conforme demais especificações previstas neste Termo

9.39.4 O licenciamento do Appliance NGFW e SD-WAN deverá ser padrão a licença de uso do fabricante em caráter permanente e perpétuo para todas as funcionalidades e quantidades mencionadas neste documento, com exceção aos itens relacionados à Atualização de Assinaturas de Proteção.

9.39.4.1 Entende-se por Licença Padrão a licença de uso do fabricante em caráter permanente e perpétuo para todas as funcionalidades e quantidades mencionadas neste documento, com exceção aos itens relacionados à Atualização de Assinaturas de Proteção.

9.39.4.2 Todos os equipamentos NGFW devem possuir esta licença ativada.

9.39.4.3 Entende-se por Licença de Atualização de Segurança a licença de uso do fabricante que permita a utilização das funcionalidades e quantidades mencionadas neste documento para os itens relacionados à Atualização de Assinaturas de Proteção.

9.39.4.4 A licença deve permitir que todas as assinaturas, listas e demais métodos de detecção e prevenção de ameaças e de filtros de conteúdo e aplicação empregados pela solução sejam atualizados até suas últimas versões disponíveis.

9.39.4.5 As Licenças de Atualização de Segurança devem ter prazo de vigência de 60 (sessenta) meses, contados a partir da aplicação destas nos produtos.

9.39.5 *Appliance* físico *firewall* de próxima geração (NGFW) - inclusos: *hardware*, licenciamento, instalação, configuração e garantia por 60 meses;

9.39.6 A serem disponibilizados em 3 (três) diferentes capacidades:

9.39.7 A solução NGFW na Sede TIPO 1 (*Next-Generation Firewall*), como composto por 2 a*ppliance* físico *on-primess* e licenciamento, *software* para gerenciamento, logs e relatórios; dimensionado com *throughput* adequado para suporte o tempo de contrato e sua extensão bem como toda a carga definida nesse termo e deverá possuir as seguintes funcionalidades habilitadas simultaneamente:

9.39.7.1 ***Firewall* de Camada 7 (*Application-Aware*)** Inspeção profunda de pacotes (DPI) para identificar e controlar aplicações independentemente da porta, protocolo ou evasões usadas.

9.39.7.2 **Controle de Aplicações** Permite criar políticas específicas com base em aplicações (ex: permitir *Zoom*, bloquear *BitTorren*t, dentre outros).

9.39.7.3 **Inspeção SSL/TLS (*Decryption*)** Inspeção de tráfego criptografado (HTTPS), com capacidade de descriptografar, analisar e recriptografar o tráfego em tempo real e localmente.

9.39.7.4 **Prevenção de Intrusões (IPS/IDS)** Detecta e bloqueia ameaças conhecidas (assinaturas) e comportamentos suspeitos (heurística/comportamental).

9.39.7.5 **Antivírus/*Antimalware* Integrado** Varredura de arquivos em tempo real e bloqueio de malwares antes que cheguem ao destino.

9.39.7.6 **Filtro de Conteúdo *Web* (*Web Filtering*)** Proxy transparente e criação de regra para acesso a sites com base, em perfis de usuários e grupos do *Active Directory*, IP, Categorias, (ex: redes sociais, pornografia, *phishing*) etc.

9.39.7.7 **Geolocalização de IPs** Criação de regras com base na localização geográfica de IPs (por exemplo, bloquear tráfego vindo de países específicos).

9.39.7.8 **Controle de Usuários e Identidade *(User-ID Integration*)** Integração com serviços de diretório (ex: *Active Directory*) para aplicar regras por usuário ou grupo, e não apenas por IP.

9.39.7.9 **VPN (*Site-to-Site* e *Client-to-Site*)** Estabelecimento de túneis IPsec ou SSL para conexão segura entre sites ou usuários remotos.

9.39.7.10 **ZTNA (Zero Trust Network Access) –** integração com a avaliação de postura de dispositivo (*compliance*, antivírus, atualizações), acesso granular com base em políticas de identidade e aplicação e capacidades de segurança baseadas em identidade, contexto e microsegmentação.

9.39.7.11 ***SandBoxing* / Análise de Ameaças em Nuvem** Execução segura de arquivos suspeitos em ambientes isolados para análise de comportamento (*zero-day protection*).

9.39.7.12 **SD-WAN Integrado** Priorização e roteamento inteligente de tráfego sobre múltiplos links WAN, com base em políticas de desempenho.

9.39.7.13 **Gerenciamento Centralizado e Logs** Interface unificada para gerenciamento de múltiplos dispositivos, auditoria, geração de relatórios e integração com SIEM.

9.39.7.14 **Detecção e Prevenção de *Botnets* e C&C** Identificação de comunicações com servidores de comando e controle (C&C) e redes zumbis.

9.39.7.15 **DNS *Security* / DNS *Filtering*** Monitoramento e controle de requisições DNS

para prevenir conexões com domínios maliciosos, *phishing* ou C&C, impedindo ataques mesmo antes da resolução de nome para IP.

9.39.7.16 ***Zero-day*** Análise Comportamental e Preditiva com a utilização de inteligência artificial e aprendizado de máquina para detecção de anomalias, comportamentos fora do padrão, e ameaças desconhecidas.

9.39.7.17 **QoS / *Traffic Shaping*** Controle de largura de banda e priorização de tráfego por aplicação, serviço ou usuário.

9.39.7.18 **Políticas Baseadas em Tempo (*Time-Based Policies*)** Regras que variam de acordo com o horário (ex: liberar acesso a redes sociais somente fora do expediente).

9.39.7.19 ***Threat Intelligence*** **Integrado** inteligência de ameaças (IoCs, domínios maliciosos, IPs suspeitos) atualizado em tempo real, usado para bloqueio automático.

9.39.7.20 **DLP *(Data Loss Prevention)*** básico integrado.

9.39.7.21 **Segurança em Nuvem (Cloud Security Posture Management / SaaS Control)** Controle de aplicações SaaS (como Google Workspace, Microsoft 365) e visibilidade de tráfego para nuvem.

9.39.7.22 Integração com SIEM – do SNOC

9.39.7.23 **Suporte a IPv6 Completo** Capacidade de inspecionar, aplicar políticas e proteger tráfego IPv6 com o mesmo nível de profundidade que o IPv4.

9.39.7.24 **A solução de SDWAN na Sede TIPO 2** que gerenciará os links MPLS, ambos os concentradores dos lotes 1 e 2, deverá ser composto em alta disponibilidade em HA ativo/ativo por 2 (dois) *appliance* físicos *on-primess*, dimensionado com throughput adequado para suporte o tempo de contrato e sua extensão bem como toda a carga definida nesse termo.

9.39.8 A solução de SDWAN na Rede Externa TIPO 3, possui um *throughput*, menor visto que sua carga foi dimensionada para esse fim.

9.39.8.1 Com vistas à implementação do Plano de *Disaster Recovery* (DR), um único equipamento localizado em uma regional estratégica (a ser definida pela CONTRATANTE) deverá estar dimensionado e licenciado para contemplar, no mínimo, todas as principais funcionalidades descritas para o equipamento do **TIPO 1**, garantindo capacidade de assumir, de forma temporária, o papel da unidade principal em caso de indisponibilidade do Datacenter da SEDE. Funcionalidades NGFW na Sede

TIPO 1: SDWAN, Filtro de Pacotes, IPS/IDS, Filtro Conteúdo (*Web* e Aplicação), **VPN** e Proteção contra *Malwares* habilitadas simultaneamente.

9.39.8.2 Gerenciamento de logs e de relatórios deverá ser centralizada para ambos os lotes, ser preciso for uma console em *Appliance* físico deverá ser fornecido;

9.39.8.3 Deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0 a 40°C.

9.39.8.4 Deve possuir fonte com alimentação bibolt 100~120VAC e 210~230VAC Deve vir acompanhado de cabo de alimentação com Deve vir acompanhado de cabo de alimentação com e PLUG AC TRIPOLAR tipo IEC 320 C14 Macho (para SEDE) e cabos com plug tripolar 2P+T no padrão ABNT NBR 14136 (Rede Externa);

9.39.8.5 Deve possuir, no mínimo, 1 (uma) interface *Ethernet* dedicada para gerenciamento e o plano de gerenciamento da solução deve ser apartado do plano de dados, com recursos de CPU, memória e interface de rede dedicados para esta função;

9.39.8.6 Deve ser fornecido em sua capacidade máxima de processamento, memória e armazenamento interno.

9.39.8.7 Deve ser fornecido em sua capacidade máxima de processamento, memória e armazenamento interno.

9.39.8.8 Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do *hardware* e de performance do equipamento.

9.39.8.9 Deve suportar o envio de notificações via e-mail, SNMP traps e mensagens de log;

9.39.8.10 Deve permitir o acesso ao equipamento via SSH e *interface web* HTTPS.

9.39.8.11 A comunicação entre a estação de trabalho do administrador e o firewall deve ser autenticada e criptografada.

9.39.8.12 Deve informar a utilização dos recursos de CPU, memória e atividade de rede.

9.39.8.13 Deve possuir visualização mínima sumarizada de aplicações, ameaças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização.

9.39.8.14 Deve possuir a funcionalidade de exportação automática dos logs

para servidor *syslog* e para a solução de gerenciamento de logs.

9.39.8.15 Desejável possuir plano de gerenciamento segregado do plano de dados, inclusive com CPU e interfaces dedicadas.

9.39.8.16 Deve permitir a importação, criação e edição de regras SNORT.

9.39.8.17 Deve possuir processamento dedicado no equipamento de segurança para funções e ações de Gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problemas. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP; 1.6. Console de Gerenciamento centralizado.

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

9.39.8.19 Deve suportar os protocolos IPv4 e IPv6.

9.39.8.20 Deve suportar VLAN no padrão 802.1q.

9.39.8.21 Deve suportar *Jumbo Frames*.

9.39.8.22 Deve suportar sub interfaces *Etherne*t lógicas.

9.39.8.23 Deve suportar o protocolo NTP.

9.39.8.24 Deve implementar mecanismo de conversão de endereços NAT (*Network Address Translation*), de forma a possibilitar a realização de NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional (possibilitando que um endereço tenha mais de um NAT dependendo da origem, destino ou porta).

9.39.8.25 Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.

9.39.8.26 Deve suportar tradução de porta (PAT).

9.39.8.27 Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6

9.39.8.28 Deve suportar os protocolos RIP, OSPF v2, OSPF v3 e BGP v4.

9.39.8.29 Deve suportar os protocolos IGMP v2, IGMP v3, PIM-SM;

9.39.8.30 Deve suportar *Virtual Routing Redundancy Protocol* (VRRP) ou

equivalente.

9.39.8.31 Deve suportar os protocolos SNMP v3 e ou NETCONF;

9.39.8.32 Deve permitir monitorar, via SNMP, falhas de *hardware*, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN, CPU, memória, status do *cluster* de Alta Disponibilidade e estatísticas de uso das interfaces de rede.

9.39.8.33 Deve suportar *Policy Based Routing* (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.

9.39.8.34 Deve suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (*Denial of Service*), De-criptografia SSL e SSH, PBF (*Policy Based Forwarding*), QoS, DHCPv6 *Relay*, IPSEc, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, *Neighbor Discovery* (ND), Recursive DNS Server (RDNSS).

9.39.8.35 A CONTRATADA deverá disponibilizar servidores de DNS secundário na função "recursivo", ou seja, ao receberem uma solicitação de qualquer usuário na qual o mesmo não tenha a informação em cache ou não sendo o seu próprio domínio, ele se encarrega em buscar essa informação em outro servidor de DNS;

9.39.8.36 Caso os servidores de DNS da CONTRATADA sejam utilizados como secundário, a CONTRATADA deverá gerenciar a transferência dos registros de zona com o seu servidor de DNS primário da CONTRATANTE. A CONTRATADA também deverá fornecer as informações relativas à compatibilidade entre os seus servidores de DNS primários e os servidores secundários;

9.39.8.37 Deve promover a integração com serviços de diretório LDAP e *Active Directory*, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.

9.39.8.38 Deve identificar de forma transparente os usuários autenticados por meio de serviço de diretório LDAP ou *Active Directory*.

9.39.8.39 Não será permitida a interceptação ou espelhamento do tráfego destinado aos servidores LDAP, *Active Directory* e proxies internos.

9.39.8.40 Não será permitida a utilização de agentes instalados nos servidores LDAP, *Active Directory*, *proxies* internos e equipamentos dos usuários, nem configuração adicional no navegador.

9.39.9 O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP e *Active Directory*.

9.39.10 O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP e *Active Directory*.

9.39.11 Deve registrar a identificação do usuário em todos os *logs* de eventos de acesso ou de ameaças gerados pelo equipamento.

9.39.12 Deve registrar os eventos dos usuários em tempo real, sem a utilização de processos em lote (batches) ou processos de correlação após a ocorrência do evento em questão;

9.39.13 Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.

9.39.14 Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.

9.39.15 Desejável identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do *firewall* o endereço IP, bem como o usuário de rede responsável pelo acesso

9.39.16 Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento;

9.39.17 Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.

9.39.18 Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.

9.39.19 Deve suportar VPN *site-to-site* em topologia *Full Meshed* (todos os gateways possuem links específicos para todos os demais *gateways*) e Estrela (*gateways* satélites se comunicam somente com um único *gateway* central).

9.39.20 Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE *gateway*s e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de *troubleshooting*;

9.39.21 Deve suportar SSL ou IPSec para "*remote access VPN*";

9.39.22 Deve suportar criptografia 3DES, AES-128, AES-256.

9.39.23 Deve suportar integridade de dados com MD5, SHA-1 e SHA-256.

9.39.24 *Diffie-Hellman Group 1, Group 2, Group 5 e Group 14*;

9.39.25 Deve suportar o protocolo IKE, fases I e II.

9.39.26 Deve suportar o protocolo IKE, fases I e II.

9.39.27 Deve suportar Certificado Digital X.509.

9.39.28 Deve suportar NAT-T (NAT Transversal).

9.39.29 Deve permitir a criação de túneis VPN SSL/TLS e IPSec.

9.39.30 Deve suportar VPN IPSec *client-to-site* (acesso remoto).

9.39.31 Deve suportar VPN *Site-to-Site*;

9.39.32 Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP.

9.39.33 Deve suportar autoridade certificadora integrada ao *gateway* VPN ou à solução de gerenciamento centralizado.

9.39.34 Deve promover a integração com diretórios LDAP e *Active Directory* para a autenticação de usuários de VPN e regras de acesso.

9.39.35 Deve suportar os métodos de autenticação de VPN: usuário e senha de base interna do próprio equipamento, usuário e senha de diretório LDAP, usuário e senha do *Active Directory*, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao *Active Directory*, certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil.

9.39.36 Deve suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12.

9.39.37 Deve suportar a solicitação de emissão de certificados a uma autoridade certificadora de confiança (enro lment) via SCEP (*Simple Certificate Enro lment Protocol*) ou CSR (*Certificate Signing Requests*).

9.39.38 Deve suportar a leitura e verificação de CRLs (*Certification Revogation Lists*).

9.39.39 Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL

9.39.40 Deve permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.

9.39.41 Deve suportar a criação de políticas de controle de uso de largura de bandas baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp.

9.39.42 Deve suportar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP.

9.39.43 Deve suportar a marcação de pacotes Dif Serv

9.39.44 Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

9.39.45 Deve implementar balanceamento de *links* utilizando as seguintes métricas e critérios para a escolha do caminho: aplicações, *jitter*, latência e perda de pacotes, permitindo que administradores configurem os valores de tais parâmetros para definir por qual interface certo tipo de tráfego será enviado.

9.39.46 Caso o item acima não seja atendido em sua totalidade, será aceita composição com outro equipamento, do tipo *appliance* físico, desde que a configuração seja realizada através da interface de gerenciamento do firewall e da Solução de Gerenciamento Centralizada, sem nenhum ônus para a Contratante, garantindo o pleno atendimento das métricas e critérios para a escolha do caminho, segundo o item acima.

9.39.47 O appliance físico do item anterior deve possuir throughput igual ou superior à discriminada no throughput das “funcionalidades de Filtro de Pacotes, IPS, Filtro de Conteúdo e Proteção contra *Malwares* habilitadas simultaneamente” do respectivo firewall.

9.39.48 Os valores dos parâmetros *jitter* e latência devem poder ser configurados em unidade mínima de milissegundos (ms).

9.39.49 A interface virtual de balanceamento deve suportar agregar no mínimo 4 (quatro) interfaces, podendo ser do tipo: física, sub interface e VPN.

9.39.50 Deve suportar balanceamento de link por hash do IP de origem e destino.

9.39.51 Deve suportar balanceamento de link por peso. Nesta opção deve ser possível definir o peso de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, 4 (quatro) links WAN.

9.39.52 Deve permitir a configuração de failover entre links principais e secundários, caso os links utilizados ultrapassem os limites previamente definidos de jitter, latência e perda de pacotes. Estes limites podem ser configurados para forçar o failover caso apenas um ou todos os limites sejam atingidos simultaneamente.

9.39.53 Deve suportar a configuração de regras que permita o failback imediato.

9.39.54 Deve ser compatível com a solução de VPN, permitindo que suas características e análises sejam realizadas nas VPNs, assim como em links WAN.

9.39.55 Deve ser compatível com VPNs montadas em interfaces virtuais com roteamento dinâmico.

9.39.56 Deve realizar o gerenciamento de tráfego por tipo de aplicação.

9.39.57 Deve selecionar o melhor caminho baseado em tipo de tráfego e do host de origem.

9.39.58 Deve suportar o monitoramento de link com ping e TCP echo.

9.39.59 Deve suportar o monitoramento de links VPN (interfaces virtuais).

9.39.60 Deve permitir a exportação de informações via netflow.

9.39.61 Deve suportar o funcionamento nos modos snifer (para inspeção de tráfego gerado por uma porta de rede espelhada), layer-2, layer-3, de forma simultânea em uma única instância de firewall

9.39.62 Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas;

9.39.63 Deve possuir capacidade de melhoria e análise das regras atuais, baseadas em camada 3 e 4 (porta/protocolo), indicando como a referida regra deverá ser

configurada em camada 7 (aplicação).

9.39.64 O fluxo de análise de regras legadas deve permitir a visualização de quais aplicações estão em uso. Caso não possua essa funcionalidade, será permitida a integração com ferramentas que executam esta função.

9.39.65 Deve possuir proteção contra ataques, no mínimo, dos tipos: IP Spoofing, Negação de Serviço (DoS e DDoS), SYN Flood Attack, ICMP Flood Attack e UDP Flood Attack, Buffer Overflow, Port Scanning, Man-in-the-Middle .

9.39.66 Deve identificar, decriptografar e analisar o tráfego SSL tanto em conexões de entrada (inbound) quanto de saída (outbound), com suporte a HTTP/2 e TLS 1.2 e 1.3 .

9.39.67 Deve permitir a decriptografia da área útil do pacote de dados (payload) para fins de controle de acesso à Internet e proteção contra ameaças.

9.39.68 Deve possuir funcionalidade de backup e restore da configuração e das políticas de segurança através do carregamento de arquivo de configuração previamente salvo.

9.39.69 Deve armazenar os backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos por meio dos protocolos FTP ou SCP.

9.39.70 Deve possuir a capacidade de identificar ataques de Advanced Persistent Threat (APT) ou Zero-Day.

9.39.71 Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (Sandbox), na nuvem do fabricante, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema, entre outros.

9.39.72 Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrado.

9.39.73 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos;

9.39.74 Deve sincronizar as assinaturas de IPS quando implementado em alta disponibilidade ativo/ativo ou ativo/passivo;

9.39.75 Deve implementar os seguintes tipos de ações para ameaças detectadas

pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo

9.39.76 Deve permitir ativar, desativar e habilitar apenas em modo de monitoração as assinaturas de prevenção contra invasão;

9.39.77 Exceções por IP de origem ou de destino devem ser possíveis nas regras e assinatura a assinatura;

9.39.78 Deve suportar controles por zona de segurança;

9.39.79 Deve suportar controles de políticas por porta e protocolo;

9.39.80 Deve suportar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

9.39.81 Deve suportar controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

9.39.81.1 Deve suportar controle, inspeção e decriptografia de SSL por política para tráfego de entrada (inbound) e Saída (outbound);

9.39.81.2 Deve suportar offload de certificado em inspeção de conexões SSL de entrada (inbound);

9.39.81.3 Deve decriptografar tráfego inbound e outbound em conexões negociadas com TLS 1.2 e superior;

9.39.82 Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, bin, zip, tar e mp3;

9.39.83 Suporte a objetos e regras multicast;

9.39.84 Deve suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens:

9.39.85 Deve suportar operação em ambientes configurados para alta disponibilidade;

9.39.86 Deve suportar a monitoração, detecção e prevenção, em tempo real, de arquivos trafegados nos seguintes protocolos: FTP, HTTP, SMTP, IMAP, POP3, como também arquivos trafegados internamente entre servidores de arquivos usando SMB, em todos os modos de implementação: transparente e L3;

9.39.87 Deve permitir especificar o tipo de arquivo, inclusive os comprimidos,

que serão analisados em cada política de controle de malware, permitindo especificar um contexto de análise para redes, VLANs e outros objetos associados ao controle de acesso do ambiente protegido;

9.39.88 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, Microsoft Active Directory e base de dados local;

9.39.89 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

9.39.90 Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Microsoft Windows Server 2019 e versões superiores;

9.39.91 Deve possuir integração com LDAP para identificação de usuários e grupos, permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;

9.39.92 Deve suportar a implementação tanto em modo transparente (layer-2) quanto em modo gateway (layer-3);

9.39.93 Deve suportar Statefull Packet Inspection de tráfego IPv4 e IPv6;

9.39.94 Deve suportar controle de acesso para serviços e protocolos pré-definidos, bem como possibilitar a adição de novos serviços e protocolos;

9.39.95 Deve suportar os protocolos H.323, SIP;

9.39.96 Deve implementar mecanismo de proteção contra ataques de falsificação de endereços IP (anti-spoofing);

9.39.97 Deve implementar mecanismo de captura de pacotes, de forma manual ou automática, quando uma ameaça for detectada;

9.39.98 Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP, UDP e ICMP

9.39.99 Deve suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6;

9.39.100 Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM,

horário ou período de tempo, e suas combinações;

9.39.101 Deve suportar a consulta a fontes externas de endereços IP, domínios e URL's podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;

9.39.102 Desejável possuir mecanismos de otimização de regras. De forma que com base na análise de tráfego o sistema automaticamente faça sugestões e melhorias nas regras existentes;

9.39.103 Deve classificar as aplicações em categorias;

9.39.104 Deve permitir o agrupamento de aplicações em grupos personalizados;

9.39.105 Deve identificar os usuários que estão utilizando as aplicações;

9.39.106 Deve permitir o bloqueio de aplicações que não estejam utili;ando suas portas padrão;

9.39.107 Deve suportar a implementação de políticas de segurança baseadas em: aplicações, categorias de aplicações, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações;

9.39.108 Deve identificar os usuários relacionados aos eventos de intrusão;

9.39.109 Deve identificar os usuários relacionados aos eventos de bloqueio;

9.39.110 Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça;

9.39.111 Deve permitir a criação de políticas de segurança que bloqueiem uma determinada ameaça;

9.39.112 Deve permitir a criação de políticas de segurança que bloqueiem um determinado ataque por meio de uma ação de DROP/RESET;

9.39.113 Deve permitir a criação de políticas de segurança que bloqueiem um determinado ataque por meio de uma ação de DROP/RESET;

9.39.114 Console de Gerenciamento Centralizado LOTE 1

9.39.114.1

Deve ser fornecida em appliance virtual, compatível VMware vSphere ESXi 7.0 ou superior, ou baseado em software, compatível com Windows Server 2019 ou superior,

ou em appliance físico com suporte à fixação em bastidor (rack) com largura de 19’ (dezenove polegadas) e altura de até duas unidades de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

9.39.114.2Características físicas:

9.39.114.2.1 Capacidade mínima de armazenamento de 900 GB;

9.39.114.2.2 Suportar no mínimo 5.000 (cinco mil) logs/flows por segundo;

9.39.114.2.3 Possuir no mínimo duas interfaces de rede Ethernet 1 (um) GbE ;

9.39.114.3Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux.

9.39.114.4Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.

9.39.114.5Deve permitir o gerenciamento centralizado dos equipamentos de firewall sejam eles virtuais ou físicos em uma mesma console, permitindo os seguintes requisitos:

9.39.114.5.1.1.1 Coleta de logs;

9.39.114.5.1.1.2 Análise de logs;

9.39.114.5.1.1.3 Gerenciamento de firewalls;

9.39.114.5.1.1.4 Correlação de logs.

9.39.114.6Deve estar licenciada e permitir a gerência centralizada de, no mínimo, 16 equipamentos.

9.39.114.7Deve estar licenciada para o limite máximo de usuários, objetos, regras de segurança, NAT e endereços IP suportados pela solução.

9.39.114.8As comunicações entre Console de Gerenciamento Centralizado e os firewalls rede externa e entre a Console de Gerenciamento Centralizado e as estações dos administradores do sistema devem ser criptografadas e autenticadas

9.39.114.9Deve ser capaz de realizar todas as configurações nos firewalls descritas nesta ata

9.39.114.10 Deve possibilitar a aplicação simultânea de configurações em todos os firewalls gerenciados pela solução.

9.39.114.11 Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.

9.39.114.12 Deve suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas de filtro de pacotes, prevenção de intrusão, controle de aplicação, filtragem de URLs, monitoração de logs, debugging, troubleshooting e captura de pacotes.

9.39.114.13 Deve ser capaz de gerenciar os firewa ls em unidades remotas, fora da rede local.

9.39.114.14 Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory

9.39.114.15 Será permitido que a solução de gerenciamento centralizado possua um “appliance virtual” específico para atendimento às necessidades de identificação e autenticação de usuários

9.39.114.16 Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura

9.39.114.17 Deve possuir licenciamento válido, garantia e suporte técnico do fabricante por no mínimo o período de vigência contratual, com possibilidade de renovação por igual período;

9.39.114.18 As funcionalidades de gerência e retenção de logs que compõem a plataforma de segurança podem funcionar em múltiplos appliances, desde que obedeçam a todos os requisitos desta especificação;

9.39.114.19 Deve centralizar logs e relatórios usando uma única interface de gerenciamento;

9.39.114.20 O gerenciamento da solução deve suportar acesso via SSH, WEB (HTTPS) e API aberta;

9.39.114.21 O armazenamento poderá ser realizado através de composição com solução de terceiros, como por exemplo, SIEM (Security Information and Event Management);

9.39.114.22 Não será permitida a instalação de cliente para administração do appliance de firewall;

9.39.114.23 Visualização de logs e relatórios relacionados às políticas de firewall e controle de aplicação;

9.39.114.24 Visualização de logs e relatórios relacionados ao IPS, Controle de

Aplicação e Anti-Malware;

9.39.114.25 Visualização de logs e relatórios relacionados às políticas de Filtro de URL;

9.39.114.26 Monitoração de logs;

9.39.114.27 Ferramentas de investigação de logs;

9.39.114.28 Visualização das capturas de pacotes realizadas nos ataques detectados;

9.39.114.29 Acesso concorrente de administradores;

9.39.114.30 Deve possibilitar a geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

9.39.114.31 Deve ter capacidade de gerar relatórios gráficos que permitam visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, permitindo comparar os diferentes consumos realizados pelas aplicações no decorrer do tempo;

9.39.114.32 Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spyware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

9.39.114.33 Deve permitir a criação de painéis (dashboards) ou relatórios customizados com, no mínimo, as seguintes informações: visibilidade do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, malware detectado, aplicações mais utilizadas, protocolos mais utilizados, principais atacantes (com informação de geolocalização);

9.39.114.34 Deve possibilitar a coleta de estatísticas de todo o tráfego associado aos dispositivos de segurança;

9.39.114.35 Deve permitir a criação de perfis customizados;

9.39.114.36 Deve permitir, de forma granular, assinalar permissões para os dministradores criarem outros usuários, alterarem e ler configurações, entre outros;

9.39.114.37 Deve permitir múltiplos administradores acessando o equipamento simultaneamente, sem restrição para leitura e escrita;

9.39.114.38 Deve suportar o bloqueio de alterações, evitando o conflito de

configurações entre diferentes administradores efetuando alterações simultaneamente;

9.39.114.39 Deve registrar, em log de auditoria, as ações dos usuários administradores com o horário da alteração;

9.39.114.40 Deve suportar a identificação e utilização de usuários nas políticas de segurança;

9.39.114.41 Deve suportar agrupamento lógico de objetos ("object grouping") para criação de regras;

9.39.114.42 Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deve ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas;

9.39.114.43 Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

9.39.114.44 Deve garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e atualização remota, de maneira centralizada;

9.39.114.45 Deve ser capaz de testar a conectividade dos equipamentos gerenciados;

9.39.114.46 Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos;

9.39.114.47 Deve permitir localizar em quais regras um objeto está sendo utilizado;

9.39.114.48 Deve permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico);

9.39.114.49 Deve suportar a geração de alertas automáticos via SNMP e syslog;

9.39.114.50 Deve informar a utilização dos recursos de CPU, memória e atividade de rede dos equipamentos gerenciados;

9.39.114.51 Deve informar o número de conexões simultâneas dos equipamentos gerenciados;

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

9.39.114.53 As consoles de gerenciamento centralizado, gerenciamento de logs, relatoria centralizada, poderão ser entregues em um único appliance, desde que atenda a todas as exigências deste documento;

9.39.115 Gerenciamento de Logs LOTE 1

9.39.115.1 Deve ser fornecida em appliance virtual, compatível VMware vSphere ESXi 7.0 ou superior, ou baseado em software, compatível com Windows Server 2019 ou superior, ou em appliance físico com suporte à fixação em bastidor (rack) com largura de 19’ (dezenove polegadas) e altura de até duas unidades de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

9.39.115.2 Deve possuir relatórios de utilização dos recursos por aplicação, URLs, ameaças e etc.

9.39.115.3 Deve possuir visualização sumarizada de todas as aplicações, ameaças e URLs que foram identificadas e controladas pela solução.

9.39.115.4 Deve permitir a criação de relatórios customizados

9.39.115.5 Deve ser capaz de receber logs de todos os firewalls especificados neste termo;

9.39.115.6 Retenção mínima de 12 meses dos logs, gráficos e relatórios de todo o tráfego de rede pela console de gerenciamento ou específica para logs.

9.39.115.7 Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário

9.39.115.8 Deve possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando: endereços IP de origem e destino dos pacotes, traduções NAT, portas e protocolos de origem e destino, usuário identificado, ação sobre o pacote (permitido ou negado).

9.39.115.9 Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços; os mais frequentes ataques e ameaças de segurança detectados com suas origens e destinos; os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de

Internet; os usuários maiores consumidores de banda de Internet; e os sítios na Internet mais visitados

9.39.115.10 Deve possuir funcionalidade de exportação de relatórios e logs para o computador local ou via FTP, SFTP ou SCP.

9.39.115.11 Deve permitir a geração automática e agendada dos relatórios.

9.39.115.12 Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução.

9.39.115.13 O appliance virtual deve estar licenciado de maneira irrestrita quanto ao armazenamento, possibilitando que órgão armazenar o volume de logs que julgar necessário, utilizando recursos computacionais próprios

9.39.115.14 Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux

9.39.115.15 Será permitida a entrega do "Console de Gerenciamento de Logs" como software agregado ao "Console de Gerenciamento Centralizado" ou ao "Console de Relatórios Centralizada".

9.39.115.16 Backup das configurações e rollback de configuração para a última configuração salva;

9.39.115.17 Visualização e comparação de configurações atuais, configuração anterior e configurações antigas.

9.39.115.18 Mecanismo de validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras;

9.39.115.19 Deve gerar alertas automáticos via Emai, SNMP;;

9.39.116 Relatórios Centralizados

9.39.116.1 Deve ser fornecida em appliance virtual, compatível com VMware vSphere ESXi 6.5 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior.

9.39.116.2 Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou no Linux.

9.39.116.3 Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas

9.39.116.4 Deve estar licenciada e permitir a gerência centralizada de relatórios, para no mínimo, 16 equipamentos.

9.39.116.5 As comunicações entre a Console de Relatórios e os firewalls e entre a Console de Relatórios e as estações dos administradores do sistema devem ser criptografadas e autenticadas

9.39.116.6 Deve ser capaz de gerar relatórios de equipamentos em unidades remotas, fora da rede local.

9.39.116.7 Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory

9.39.116.8 A console deve suportar acesso via SSH, cliente e WEB (HTTPS).

9.39.116.9 Deve coletar logs dos Firewalls, do "Console de Gerenciamento Centralizado" e do "Console de Gerenciamento de Logs"

9.39.116.10 Deve garantir a geração de relatórios com mapas geográficos, ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego

9.39.116.11 Deve permitir a extração de relatórios.

9.39.116.12 Deve possuir relatórios pré-definidos.

9.39.116.13 Deve permitir a geração de relatórios de logs de tráfego de dados.

9.39.116.14 Deve permitir a geração de relatórios de logs para auditoria das configurações de regras, objetos e acessos.

9.39.116.15 Deve possibilitar o envio de maneira automática de relatórios por e-mail.

9.39.116.16 Deve permitir o agendamento da geração de relatórios.

9.39.116.17 Deve ter a capacidade de definir filtros nos relatórios.

9.39.116.18 Deve gerar alertas automáticos via e-mail, snmp e syslog baseados em eventos de ocorrência como log, severidade de log, entre outros.

9.39.116.19 Deve permitir a criação de painéis (dashboards) customizados para visibilidades do tráfego de aplicativos, categorias de url, ameaças, serviços, países, origem e destino.

9.39.116.20 Deve possibilitar a visualização na interface gráfica de usuário (gui) da "console de relatoria centralizada as seguintes informações do sistema: logs diários recebidos, alertas gerados, entre outros.

9.39.116.21 Será permitida a entrega do "Console de Relatoria Centralizada" como software agregado ao "Console de Gerenciamento Centralizado" ou ao "Console de Gerenciamento de Logs".

9.39.117 LOTE 1 - Características Específicas Solução de proteção NGFW a ser fornecida pelo MSS

FIREWALL TIPO 1 - SEDE

9.39.117.1 Throughput de 09 Gbps 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. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

9.39.117.2 A solução na Sede deverá ser disponibilizada em HA alta disponibilidade em Cluster **ATIVO-ATIVO**.

9.39.117.3 O HA (modo de alta disponibilidade) deve possibilitar monitoração de falha de link;

9.39.117.4 A configuração em alta disponibilidade deve possibilitar a instalação de cada membro do cluster, de forma que o sincronismo de sessões e configurações deve ocorrer sobre a camada 3 (IP);

9.39.117.5 Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 19 Gbps.

9.39.117.6 Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 9 Gbps

9.39.117.7 Deve permitir, no mínimo, 1.900.000 conexões simultâneas

9.39.117.8 Deve permitir, no mínimo, 200.000 novas conexões por segundo

9.39.117.9 Deve permitir, no mínimo, 4000 VLANs.

9.39.117.10 Deve permitir, e estar licenciado para a utilização de 2000 túneis VPN site-to-site simultâneos.

9.39.117.11 Deve permitir, e estar licenciado para a utilização de 1800 túneis VPN client-to-site simultâneos.

9.39.117.12 Deve suportar a fixação em bastidor (rack) padrão 19' (dezenove

polegadas) e altura de no máximo três unidades de rack (3U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

9.39.117.13 O appliance deve possuir, no mínimo, 10 (dez) portas 100/1000/10000 BASE-T E/ou SFP podendo ser uma composição entre os dois tipos, acompanhadas de seus respectivos transceivers.

9.39.117.14 Deve possuir, no mínimo, 4 (quatro) interfaces 10 (dez) Gigabit-Ethernet padrão SFP+, com transceivers SFP+ 10GB- SR, para conexão ao meio via cabo de fibra ótica.

9.39.117.15 Deve possuir, disco Solid State Drive (SSD) ou cartão eMMC de, no mínimo, 480GB cada disco.

9.39.117.16 Deve possuir, no mínimo, 5 (cinco) interfaces 1 (um) Gigabit-Ethernet padrão SFP, para conexão ao meio via cabo de fibra ótica.

9.39.118 LOTE 1 - Características Específicas da solução de SD-WAN (concentradora rede principal lote 1 em alta disponibilidade ativo/ativo).

FIREWALL TIPO 2 - SEDE

9.39.118.1 A solução na Sede deverá ser disponibilizada em HA alta disponibilidade em Cluster **ATIVO-ATIVO**.

9.39.118.2 O HA (modo de alta disponibilidade) deve possibilitar monitoração de falha de link;

9.39.118.3 A configuração em alta disponibilidade deve possibilitar a instalação de cada membro do cluster, de forma que o sincronismo de sessões e configurações deve ocorrer sobre a camada 3 (IP);

9.39.118.4 Firewall Throughput 7.5 Gbps

9.39.118.5Aceitar 30.000 Novas sessões por segundo

9.39.118.6 Aceitar 2milhoes de sessões concorrentes

9.39.118.7 Aceitar Throughput de IPS de 500 Mbps

9.39.118.8Throughput de NGFW de 360 Mbps

9.39.118.9 Em relação ao túnel IPSec VPN, SDWAN, deve possuir o throughput mínimo de 4 Gbps

9.39.118.10 Threat Protection Throughput 250 Mbps

9.39.118.11 Throughput SSL-VPN 250 Mbps

9.39.118.12 Deve suportar a fixação em bastidor (rack) padrão 19’ (dezenove polegadas) e altura de no máximo três unidades de rack (3U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

9.39.118.13 O appliance deve possuir, no mínimo, 4 (dez) portas 1 Gigabit BASE-T E/ou SFP podendo ser uma composição entre os dois tipos, acompanhadas de seus respectivos transceivers.

9.39.118.14 Deve possuir, 1 disco Solid State Drive (SSD) no mínimo, 480GB

9.39.119 LOTE 1 Características Específicas Solução SDWAN REDE EXTERNA

FIREWALL REDE EXTERNA – TIPO 3

9.39.119.1 Throughput de 2 Gbps 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. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

9.39.119.2 Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 4 Gbps.

9.39.119.3 Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 3 Gbps.

9.39.119.4 Deve permitir, no mínimo, 700.000 conexões simultâneas

9.39.119.5 Deve permitir, no mínimo, 35.000 novas conexões por segundo

9.39.119.6 Deve permitir, no mínimo, 4000 VLANs.

9.39.119.7 Deve permitir, e estar licenciado para utilização de 2000 túneis VPN site-to-site simultâneos

9.39.119.8 Deve permitir, e estar licenciado para utilização de 1500 túneis VPN client-to-site simultâneos.

9.39.119.9 Deve suportar a fixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de no máximo uma unidade de rack (1U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços,

trilhos etc).

9.39.119.10 O appliance deve possuir, no mínimo, 03 (três) portas de rede 1G RJ-45.

9.39.119.11 O appliance deve possuir uma porta 10/100/1000 para gerenciamento “out-of-band”.

9.39.119.12 Deve possuir, disco Solid State Drive (SSD) ou cartão eMMC de, no mínimo, 128GB.

9.40 O Serviço de Segurança Gerenciada (MSS) tem por objetivo ofertar uma camada de segurança para a toda Rede de acordo com as especificações do Termo de Referência

A CONTRATADA deverá prover suporte assistido de Gerência de Rede e Segurança em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias do ano,

Algumas atividades relacionadas à segurança da informação são de responsabilidade, tais como, mas não se limitando a:

9.40.1 Prevenção de ataques cibernéticos;

9.40.1.1 Detecção de riscos, vulnerabilidades e ameaças à rede da CONTRATANTE;

9.40.1.2 Oferecer resposta rápida contra incidentes de segurança detectados;

9.40.1.3 Realizar o gerenciamento de toda a solução de SDWAN/Firewall para proteção dos circuitos, administrando e configurando-o de forma a minimizar os incidentes de Segurança;

9.40.2 Prestar todo o suporte necessário para a operacionalidade das atividades, auxiliando os tomadores de decisões a fazer escolhas conscientes,

9.40.3 O Serviço de Segurança Gerenciada deve contemplar a monitoração proativa do (s) dispositivo (s) de segurança ofertado (s), pela CONTRATADA;

9.40.4 Implementar novas regras nos equipamentos de segurança da solução ofertada pela CONTRATADA e deverá contemplar, em conformidade com o solicitado pela CONTRATANTE;

9.40.4.1 Análise e supervisão dos eventos de segurança;

9.40.4.2 Detecção de alertas de segurança;

9.40.4.3 Gestão e a resposta a incidentes de segurança;

9.40.5 Periodicamente sugerir alterações nas regras dos equipamentos de segurança, visando melhorar a proteção da rede

9.40.6 A CONTRATANTE deverá ter acesso irrestrito os appliances da solução de segurança de forma a realizar a correta fiscalização técnica dos serviços;

9.40.7 Criação e administração de políticas de IPS/IDS;

9.40.8 Criação e administração de políticas de firewall;

9.40.9 Monitoração de logs.

9.40.10 Atuar pro ativamente para solucionar possíveis problemas e incidentes de segurança;

9.40.11 A solução de segurança deverá atender aos seguintes Níveis de Serviços:

9.40.11.1 Prioridade N1: Indisponibilidade de componentes críticos do serviço, criação e alteração de regras: no máximo em até 1 horas;

9.40.11.2 Prioridade N2: Indisponibilidade parcial módulos ou componentes críticos do serviço: no máximo em até 4 horas;

9.40.11.3 . Prioridade N3: Indisponibilidade de componentes não críticos do serviço: no máximo em até 8 horas;

9.40.11.4 Prioridade N4: Indisponibilidade parcial módulos ou componentes não críticos do Serviço: no máximo em até 24 horas;

9.40.11.5 Prioridade N5: Requisições de logs, relatórios ou alteração de configurações e mudanças que não impactam na disponibilidade do ambiente: no máximo em até 48 horas.

9.40.11.6 Requisições que se enquadrem em tipo de projeto, o prazo será acordado com a CONTRATANTE;

9.40.12 A entrega dos relatórios mensais é condição necessária à atestação dos serviços, pelo CONTRATANTE, de acordo com o descrito no item 10;

10. DOS SERVIÇOS ESPECIALIZADOS DE MANUTENÇÃO E SUPORTE TÉCNICO

10.1 A assistência técnica corretiva será realizada sempre que solicitada pela CONTRATANTE por meio de abertura de chamado técnico, acionando diretamente a CONTRATADA, observando o tempo de início do atendimento e a severidade da ocorrência prevista na tabela própria dos níveis de serviços contratados, descritos neste instrumento.

10.2 A resolução de chamados de Suporte Técnico que necessitem intervenção direta nos ambientes da CONTRATANTE deverá ser precedida de planejamento e somente poderá ser implementada no ambiente, fora do horário de produção e após avaliação do impacto.

10.3 Nos atendimentos aos chamados técnicos abertos, deverá ser disponibilizado suporte técnico personalizado por um analista designado como especialista no *software*, via atendimento de suporte remoto.

10.4 Suporte especializado deverá atender os seguintes requisitos técnicos:

10.4.1 Permitir a abertura, acompanhamento e validação de chamados através de e-mail e/ou website (portal do cliente) e/ou telefone (0800) no regime 24x7x365, com atendimento em português;

10.4.2 Possuir processo de escalação funcional, mapeamento e documentação, com os seguintes níveis de atendimento: N1, N2 e N3, conforme melhores práticas descritas pelo ITIL;

10.4.3 Os prazos de atendimento da solução devem ter como referência os níveis de severidade, todos informados na tabela abaixo, ficando a contratada sujeita às sanções previstas na lei em caso de descumprimento contratual.

Tabela de Severidades dos Chamados e Prazos de Atendimento / Solução			
Severidade	**Descrição**	**Tempo de 1º contato após abertura do chamado**	**Tempo de Solução**
Urgente	Objeto totalmente inoperante	15 minutos	até 2 horas
Importante	Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução	até 1 hora	até 4 horas
Normal	Solução não inoperante, mas com problema de funcionamento – Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução	até 2 horas	até 24 horas

Informação	Solicitações de informações diversas ou dúvidas sobre a solução	até 8 horas	até 48 horas

10.4.4 A severidade do chamado poderá ser reavaliada quando verificado que a mesma foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução.

10.4.5 A cada abertura de chamado CONTRATADA poderá solicitar a prorrogação de quaisquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado. Caberá à CONTRATANTE aceitar ou não o pedido de prorrogação do prazo.

10.4.6 Possuir canal com os fabricantes envolvidos na solução dos incidentes, bem como ser responsável pela abertura e acompanhamento dos chamados junto aos mesmos;

10.4.7 Possuir os processos de gerenciamento de incidentes, requisição, eventos, problemas, mudanças, incidentes críticos e atendimento aos usuários VIPs mapeados e documentados de acordo com as melhores práticas descritas pelo ITIL;

10.4.8 Assegurar o atendimento presencial previamente acordado nas seguintes situações:

- Migração de versionamento dos equipamentos gerenciados;
- Modernização dos equipamentos gerenciados;
- Incidentes massivos ou desastres;
- Inacessibilidade, ocasionado pela CONTRATADA, dos equipamentos gerenciados.

10.4.9 Suporte técnico de 2º nível quanto a dúvidas de customização e configuração do equipamento e console de gerenciamento.

10.4.10 A Manutenção Preventiva deverá atender os seguintes requisitos técnicos:

10.4.10.1 Atualizar os *firmwares* e/ou *softwares* das soluções que compõem a solução e das respectivas consoles de gerenciamento;

10.4.10.2 Realizar os ajustes e melhorias constantes, de acordo com as melhores práticas dos fabricantes; mantê-las documentadas e acessíveis no website (portal do cliente);

10.4.10.3 Propor melhorias no ambiente de forma proativa, periodicamente; mantê-las documentadas no website (portal do cliente) e submetê- las para a aprovação da CONTRATANTE;

10.4.10.4 Realizar procedimentos, com base em rotinas pré-definidas, de operações de teste de restauração, no mínimo, semanal.

10.5 Na abertura de chamados técnicos serão fornecidas informações pela CONTRATANTE, como:

10.5.1.1 Anormalidade observada;

10.5.1.2 Nome do responsável pela solicitação do serviço;

10.5.1.3 Sistema/versão/módulo/item;

10.5.1.4 Natureza do problema;

10.5.1.5 Descrição da natureza enfrentada;

10.5.1.6 Severidade do chamado, a ser definida conforme tabela própria dos níveis de serviços contratados, descritos neste instrumento.

10.6 O atendimento técnico deverá atender os seguintes requisitos técnicos:

10.6.1 As solicitações de serviço, sejam de suporte ou consultoria, só poderão ser realizadas pelos contatos cadastrados, através dos métodos abaixo, em qualquer horário:

1. E-mail;
2. Telefone;
3. Horário de Atendimento:

a. O atendimento remoto de Suporte e Monitoramento pelos canais: telefônico ou *web* ou e-mail, irá funcionar em regime 24 horas por dia, 7 dias por semana e 365 dias do ano (24x7x365) para incidentes e solicitações elegíveis de se resolver remotamente;

b. O atendimento presencial de Suporte de incidentes e solicitações elegíveis de se resolver presencialmente irá funcionar, preferencialmente, no horário comercial de 9:00h às 18:00h. Exceto quando o suporte for emergencial, ou ações que irão demandar possível parada técnica, como, por exemplo (upgrade de versões). Nestes casos, o atendimento deverá ser fora do horário comercial em regime 24x7x365.

10.6.2 A CONTRATADA, deverá apresentar os Relatórios Mensais que deverão ser entregues até o 5° (quinto) dia útil do mês subsequente, contendo:

A. Identificação do chamado;

B. Data e hora do início e término do atendimento

C. Atividades executadas

D. Solução do chamado técnico;

E. Identificação do defeito;

F. Técnico responsável pela solução do defeito, as providências

adotadas, origem do problema e outras informações pertinentes;

G. Atualizações de software/versão realizadas;

H. Acionamentos feitos à equipe da CONTRATADA;

I. Relatórios Extraordinários.

10.6.3 Após o envio do relatório, a CONTRATADA deverá solicitar à Comissão de Fiscalização do Contrato o ateste do mesmo. Esta será responsável pela análise e o aceite do pedido ou deverá rejeitar e emitir relatório de não conformidade, que deve constar pelo menos as pendências a serem resolvidas pela CONTRATADA.

11 PLANEJAMENTO, FORNECIMENTO DOS SERVIÇOS

11.1 A execução do objeto será iniciada a partir da data designada no Memorando de Início de Serviços, o qual autoriza a CONTRATADA a seguir e cumprir o cronograma de atividades definido na tabela abaixo.

11.2 A CONTRATADA deverá garantir a qualidade e a estabilidade dos serviços prestados em todas as etapas utilizando as melhores práticas de mercado, de tal forma que a CONTRATANTE tenha uma solução viável do ponto de vista técnico com alto grau de segurança, escalabilidade, usabilidade edesempenho.

11.3 Para a execução dos serviços especializados a CONTRATADA entregará, para validação da CONTRATANTE, um Plano de Trabalho para elaboração do Plano de Projeto (Modelo Anexo) e, ainda, os descritos abaixo que devem estar integrados em uma única documentação técnica:

11.3.1 LOTE 1:

11.3.1.1 **Projeto de Configuração, Customização e Parametrização:** Elaboração da documentação necessária à correta configuração e parametrização dos roteadores, *switche*s, sistema de gerenciamento, etc. para garantir a correta operação e funcionalidade da solução de segurança de conectividade no ambiente tecnológico da PGE-RJ. Neste projeto deve prever, ainda, a migração de todas as rotas e regras de acesso existentes e em uso nos ativos de rede de computadores da PGE, que se fizerem necessárias para garantir a segurança lógica e a disponibilidade do ambiente computacional da PGE-RJ.

11.3.2 LOTE 1 e 2:

11.3.2.1 **Plano de Integração dos Serviços** – neste documento deverá constar, no mínimo, a arquitetura desenhada pela CONTRATADA para a integração dos serviços, na estrutura existente na CONTRATANTE, relativamente aos itens que forem

pertinentes: rede TCP/IP, balanceamento de carga, gerenciamento centralizado da solução, segurança, controle de banda e de acesso.

11.3.3 LOTE 1 e 2:

11.3.3.1 **Levantamento de Dados/Vistoria:** coleta dos dados necessários à elaboração do Planejamento e execução dos serviços, através de reuniões entre profissionais e especialistas, da CONTRATANTE e da CONTRATADA, bem como de vistorias e levantamentos em campo, visando complementar os dados fornecidos pela CONTRATANTE;

11.3.3.2 **Plano de Teste:** tem como finalidade estabelecer os procedimentos para aceitação em campo das adequações, migrações de rotas e regras de acesso, configurações e parametrizações efetuadas pela CONTRATADA, verificando o correto funcionamento dos equipamentos e serviços implantados. Este Plano deverá definir os seguintes aspectos, dentre outros: a forma de atuação das áreas de implantação e de operações; descrição dos testes a serem realizados e respectivos procedimentos de execução; critérios para a avaliação dos resultados.

11.3.3.3 Poderão ser solicitados, a qualquer momento, durante o contrato, testes de failover, desde que previamente agendados em data e horário definidos em conjunto com a equipe técnica da CONTRATADA. Esses testes deverão ser realizados em todos os equipamentos que operam em regime de Alta Disponibilidade (HA), incluindo os links de Internet da SEDE, o concentrador SD-WAN e os dispositivos SD-WAN da rede externa. Será exigida a comprovação de que o tráfego foi redirecionado automaticamente para o link secundário. Ao final dos testes, deverá ser elaborado e entregue um relatório completo contendo os resultados obtidos.

11.3.3.4 Durante todo o contrato e principalmente na fase de aceitação, deverá ser realizado testes de throughput em condições de pico. Os testes deverão incluir, obrigatoriamente, a geração prática de tráfego próximo a 100% da largura de banda contratada, sustentado por um período mínimo de 1 hora (uma hora) contínuas, com jitter ≤ 10 ms e perda de pacotes (packet loss) ≤ 0,1%. Ao final dos testes, deverá ser elaborado e entregue um relatório completo contendo os resultados obtidos, comprovando largura de banda contratada.

11.3.3.5 **Projeto de Adequação da Infraestrutura:** elaboração da documentação necessária à adaptação das instalações existentes, visando à instalação dos novos equipamentos, como cabeamento específico (se necessário), remanejamento de cabeamento (se necessário), instalação elétrica etc. Pela especificidade, as adaptações na

rede elétrica serão de responsabilidade da CONTRATANTE, exceto o fornecimento e instalação da tomada elétrica específico para conectar os equipamentos de rede da CONTRATADA;

11.3.3.6 Plano de *Disaster Recove*ry (DR) para Infraestrutura de Rede:

11.3.3.6.1 Deverá ser criado, testado e documentado um fluxo de *Disaster Recovery* que contemple, no mínimo, cenário de Perda total do Datacenter da SEDE

11.3.3.6.2 Neste caso, a arquitetura de contingência deverá prever a utilização de uma regional estratégica (a ser definida) como ponto de *fallback*, utilizando os recursos disponíveis no ambiente de SD-WAN e no NGFW (*Next-Generation Firewall*), com as seguintes capacidades:

11.3.3.6.3 Conectividade com o PRODERJ: via VPN estabelecida entre o NGFW da regional e o ambiente do PRODERJ, garantindo acesso à base da Dívida Ativa;

11.3.3.6.4 Acesso à Internet: utilizando a conectividade do PRODERJ como rota de saída para internet, em caráter emergencial;

11.3.3.6.5 Interligação com outras regionais: por meio dos links das operadoras contratadas nos Lotes 1 e 2, garantindo continuidade de comunicação entre as unidades descentralizadas.

11.3.3.6.6 Todo o plano deverá conter diagramas, fluxos operacionais e procedimentos de ativação e retorno ao estado original (*rollback*), além de ser testado e validado periodicamente, conforme cronograma acordado com a CONTRATANTE.

11.4 A CONTRATADA deverá utilizar, no mínimo, a seguinte mão de obra especializada como a Equipe de Trabalho:

11.4.1 01 (um) profissional sênior de nível superior com especialização na solução proposta pela CONTRATADA.

11.4.2 01 (um) profissional sênior de nível superior com especialização em gerência de projetos.

11.4.3 A CONTRATADA deverá comprovar a especialização de seus profissionais mediante a apresentação de cursos e certificados de especialização que teve aproveitamento.

11.5 A equipe técnica da CONTRATADA que irá executar a instalação deverá trabalhar sob a orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação (Gerente de Projeto) e com acompanhamento do profissional técnico indicado pela CONTRATANTE. Caberá ao

Gerente de Projeto coordenar e orientar todo o processo de planejamento, fornecimento, instalação, configuração, integração, migração e testes dos produtos, acompanhando o cumprimento dos prazos e atestando a qualidade dos entregáveis.

11.6 Todas as documentações deverão ser apresentadas em meio digital (por opção da CONTRATANTE pode ser por meio impresso em folha A4 ou A3). Estas serão consideradas como efetivamente entregues e aceitas somente após a validação pela Comissão de Fiscalização da CONTRATANTE.

11.7 As documentações digital ou impressa deverão ser emitidas utilizando a logomarca da CONTRATADA e deverão conter o nome, data e assinatura digital do Gerente de Projeto e Preposto da CONTRATADA.

11.8 Qualquer alteração no corpo técnico ou gerencial da CONTRATADA não poderá afetar o cronograma de entrega nem a execução do Plano de Projeto.

11.9 Regras de Recebimento Provisório e Definitivo

11.9.1 O recebimento provisório dos serviços e soluções tecnológicas objeto deste Termo de Referência ocorrerá após a conclusão das etapas de implantação, instalação, configuração, parametrização, testes e migração, conforme definido no cronograma de atividades a seguir. A formalização será feita por meio de Termo de Recebimento Provisório, emitido pela Comissão de Fiscalização da CONTRATANTE, após a verificação preliminar de que todos os requisitos contratuais, técnicos e de desempenho foram atendidos de forma satisfatória.

11.9.2 Durante o período de recebimento provisório, a CONTRATADA deverá realizar eventuais ajustes, correções e melhorias necessárias, conforme apontamentos da CONTRATANTE, de modo a atender integralmente as especificações estabelecidas no contrato, no Plano de Projeto e demais documentos técnicos de referência.

11.9.3 O recebimento definitivo será formalizado por meio de Termo de Recebimento Definitivo, emitido após o período de observação, homologação e operação assistida definido no cronograma, desde que todas as pendências técnicas, operacionais e documentais tenham sido plenamente sanadas, incluindo a aprovação final da documentação técnica, dos relatórios de testes, da transferência de conhecimento e demais entregáveis previstos.

11.9.4 O prazo para emissão do Termo de Recebimento Definitivo não poderá exceder 90 (noventa) dias, contados a partir da data de assinatura do Termo de Recebimento Provisório.

11.9.5 A CONTRATANTE poderá, a qualquer momento antes da emissão do

recebimento definitivo, realizar novas verificações, testes complementares ou auditorias, visando assegurar o cumprimento integral das condições pactuadas.

11.10 A CONTRATADA deve seguir e cumprir os prazos máximos do cronograma definido na tabela abaixo:

CRONOGRAMA DE ATIVIDADES DE IMPLANTAÇÃO DOS SERVIÇOS (LOTE 1 e 2)			
ITEM	**DESCRIÇÃO DAS ATIVIDADES**	**MÉTRICA**	**PRAZO (Dias Consecutivos)**
01	Reunião de início dos serviços – Apresentação do Preposto, a composição da equipe de trabalho, a Metodologia de Trabalho, os recursos necessários para iniciar os serviços, pontos de atenção da Comissão de Fiscalização e modelo de ordem de serviço.	Prazo, em dias consecutivos, a contar da data designada no Memorando de Início de Serviço.	02
02	I - Vistoria Prévia – A CONTRATADA é autorizada a fazer análise do ambiente tecnológico da CONTRATANTE (18 Dias); II – A CONTRATADA elabora e entrega relatório executivo sumário de diagnóstico e viabilidade técnica à CONTRATANTE (2 Dias).	Prazo, em dias consecutivos, após a entrega do(s) produto(s) descrito(s) no Item anterior.	20
03	A CONTRATANTE Aprova o(s) serviços(s) descrito(s) no item anterior emitindo a Ordem de Serviço para autorizar a CONTRATADA a iniciar a elaboração do Plano de Projeto.	Prazo, em dias consecutivos, após a entrega do(s) produto(s) descrito(s) no Item anterior.	03

04	A CONTRATADA elaborar o Plano de Projeto (Modelo Anexo) e outros necessários à implantação da solução.	Prazo, em dias consecutivos, após a entrega do(s) produto(s) descrito(s) no Item anterior.	05
05	**Finalização**	**Total**	**30**

CRONOGRAMA DE ATIVIDADES DE IMPLANTAÇÃO DOS SERVIÇOS (LOTE 1 e 2)			
ITEM	**DESCRIÇÃO DAS ATIVIDADES**	**MÉTRICA**	**PRAZO (Dias consecutivos)**
05	I - Aprovação ou rejeição do Plano de Projeto e outros pela CONTRATANTE (2 dias). II - A CONTRATADA faz ajustes nos Plano (3 dias) (Opcional).	Prazo, em dias consecutivos, após a entrega do(s) produto(s) descrito(s) no Item anterior.	05
06	A CONTRATADA executa as atividades previstas nos Planos de projeto, visando Entregar, Instalar, Configurar, Testar, Implantar a solução completa de rede (LOTE 1 – IP, MPLS, SD-WAN (segurança) e LOTE 2– IP – MPLS)	Prazo, em dias consecutivos, após a entrega do(s) produto(s) aprovado(s) descrito(s) no Item anterior.	60
07	I - A CONTRATANTE com o suporte da CONTRATADA homologa ou rejeita a Solução Tecnológica Implantada. II A CONTRATADA deve realizar operação e monitoramento completo durante uma semana com todas rotas e regras	Prazo, em dias consecutivos, após a entrega do(s) produto(s) aprovado(s) descrito(s) no Item	10

	migradas para que a CONTRATANTE possa homologar a qualidade e desempenho da solução tecnológica. III- A CONTRATADA faz os ajustes necessários da Entrega (Opcional);	anterior.	
08	I - A CONTRATANTE com o suporte da CONTRATADA Aceita ou Rejeita a Entrega da Documentação Técnica e o Licenciamento dos produtos da solução tecnológica. (2 dias) II - A CONTRATADA faz os ajustes nos Entregáveis Supra (3 dias) (Opcional).	Prazo, em dias consecutivos, após a entrega do(s) produto(s) aprovado(s) descrito(s) no **anterior.**	05
10	I - A CONTRATADA deve realizar a transferência de conhecimento, apresentação do Dashboard de monitoramento e os procedimentos de acompanhamento dos chamados. (9 dias)	Prazo, em dias consecutivos, após a entrega do(s) produto(s) aprovado(s) descrito(s) no Item anterior.	10
11	**Finalização**	**Total**	**90**
12	A CONTRATADA fica autorizada a iniciar os serviços de Administração, Operação, Monitoramento, manutenção e suporte da solução tecnológica implantada.	Prazo, em dias consecutivos, após a entrega do(s) produto(s) aprovado(s) descrito(s) no Item anterior.	Até o Término do Contrato.

Obs: A critério da CONTRATADA e autorizada pela CONTRATANTE, os serviços podem ser realizados em paralelo sem comprometer a qualidade e desempenho dos serviços prestados.

12 DO ACORDO DE NÍVEL DE SERVIÇO - ANS

12.1 Estabelece os critérios que deverão ser obedecidos para que o serviço em questão seja considerado satisfatório. Características Gerais:

12.1.1 Os níveis mínimos de serviços são critérios objetivos e mensuráveis que visam aferir e avaliar diversos fatores relacionados com os serviços contratados, como a qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança.

12.1.2 Os serviços serão medidos e apurados mensalmente, de modo a alcançar as respectivas metas exigidas, conforme definido neste termo;

12.1.3 Serão aplicadas glosas, sob forma de desconto, à CONTRATADA, referentes a falhas nos serviços executados ou em sua infraestrutura, que afetem a qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança dos serviços, quando a responsabilidade for da CONTRATADA;

12.1.4 O valor do desconto, decorrente das glosas descritas nesta seção, e detectadas, conforme disposto neste Termo de Referência, deverá ser concedido na fatura do mês de referência da prestação do serviço, em que foi identificado o não atendimento aos níveis de qualidade de serviço determinados neste Termo;

12.1.5 O faturamento somente poderá ser emitido pela CONTRATADA e atestado pelo fiscal do contrato, após a aferição dos descontos a serem concedidos, decorrentes das glosas aplicadas, os quais deverão ser lançados na fatura do mês de prestação do serviço, onde foram detectadas as ocorrências que ensejaram o não atendimento aos níveis de qualidade de serviço determinados neste Termo;

12.1.6 O ANS é composto de indicadores objetivos indicados no item 12;

12.1.7 Independentemente da glosa e advertências aplicadas, poderá ser aberto procedimento apuratório para aplicação de sanções maiores, mediante justificativa fundada em prejuízos ou transtornos causados em decorrência da entrega imperfeita do objeto contratado.

12.2 Acordo de Nível de Serviço (ANS): Tabela SLA resposta a INCIDENTE NIVEL DE Criticidade.

NIVEL		TIPO TICKET	SLA PRIMEIRA RESPOSTA	SLA RESOLUÇAO	ATENDIMENTO	ACIONAMENTO FABRICANTE	ATENDIMENTO
N0	DESASTRE	DESASTRE	05 min	IMEDIATO pelo tempo necessário	24X7	IMEDIATO pelo tempo necessário	PRESENCIAL/ REMOTO

N1	CRITICA Alta	INCIDENTE	15min	2H	24X7	a partir da 2h	PRESENCIAL/ REMOTO
		REQUISIÇÃO	15min	2H	24X7	a partir da 2h	REMOTO
N2	Alta	INCIDENTE	15min	4H	24X7	a partir da 4h	PRESENCIAL/ REMOTO
		REQUISIÇÃO	15min	4H	24X7	a partir da 4h	REMOTO
N3	Média	INCIDENTE	15min	8H	24X7	a partir da 8h	REMOTO
		REQUISIÇÃO	15min	8H	24X7	a partir da 8h	REMOTO
N4	Baixa	INCIDENTE	45min	24H	8x5	se for necessário	REMOTO
		REQUISIÇÃO	45min	24H	8x5	se for necessário	REMOTO

NIVEIS		**DEFINIÇÕES**
N0	DESASTRE	Está indisponível a todos os clientes Em até 2 (duas) horas, um especialista do time do MSS ou especialista indicado pela Contratada, com aceite da CONTRATANTE, deverá estar presente nas dependências da PGERJ.
N1	CRITICA Alta	Incidente crítico com muito impacto/
N2	Alta	Grande com impacto significativo
N3	Média	O impacto é inconveniente não impede a operação ou os negócios
N4	Baixa	Impacto baixo ou zero

INSTRUMENTO DE MEDIÇÃO DE RESULTADO LOTES 1 E 2 – SERVIÇOS DE SUPORTE E SEGURANÇA				
ITEM	**INDICADOR**	**MÉTRICAS**	**META MENSAL**	**GLOSA POR DESCUMPRIMENTO DA META**
01	Triagem de incidentes de segurança. (Em horas).	Tempo = Hora da triagem – Hora de entrada do evento de segurança <= 15 minutos.	>= 99,5 %	0,55%
02	Resposta para os incidentes de segurança com gravidade considerada ALTA pelo CONTRATANTE. (Em horas).	Tempo = Hora do início da resposta – hora da triagem <= 30 minutos.	>= 99,5 %	0,65%
03	Resposta para os incidentes de segurança com gravidade considerada MÉDIA pelo CONTRATANTE. (Em horas).	Tempo = Hora do início da resposta - hora da triagem <= 60 minutos.	>= 99,5 %	0,55%
04	Resposta para os incidentes de segurança com gravidade considerada BAIXA pelo CONTRATANTE. (Em horas).	Tempo = Hora do início da resposta – hora da triagem <= 120 minutos.	>= 99,5 %	0,55%
05	Correção de incidentes nos serviços de segurança, que façam parte do escopo deste projeto, em caso de Indisponibilidade. (Em horas)	Tempo = Hora do restabelecimento – Hora do início da indisponibilidade <= 120 minutos.	>= 99,5 %	0,55%
06	Indicação de solução de controle para tratamento de grave vulnerabilidade ou ameaça emergente, nos equipamentos e softwares utilizados pela CONTRATADA para entrega dos Serviços. Disponibilizados pelos fabricantes. (Em horas).	Tempo = Hora de conclusão do planejamento da requisição de mudança – hora de disponibilização dos patches e hot- fixes ou divulgação de grave vulnerabilidade ou ameaça emergente <= 72 horas.	>= 99,5 %	0,55%
07	Aplicação de patches e hotfixes ou atualização dos firmwares e/ou softwares das soluções entregues. Sem gravidade. (Em horas).	Tempo = Hora de conclusão do planejamento da requisição de mudança – hora de disponibilização dos patches e hot- fixes ou atualização de firmware <= 96 horas.	>= 99,5 %	0,55%
08	Resposta a incidentes - tempo para responder a um incidente de phishing desconhecido relatado pelo cliente	Iniciar análise em até 30 minutos.	>= 99,7 %	0,55%
09	Alerta de Vulnerabilidades – Vulnerabilidades críticas das Soluções Assistidas.	Em até 24 horas após publicação.	>= 99,7 %	0,55%
10	Tratamento de Incidentes Críticos e médios Detectados.	Em até 20 Minutos para iniciar o tratamento.	>= 99,7 %	0,55%
11	Abertura de chamados de suporte.	Tempo = Hora de abertura do chamado – hora da triagem <= 10 minutos.	>= 99,7 %	0,55%

INSTRUMENTO DE MEDIÇÃO DE RESULTADO LOTES 1 E 2 – SERVIÇOS DE SUPORTE E SEGURANÇA				
ITEM	**INDICADOR**	**MÉTRICAS**	**META MENSAL**	**GLOSA POR DESCUMPRIMENTO DA META**
12	Finalizar a requisição de serviço ou incidente sem a devida resolução ou sem realizar os testes necessários para aferir a efetiva resolução.	Quantidade de requisições finaliza- das com resolução/ quantidade de requisições finalizadas * 100.	>= 99,7 %	0,55%
13	Finalizar uma requisição de serviço sem documentar os procedimentos executados para atendimento da solicitação.	Quantidade de requisições finaliza- das com documentação / quantidade de requisições finalizadas * 100.	>= 99,0%	0,55%
14	Relatório de Investigação e Remediação do Incidente.	8 Horas (a partir da detecção do incidente).	>= 99,7 %	0,55%
15	Comunicação de incidentes aos gestores de TI do CONTRATANTE. (Em horas).	Tempo = Hora da comunicação – hora da triagem <= 60 minutos.	>= 99,7 %	0,55%
16	Finalizar um incidente sem documentar a causa, a solução de contorno (se houver) ou os procedimentos adotados para solução.	Quantidade de incidentes finaliza- dos sem documentar a causa, a solução de contorno (se houver) ou os procedimentos adotados para solução / Quantidade de incidentes finalizados * 100.	>= 99,5 %	0,55%
17	Finalizar um problema sem documentar a investigação realizada, a causa-raiz ou a solução aplicada.	Quantidade de problemas finaliza- dos sem documentar a investigação realizada, a causa- raiz ou a solução aplicada / Quantidade de problemas finalizados * 100.	>= 99,5 %	0,55%
18	Entrega mensalmente dos relatórios.	Unidade. Até quinto dia útil do mês seguinte.	100%	0,55%
TOTAL GLOSAS – podendo chegar até				**10%**

Tabela de Medição de serviços

12.3 Taxa de Entrega para toda Rede

12.3.1 A CONTRATADA deverá garantir a taxa máxima de perda de pacotes de 2 % para todas as localidades objeto desta contratação.

12.3.2 As penalidades abaixo serão aplicadas nos valores individuais de cada acesso e constarão na fatura mensal do mês subsequente à prestação do serviço:

Taxa de entrega mensal média (%)	Penalidade (Desconto)
Abaixo de 99,7 a 99,5	0,50%
Abaixo de 99,5 a 99,3	1 %
Abaixo de 99,3 a 99,0	3%
Abaixo de 99,0 a 80,0	5 %
Abaixo de 80,0	10 %

Tabela 4 – Taxas de entrega e suas penalidades

12.4 Disponibilidade

12.4.1 A CONTRATADA deverá garantir a disponibilidade mensal do serviço para todas as localidades objeto desta contratação de 99,5% (aproximadamente equivalente a 3 horas e 39 minutos de interrupção máxima em um mês de 30 dias).

12.4.2 As penalidades abaixo serão aplicadas nos valores individuais de cada localidade do Núcleo Central ou do acesso à internet, e constarão na fatura mensal do mês subsequente à prestação do serviço.

Diferença entre a disponibilidade acordada e a medida (%)	Penalidade (desconto)
Acima de 0,7 até 1,2	0,50%
Acima de 1,2 até 2,4	1%
Acima de 2,4 até 5	5%
Acima de 5	10 %

Tabela 5 – Diferenças entre disponibilidades acordadas/medidas e suas penalidades

O cálculo do índice de disponibilidade será feito baseado na seguinte fórmula: Índice de Disponibilidade Mensal apurada = (1 – (interrupção de cada localidade (minutos) / 43.200 (minutos)) x 100; onde 43.200 minutos é igual a 30 dias corridos.

12.5 Latência

12.5.1 A CONTRATADA deverá garantir a latência média (Rede MPLS) para as seguintes velocidades discriminadas na tabela a seguir:

Velocidade	Localidade	Latência Média
100 Mbps	MPLS Estado Rio de Janeiro	20 ms
300 Mbps	MPLS Estado Rio de Janeiro	20 ms
1 Gbps	IP Dedicado -Sede PGE (Internet)	10 ms
2 Gbps	Concentradores MPLS SEDE	20 ms
300 Mbps	MPLS – Brasília	40 ms
100 Mbps	MPLS – Brasília	40 ms

Tabela 6 – Garantia de latência média

TIPO	TIPO
Fórmula de Cálculo	Tempo em que um pacote IP leva para ir de um ponto a outro da rede e retornar à origem. A apuração da latência na rede da PGE/RJ será efetuada com o envio de pacotes ICMP de tamanho fixo de 1500 bytes, entre terminais de origem e destino localizados em sítios da rede dentro do mesmo Backbone e retornando à origem onde será realizada a medição do tempo de resposta destes pacotes A latência corresponde ao tempo de ida e volta do pacote.
Cálculo	Para os links MPLS, as medições de latência devem ser feitas entre roteador da PGE-Sede e os roteadores remotos fim a fim. - Para os links de internet, as medições de latência devem ser feitas entre o Roteador internet ou Appliance SD-WAN, e o roteador de borda da CONTRATADA. O tempo de resposta limite a ser aguardado para cada pacote deverá ser de 5 segundos. Valores superiores a este tempo serão considerados “timeout”. Cada medida deverá ser realizada através do envio de uma série de 4 pacotes ICMP por vez. Os intervalos de observação deverão ser de 5 (cinco) minutos durante o intervalo de tempo demandado pela PGE/RJ. Todos os resultados obtidos através das medições deverão ser disponibilizados e considerados no indicador diário de latência. Para garantir a validade das medidas, a CONTRATADA poderá configurar os roteadores da rede (nível 3 da camada OSI) para tratarem os pacotes ICMP com

	prioridade, porém nunca superior ao restante do tráfego. Os valores das médias diárias das medidas deverão ser inferiores ao valor estabelecido para a latência máxima permitida (limiar de qualidade).
Periodicidade da Aferição	Mensalmente com apresentação de relatório do intervalo solicitado. Este indicador deverá ser constantemente monitorado.

Tabela 7 – Indicador: Latência da Rede

12.5.2 A CONTRATADA sofrerá a penalidade de 5% (cinco por cento) na fatura mensal de cada acesso, caso seja constatado que os valores de latência média máxima não forem atingidos.

12.5.3 A CONTRATADA estará sujeita à penalidade de 1% (um por cento) sobre o valor da fatura mensal, caso não entregue os Relatórios Mensais até o 5º (quinto) dia útil do mês subsequente.

12.5.4 Os índices que refletem os parâmetros de qualidade anteriormente indicados (Taxa de Entrega e Disponibilidade mais Latência) serão medidos e apresentados pela CONTRATADA à CONTRATANTE na forma de relatórios mensais (Relatórios de Nível de Serviço).

12.5.5 A CONTRATADA deverá informar à CONTRATANTE, por escrito e com antecedência mínima de 05 (cinco) dias úteis, sobre quaisquer interrupções ou interferências programadas que possam causar alguma alteração no desempenho dos serviços.

12.5.6 O Relatório de Nível de Serviço mensal deverá ser entregue em meio digital.

12.5.7 A CONTRATADA deverá apresentar, no Relatório de Nível de Serviço, gráficos que demonstrem o comportamento da utilização da banda de comunicação disponível para cada localidade de interesse da PGE/RJ (Núcleo Central, Rede Externa e acesso à internet).

12.5.8 As interrupções programadas por solicitação da CONTRATANTE ou por necessidade da CONTRATADA (estas em função de parada técnica para manutenção/reconfiguração, desde que previamente acertadas com a CONTRATANTE), não serão contabilizadas para o cálculo de disponibilidade do serviço.

12.5.9 A CONTRATADA deverá se comprometer a adotar as providências julgadas necessárias à expansão do seu *Backbone*, utilizado pela Rede PGE/RJ, quando

a capacidade de tráfego no mesmo atingir 70% da capacidade total.

12.6 Taxa de Erro

12.6.1 A taxa de erro representa a perda de pacote em cada acesso, sendo medida com o objetivo de verificar a qualidade dos serviços prestados:

A. Para testes na Rede PGE/RJ, a taxa de erro será avaliada através do envio de pacotes de 1500 bytes por um período de 5 (cinco) minutos;

B. Para a realização desse teste, será considerada a interligação da porta POP do Backbone IP-MPLS da CONTRATADA (operadora A e operadora B) e a porta do CPE da localidade atendida;

C. A taxa de erro deverá ser medida na ativação de um novo circuito e por solicitação da CONTRATANTE junto à CONTRATADA (operadora A e operadora B);

D. As informações para cálculo da taxa de erro serão obtidas das estatísticas geradas pelo CPE de acesso;

E. A taxa de erro será obtida dividindo-se o número de bits recebidos com erro pelo número total de bits transmitidos no período de testes;

F. A taxa de erros máxima admissível obedecerá aos parâmetros contidos na tabela a seguir:

Capacidade	Taxa de Erro Máximo
100 Mbps	1×10^{-9}
Acima de 100 Mbps	1×10^{-9}

Tabela 8 – Taxa de Erro

12.7 Provisionamento dos Serviços

12.7.1 A indisponibilidade dos *appliance*s SD-WAN das unidades remotas não implicará na indisponibilidade dos serviços dos links MPLS dessas unidades.

12.7.2 A indisponibilidade total do cluster de appliances SD-WAN da Sede ou do roteador MPLS da Sede implicará automaticamente na indisponibilidade do serviço de link MPLS das unidades remotas.

12.7.3 Não serão consideradas indisponibilidades as seguintes situações: 12.7.3.1.Paradas programadas pela CONTRATADA e aprovadas pela PGE/RJ. Neste caso, a autorização deve ser solicitada pela CONTRATADA com, pelo menos, 5 (cinco) dias úteis de antecedência;

12.7.3.2 Paradas ocasionadas nos equipamentos por erros de configuração

causados pela PGE/RJ, sem responsabilidade da CONTRATADA;

12.7.3.3 Paradas ocasionadas por casos fortuitos ou de força maior, devidamente comprovados.

12.8**Serviço de *Backbone* (Anti-DDOS), deverá possuir o seguinte SLA**:

12.8.1 Prazo para entrega de relatórios mensais: até 5 (cinco) dias úteis.

12.8.2 Prazo para entrega de relatórios de incidente (após mitigação do ataque): até 5 (cinco) dias úteis.

12.8.3 Atendimento às solicitações em regime 24x7xtodos os dias do ano:

12.8.4 Prioridade 1: Requisição de adição/retirada de rede monitorada, modificação na lista de contatos autorizados do cliente, relatórios de dados do tráfego do cliente monitorado em um período especifico. Prazo máximo de 2 horas.

12.8.5 Prioridade 2: Requisição da lista de redes monitoradas, alertas e mitigações, informações sobre ataques recebidos, lista de contatos autorizados pelo cliente. Prazo máximo de 8 horas.

12.8.6 SLA de Mitigação de Ocorrência de Incidentes.

12.8.7 Tempo de Detecção = **Ocorrências** Início do Ataque/ Detecção do Ataque/ Contato com a PGERJ = **Prazo Até 15 minutos**

12.8.8 A apuração e/ou contabilização das grandezas acima definidas, para efeito de aferição de resultados, dar-se-á mensalmente.

12.9Observações

12.9.1 As penalidades contratuais decorrentes da inexecução dos serviços poderão ser aplicadas independentemente dos descontos aplicados por força do Acordo de Nível de Serviços - ANS.

12.9.2 A Comissão de Fiscalização do Contrato da PGE/RJ poderá elaborar relatório, informando à CONTRATADA sobre o resultado da medição dos serviços, mediante aplicação do Acordo de Nível de Serviço, apurado para que a CONTRATADA tome providências para correções.

12.9.3 O setor financeiro da PGE/RJ receberá junto com nota fiscal do mês, quando e se for o caso, relatório contendo a pontuação.

13. DA FORMAÇÃO DE CONSÓRCIOS E SUBCONTRATAÇÃO

13.1 Será permitida a formação de Consórcios, de acordo com o disposto no Art. 15 da Lei 14.133/21, constituídos por empresas nacionais ou por empresas nacionais e estrangeiras, exclusivamente para o **Lote 01**, limitado a 3 (três) membros por consórcio, desde que atendam integralmente os requisitos de habilitação e as condições estabelecidas neste Edital.

13.2 A justificativa da permissão de consórcio para **somente o Lote 01** deve-se ao fato de que algumas licitantes que não possuem em seu catálogo de serviços a solução de AntiDDoS, Gerenciamento de Segurança MSS e pouca ou nenhuma infraestrutura física própria em regiões mais remotas do Estado, precisando assim fazer uso de provedores locais para agregar o serviço via consorciamento.

13.3 Na constituição de consórcio deverão ser atendidas as seguintes exigências:

13.3.1 Indicação da empresa líder do Consórcio, que deverá atender às seguintes condições de liderança:

13.3.2 No consórcio de empresa brasileira e estrangeira, a liderança caberá obrigatoriamente à empresa brasileira;

13.3.3 No caso de consórcio com empresa estrangeira a empresa líder será responsável por todas as providências que forem necessárias para atender a legislação nacional nos aspectos legais e de comércio exterior;

13.3.4 À empresa líder caberão as seguintes obrigações:

13.3.4.1 Responsabilizar-se por todas as comunicações e informações do Consórcio;

13.3.4.2 Responder e Administrar o contrato;

13.3.4.3 Apresentar Termo de Compromisso público ou particular de constituição em Consórcio, subscrito pelas consorciadas, contendo a indicação da empresa líder responsável pelo consórcio e as seguintes responsabilidades:

13.4 Compromissos e obrigações das consorciadas, dentre os quais o de que cada consorciada responderá, individual e solidariamente, pelas exigências e ordens fiscais, administrativas e contratuais pertinentes ao objeto da licitação;

13.5 Declaração expressa de responsabilidade solidária, ativa e passiva, das consorciadas pelos atos praticados pelo consórcio em relação à licitação e,

posteriormente, ao eventual Contrato, até o final de sua execução;

13.6 Compromisso de que o consórcio não terá a sua composição ou constituição alterada ou, sob qualquer forma, modificada, sem prévia e expressa anuência da CONTRATANTE, até a conclusão dos trabalhos ou serviços que vierem a ser contratados;

13.7 Compromisso expresso de que o consórcio não se constitui, nem se constituirá em pessoa jurídica distinta da de seus membros, nem terá denominação própria ou diferente das suas consorciadas;

13.8 Compromissos e a divisão do escopo no fornecimento para cada uma das consorciadas, individualmente, em relação ao objeto da licitação, bem como o percentual de participação de cada uma em relação ao custo do fornecimento dos serviços previstos;

13.9 A empresa consorciada fica impedida de participar, no mesmo lote, em mais de um consórcio ou de forma isolada.

13.10 A empresa consorciada não poderá participar dos demais lotes;

13.11 A licitante vencedora, no caso de consórcio, fica obrigada a promover, antes da celebração do contrato, a constituição e o registro do consórcio, por escritura pública ou documento particular registrado na Junta Comercial, discriminando a empresa líder, a participação de cada uma das empresas e a responsabilidade solidária dos consorciados por atos praticados na fase de licitação e no decorrer da execução do contrato.

13.12 Para efeito de habilitação, cada consorciada deverá apresentar os documentos exigidos para habilitação deste Edital, admitindo-se, para efeito de qualificação técnica, o somatório dos atestados apresentados por cada empresa a fim de atingir o quantitativo total exigido. Para efeito de qualificação econômico-financeira, deverão ser demonstradas individualmente, por parte de cada pessoa jurídica participante do certame e são aplicáveis a todos os lotes, exceto para a comprovação do patrimônio líquido, quando da participação em consórcio, que neste caso será comprovado pelo somatório dos valores de cada consorciado, na proporção de sua participação.

13.13 As empresas estrangeiras que não funcionem no País atenderão aos requisitos de habilitação deste Edital, mediante documentos equivalentes, autenticados pelos respectivos consulados e traduzidos por tradutor juramentado.

13.14 As empresas estrangeiras participantes de consórcio deverão possuir

representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente.

13.15 Não poderá participar do consórcio empresa ou firma na qual figure, entre seus diretores, responsáveis técnicos ou sócios, funcionários, empregados ou ocupante de cargo comissionado e servidores na CONTRATANTE.

13.16 O prazo de duração do consórcio deverá ser maior do que o prazo de vigência do contrato.

13.17 Não será permitida a subcontratação das atividades diretamente relacionadas ao objeto principal da contratação, especialmente aquelas inerentes à prestação do serviço de comunicação de dados, incluindo gerenciamento, operação, suporte e garantia dos níveis de serviço (SLA).

Será admitida, excepcionalmente, a subcontratação restrita às atividades complementares e aos meios de acesso da última milha, desde que:

I – não implique transferência integral ou parcial da responsabilidade pela execução do objeto contratado;
II – não acarrete prejuízo à qualidade dos serviços ou à sua economicidade;
III – não comprometa os níveis de serviço (SLA) estabelecidos;
IV – permaneça sob a responsabilidade integral da CONTRATADA;
V – seja previamente informada à CONTRATANTE, quando aplicável.

13.18 Entende-se com atividade complementar aquelas atividades de apoio para montagem ou manutenção do item de serviço;

13.19 Entende-se como meio de acesso da última milha a rede ou meio físico que interliga diretamente o provedor e o cliente;

13.20 A subcontratação não exime a responsabilidade da CONTRATADA, observada a qualidade, a fidelidade ao objeto e a garantia sobre a totalidade dos serviços prestados, cabendo-lhe também a devida supervisão e coordenação dessas atividades;

13.21 A subcontratação fica condicionada à expressa anuência da PGE-RJ;

13.22 A subcontratação observará estritamente os limites estabelecidos no subitem 13.17, sendo vedada a transferência, total ou parcial, das atividades essenciais relacionadas ao objeto principal da contratação.

Permanecerá sob responsabilidade exclusiva da CONTRATADA a execução integral

do contrato, inclusive quanto à qualidade dos serviços prestados, ao cumprimento dos níveis de serviço (SLA) e às obrigações contratuais, não sendo admitida a transferência de responsabilidade à(s) subcontratada(s). A eventual subcontratação não exime a CONTRATADA de suas responsabilidades legais e contratuais, nos termos do art. 122 da Lei nº 14.133/2021.

14. POSSIBILIDADE DE PARTICIPAÇÃO DE COOPERATIVA

14.1 Fica vedada a participação de cooperativas na execução deste contrato. A CONTRATADA deverá ser uma empresa habilitada a prestar diretamente os serviços contratados, atendendo às exigências técnicas e contratuais estabelecidas, sem transferência de responsabilidade para cooperativas ou associações similares.

15. DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

A CONTRATADA deverá:

15.1 A CONTRATADA será responsabilizada pela entrega dos bens ou prestação dos serviços dos itens da contratação conforme prazos, especificações, garantias e ritos estabelecidos neste;

15.2 Cabe à CONTRATADA, com base em atividades de monitoramento contínuo e seguindo as melhores práticas e frameworks consolidados no mercado (como ITIL, COBIT, NIST, entre outros), propor melhorias no ambiente da CONTRATANTE. Tais melhorias poderão envolver recomendações relacionadas a equipamentos, roteamento, configurações, acessos, regras de firewall, SDWAN, permissões e demais aspectos da infraestrutura de rede, com o objetivo de otimizar desempenho, segurança e disponibilidade dos serviços.

15.3 Elaborar o Plano de Trabalho, de acordo com as condições estabelecidas pela CONTRATANTE.

15.4 Prestar os serviços, somente após o recebimento da respectiva Ordem de Serviço – OS emitida pela CONTRATANTE, na qual deverá estar registrada a concordância de, no mínimo, 2 (dois) membros da Comissão de Fiscalização do Contrato.

15.5 Cumprir todos os requisitos de segurança da informação, respeitando a

preservação do sigilo, da integridade, dos direitos autorais e dos aspectos legais concernentes aos documentos que lhe forem entregues para a prestação dos serviços.

15.6 Deverá ser possível realizar, para atendimento a necessidades especiais e temporária, o aumento emergencial da largura de banda em pelo menos 50% da capacidade contratada, como por exemplo: Eventos considerados críticos, transmissões on-line ou mutirões de atendimento ao contribuinte.

15.7 Observar que existe a possibilidade de se instalar novos sítios, de acordo com o interesse do CONTRATANTE, e nesses casos a CONTRATADA deverá providenciar os meios de acesso e as instalações necessárias ao funcionamento das localidades informadas.

15.8 Cumprir e aceitar todos os requisitos do Acordo de Nível de Serviços (ANS).

15.9 A CONTRATADA deverá enviar relatatório mensalmente conforme

15.10 Resumo descritivo da operação dos serviços no período em questão

15.11 Solução de Incidentes de segurança associados ao Suporte assistido de gerência de rede e segurança;

15.12 Ações de melhorias implantadas no mês;

15.13 Análise das ocorrências de acionamento fora do horário administrativo e ações tomadas ou sugeridas, quando não forem da competência da CONTRATADA, para evitar a recorrência;

15.14 Número de políticas implementadas de detecção e resposta automática a incidentes de segurança da informação;

15.15 Políticas de segurança revistas e/ou criadas para melhoria do ambiente

15.16 Será disponibilizado um modelo para ser usado como referência, para cada *link* contratado, um relatório com as seguintes informações:

A. Identificação do link

B. Identificação da localidade (de acordo com as denominações da CONTRATANTE)

C. Velocidade do link

D. Tipo do Link

E. Média de uso no período em Mbps

F. Disponibilidade do link em %.

G. Taxa Erros e retransmissões em %.

H. Média de latência no período em milissegundos.

I. Atendeu o acordo de nível de serviço previsto no contrato (Sim ou Não)

J. Valorado em reais e descriminado

K. E caso não atenda o acordo de nível de serviço previsto no contrato, deverá constar o valor da(s) multa(s) e o valor total a ser pago pela CONTRATANTE já descontado a(s) multa(s);

15.17 O envio do relatório deverá ocorrer em até o 5° (quinto) dia útil do mês após o encerramento do mês de referência, sendo enviado para equipe de fiscalização da CONTRATANTE, mesmo que seja possível extrair da ferramenta de Gerência Disponibilizada o relatório mensal.

15.18 O envio do relatório deverá ocorrer em até o 5° (quinto) dia útil do mês após o encerramento do mês de referência, sendo enviado para equipe de fiscalização da CONTRATANTE, mesmo que seja possível extrair da ferramenta de Gerência Disponibilizada o relatório mensal

15.19 O relatório terá de possuir o formato xlsx, pdf ou outro acordado com a CONTRATANTE.

15.20 Instalar, configurar, manter, recuperar e aplicar atualizações corretivas ou evolutivas de novas versões ou releases para aplicativos, softwares básicos e demais componentes necessários ao pleno funcionamento do objeto desta contratação, sob solicitação ou mediante aval da PGERJ;

15.22 Monitorar e acompanhar o desempenho e disponibilidade, atuando para manter os níveis definidos nesta especificação, da infraestrutura de servidores e serviços que compõem da CONTRATADA;

15.23 Realizar rotinas de verificação dos sistemas e aplicações suportados, inclusive a implantação e manutenção de rotinas automáticas;

15.24 Ficará a cargo de cada CONTRATADA a realização de backups em todos os seus equipamentos e responsavél pela disponibilidade e integridade desses backups.

15.25 A CONTRATADA deverá entregar um plano operacional de resposta a incidentes, baseado em MITRE ATT&CK ou NIST SP 800-61, contendo:

15.25.1 Fluxo de comunicação;

15.25.2 Níveis de criticidade;

15.25.3 Medidas de contenção e recuperação;

15.25.4 Prazos por categoria de incidente.

15.26 Ficará a cargo de cada CONTRATADA a realização dos backups de todos os seus equipamentos, sendo também de sua responsabilidade garantir a disponibilidade e a integridade desses backups.

15.27 Fornecer os serviços de implantação dos enlaces e executar os procedimentos de implantação, instalação, manutenção, comissionamento, integração, testes de funcionamento e operação de todos os produtos, equipamentos e softwares fornecidos, responsabilizando- se por todas as conexões, materiais, acessórios e mãode-obra, de forma a atender integralmente às necessidades do CONTRATANTE, conforme especificado

15.28 Cumprir todos os requisitos do Termo de Referência e seus Encartes Técnicos, referentes às condições gerais e aos prazos para prestação dos serviços, responsabilizando-se pelas eventuais despesas de deslocamento de técnicos, diárias, hospedagem e demais gastos relacionados com a equipe técnica, sem qualquer custo adicional ao CONTRATANTE;

15.29 Para cada instalação de circuito de dados, utilizar equipamentos atualizados tecnologicamente em sua última versão, não podendo estar em situação de End-ofLife ou End-of-Sale, estarem sendo suportados e recebendo atualizações de segurança do fabricante, e que atendam integralmente os requisitos técnicos estabelecidos no Termo de Referência, bem como realizar a substituição de qualquer componente sempre que solicitado pela CONTRATANTE, com a devida justificativa técnica;

15.30 Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, as partes do objeto deste contrato em que se verificarem vícios, defeitos ou incorreções resultantes dos materiais empregados ou da execução dos serviços;

15.31 A CONTRATADA realizará os serviços de implantação, suporte, operação, administração e manutenção da solução. Além disso, irá fornecer acesso aos administradores de tecnologia da informação do CONTRATANTE para realização de serviços de monitoramento e auditoria.

15.32 Respeitar a Política de Segurança do CONTRATANTE e fornecer todas as informações solicitadas por ele;

15.33 Acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades;

15.34 Responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, os quais não têm qualquer vínculo empregatício com a CONTRATANTE;

15.35 Manter atualizados os números de telefone, os endereços de e-mail, site web para a abertura de chamados.

15.36 Disponibilizar canais de acesso em regime 24x7x365, por meio de número de telefone e/ou Internet, para a abertura de chamados técnicos, objetivando a resolução de problemas e dúvidas quanto aos serviços, produtos e funcionamento dos equipamentos e serviços contratados, pelo período total da garantia contratada e permitir a utilização de estrutura de pesquisa em base de conhecimento de solução de problemas e documentos técnicos do Fabricante.

15.37 A CONTRATADA deverá realizar todos os serviços necessários para interligação de seu MSS ou NOC às instalações da CONTRATANTE, por meio de uma VPN IPsec, com a finalidade exclusiva de realizar intervenções remotas e monitoração, durante a vigência do Contrato. Todo acesso de monitoração do ambiente e eventuais intervenções remotas pela CONTRATADA, deverão ser feitos exclusivamente por esse serviço de comunicação de dados, sendo vedada a utilização da Internet para tal fim.

15.38 Dar garantias técnicas dos serviços executados.

15.39 Atendimento às solicitações de alterações (inclusão e exclusão) de Rotas e regra de acesso.

15.40 Atendimento às solicitações de logs e relatórios.

15.41 Toda e qualquer alteração na configuração da solução (aplicação de novas rotas, exclusão de rotas, atualização de versões, aplicações de “patches”, etc.) ocorrerá mediante autorização formal da CONTRATANTE.

15.42 Na ocorrência de Incidentes:

15.42.1 No caso de detecção de algum incidente de segurança, a CONTRATADA deverá notificar a CONTRATANTE dentro do período

estabelecido no ANS, para que sejam tomadas as medidas corretivas e legais necessárias;

15.42.2 Tomar as providências necessárias, em caso da ocorrência de algum incidente (análise dos logs, rastreamento da ocorrência);

15.42.3 São considerados incidentes de rede e segurança: indisponibilidade de serviços, perda de desempenho da rede, os acessos indevidos, ataques por força bruta, ou qualquer outra ação que vise prejudicar a funcionalidade ou a disponibilidade dos serviços da CONTRATANTE;

15.42.4 A CONTRATADA comunicará imediatamente a CONTRATANTE, para que possam ser tomadas ações preventivas, nos casos de tentativas, sem sucesso, de acessos indevidos, de instalação de códigos maliciosos, ou de qualquer outra ação que venha pôr em risco a segurança do ambiente da CONTRATANTE, em que seja evidenciada a insistência, por parte da pessoa mal-intencionada;

15.43 Comunicar à CONTRATANTE, por escrito, no prazo máximo de 5 (cinco) dias úteis que antecedem o prazo de vencimento das entregas, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos de execução dos serviços, propondo as ações corretivas necessárias para a execução dos mesmos.

15.44 Submeter à aprovação da CONTRATANTE qualquer alteração que se tornar essencial à continuação da execução ou prestação dos serviços.

15.45 Arcar com todas as despesas referentes à prestação dos serviços, tais como: despesas com viagens, fretes, seguros, taxas, transportes e embalagens, bem como, os encargos trabalhistas, previdenciários, comerciais e salários dos seus empregados, para entrega do serviço no prazo estipulado.

15.46 Comprovar que os responsáveis pelos serviços de consultoria, manutenção e suporte técnico possuam a qualificação técnica necessária do fabricante dos produtos e a experiência comprovada em atividades similares, as quais irão executar, a fim de atender as especificações técnicas contidas neste instrumento, de forma a garantir a máxima qualidade na prestação.

15.47 Manter seus funcionários ou representantes credenciados, devidamente identificados, quando da execução de qualquer serviço nas dependências da CONTRATANTE, referente ao objeto contratado, observando as normas de segurança (interna e de conduta).

15.48 Responder integralmente pelos danos causados ao patrimônio da PGE/RJ ou de terceiros por seus empregados, direta ou indiretamente, em decorrência de ação ou omissão de seus empregados ou de seus Prepostos, devendo ser adotadas as providências necessárias ao integral ressarcimento, não se excluindo ou reduzindo essa

responsabilidade.

15.49 Responder em razão da fiscalização ou do acompanhamento realizado pela CONTRATANTE.

15.50 Arcar com os ônus resultantes de quaisquer ações, demandas, custos e despesas decorrentes de contravenções, seja por culpa sua ou de quaisquer de seus empregados ou Prepostos, obrigando-se, outrossim, a quaisquer responsabilidades decorrentes de ações judiciais ou extrajudiciais de terceiros, que lhe venham a ser exigidas por força da lei, ligadas ao cumprimento do Contrato a ser firmado.

15.51 Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com a CONTRATANTE.

15.52 A CONTRATADA deverá manter durante a vigência do contrato, as condições de habilitação exigidas na licitação, devendo comunicar a CONTRATANTE a superveniência de fatos impeditivos da manutenção dessas condições.

15.53 Responder por todos os vícios e defeitos dos serviços prestados durante toda a vigência do Contrato, contados a partir do aceite definitivo da prestação (atesto).

15.54 Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados, não podendo invocar posteriormente, desconhecimento para cobrança de serviços extras.

15.55 Aceitar, nas mesmas condições pactuadas, os acréscimos ou supressões que se fizerem necessários no objeto, até o limite previsto no artt. 125 da lei 14.133/2021.

15.56 Designar, observado o disposto no art.118 da Lei n.º 14.133/21, Preposto para representar administrativamente a CONTRATADA sempre que necessário, o qual deverá estar habilitado a responder qualquer indagação pela CONTRATADA sobre a parte operacional e de qualidade dos serviços executados, bem como solucionar qualquer problema relacionado com a sua execução e qualidade, que esteja em desacordo com a Proposta da CONTRATADA e durante a vigência do Contrato.

15.57 O Preposto deverá ser identificado perante a fiscalização do Contrato, a qual fará constar o nome, a qualificação, o endereço físico e eletrônico, além do número de telefone. A CONTRATADA deverá comunicar à Fiscalização qualquer alteração do Preposto que a representa:

15.57.1 Acatar as exigências da Fiscalização da PGE/RJ quanto à execução dos

serviços, qualidade e providenciar a imediata correção de deficiências constatadas que estejam em desacordo com o disposto no Contrato, quanto à execução dos serviços contratados;

15.57.2 Deverá ser disponibilizado um canal direto com o preposto via WhatsApp, juntamente com a equipe técnica, durante o período do contrato, 8X5 durante o horário comercial, em casos de incidentes críticos fora do horário comercial.

15.58 Comunicar ao Fiscal do Contrato, por escrito (Nota Técnica) e tão logo constatado problema ou a impossibilidade de execução de qualquer obrigação contratual, para a adoção das providências cabíveis;

15.58.1 Manter atualizado o número de telefone (fixo ou celular) para contatos ou abertura de chamados;

15.58.2 Prover os serviços ora contratados, com pessoal adequado e capacitado em todos os níveis de trabalho;

15.58.3 Garantir uma solução com alta performance no tempo de resposta satisfatória;

15.58.4 Iniciar e concluir os serviços nos prazos estipulados;

15.58.5 Responder pelos serviços que executar, na forma do presente instrumento e da legislação aplicável;

15.58.6 A CONTRATADA deverá observar às cláusulas contratuais e o rigoroso cumprimento das suas atribuições e responsabilidades.

15.58.7 A CONTRATADA deverá assinar o documento Termo de Confidencialidade e Sigilo e entregá-lo ao CONTRATANTE até a data marcada para a reunião de início de projeto. Consiste em condição para a prestação de todos os serviços, estabelecendo sigilo das informações do ambiente da CONTRATANTE, com acesso mínimo e restrito aos técnicos designados para a prestação dos serviços.

15.58.8 A CONTRATADA não poderá configurar links de dados oriundos de outros contratos no mesmo ambiente físico e lógico da rede corporativa a ser estabelecida por esta contratação.

15.58.9 Toda informação referente à CONTRATANTE que a CONTRATADA vier a tomar conhecimento por necessidade de execução dos serviços ora contratados não poderá ser divulgada a terceiros sem autorização expressa do CONTRATANTE.

15.58.10 A CONTRATANTE terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação, que devem

ser gerados e entregues de acordo com os padrões e formatos definidos pela CONTRATANTE.

15.58.11 Dar garantias técnicas dos serviços executados nos limites razoáveis da lei.

16. DAS OBRIGAÇÕES DA CONTRATANTE

A CONTRATANTE deverá:

16.1 Acompanhar e fiscalizar a execução do Contrato por meio de representantes especialmente designados, nos termos do art. 117 da Lei nº 14.133/21 e do Decreto Estadual nº 48.817/2023.

16.2 Manter a CONTRATADA informada acerca da composição da Comissão de Fiscalização, cientificando-lhe para fins de propiciar que seus Prepostos possam reportar eventuais falhas ou problemas detectados, bem como, possam apresentar-lhes os faturamentos correspondentes às prestações executadas.

16.3 Disponibilizar o local e os meios adequados para a execução dos serviços.

16.4 Efetuar os pagamentos nas condições e preços pactuados, especialmente no que diz respeito aos eventuais descontos decorrentes de desconformidades apuradas na prestação dos serviços, ficando esclarecido que estes somente serão aplicados a contar do segundo mês de vigência do Contrato.

16.5 Prestar as informações e esclarecimentos necessários à execução do objeto contratual pela CONTRATADA.

16.6 Documentar e notificar por escrito a CONTRATADA, a ocorrência de eventuais imperfeições, falhas ou irregularidades no curso da execução dos serviços, fixando prazo para a sua correção ou regularização.

16.7 Não permitir que pessoas estranhas à CONTRATADA examinem ou provoquem qualquer alteração nos serviços do presente objeto.

16.8 Observar e pôr em prática as recomendações técnicas feitas pela CONTRATADA relacionadas às condições de funcionamento, quando julgar pertinente ou oportuno.

16.9 Receber provisória e definitivamente o objeto do Contrato nas formas definidas.

16.10 A CONTRATANTE poderá pedir qualquer outro relatório referente às informações técnicas, que considere necessária a gestão;

16.11 Franquear à CONTRATADA acesso às suas instalações para fins de fiscalização, conformidade de segurança e adequações técnicas;

16.12 Destaca-se que o CONTRATANTE não aceitará, sob nenhum pretexto, a

transferência de responsabilidade da CONTRATADA para outras entidades, sejam fabricantes, representantes ou quaisquer outros;

16.13 A CONTRATANTE, no momento da implantação da solução, indicará as pessoas que poderão autorizar as referidas alterações. A CONTRATADA implementará mecanismos de autenticação que garantam a identificação destas pessoas.

16.14 As alterações das configurações ocorrerão em horários determinados pela CONTRATANTE.

17. DAS HABILITAÇÕES

17.1 Habilitação Jurídica:

a) Sociedade Limitada Unipessoal - SLU: ato constitutivo, estatuto ou contrato social em vigor inscrito no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhado de documento comprobatório do administrador, sendo assim enquadrada a sociedade identificada como Empresas Individual de Responsabilidade Limitada – EIRELI, na forma do art. 41, da Lei nº 14.195, de 26 de agosto de 2021;

b) Sociedade Empresária Estrangeira em funcionamento no País: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020 ou norma posterior que regule a matéria;

c) Sociedade Simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

d) Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

e) Quando cabível, os documentos apresentados devem estar acompanhados de todas as alterações ou da consolidação respectiva.

17.2 Habilitação Fiscal, Social e Trabalhista:

a) Regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social;

b) Regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

c) Declaração de que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

d) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

e) Prova de inscrição no cadastro de contribuintes estadual/distrital, relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

f) Prova de regularidade com a Fazenda do Estado do Rio de Janeiro, mediante a apresentação de:

I. Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa, expedida pela Secretaria de Estado de Fazenda; e

II. Certidão Negativa de Débitos em Dívida Ativa, ou Certidão Positiva com efeito de Negativa, para fins de participação em licitação, expedida pela Procuradoria Geral do Estado.

g) Regularidade com a Fazenda Estadual ou Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre, com a apresentação, conforme o caso, de:

I. **Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa, perante o Fisco estadual, pertinente ao Imposto sobre Operações relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual, Intermunicipal e de Comunicação - ICMS**, bem como de Certidão perante a Dívida Ativa estadual, podendo ser apresentada Certidão Conjunta em que constem ambas as informações;

II. **Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa do Imposto sobre Serviços de Qualquer Natureza** – ISS.

h) Caso o fornecedor seja considerado isento dos tributos estaduais <OU> municipais relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei;

i) Na hipótese de cuidar-se de microempresa ou de empresa de pequeno porte, na forma do art. 42 da Lei Complementar nº 123/2006, a documentação somente será exigida para efeito de assinatura do contrato, caso se sagre vencedora no certame;

j) Em sendo declarada vencedora do certame microempresa ou empresa de pequeno porte com débitos fiscais e trabalhistas, ficará assegurado, a partir de então, o prazo de 5 (cinco) dias úteis para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de negativas, na forma do art. 43, § 1º, da Lei Complementar nº 123/2006.

k) O prazo acima poderá ser prorrogado por igual período, a critério exclusivo da Administração Pública;

l) A não regularização da documentação no prazo estipulado implicará a decadência do direito à contratação, na forma do § 2º, do art. 43, da Lei Complementar nº 123/2016, sem prejuízo da aplicação das sanções previstas neste Edital.

17.3 Habilitação Econômico – Financeira:

a) Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor, caso se trate de pessoa jurídica, ou certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou da sede do fornecedor, caso se trate de sociedade simples;

b) Não será causa de inabilitação do licitante a anotação de distribuição de processo de recuperação judicial ou de pedido de homologação de recuperação extrajudicial.

c) Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, vedada a sua substituição por balancetes ou balanços provisórios.

c.1) Os documentos referidos acima limitar-se-ão ao último exercício social no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

c.2) Os fornecedores criados no exercício financeiro da contratação deverão atender a todas as exigências da habilitação e ficam autorizados a substituir os demonstrativos contábeis pelo balanço de abertura;

c.2.1) Poderá ser apresentado o balanço intermediário, caso autorizado por lei ou pelo contrato/estatuto social.

c.4) Para fins de habilitação econômico-financeira de sociedade empresária em recuperação judicial deverão ser considerados os valores constantes no Plano de Recuperação Judicial, homologado pelo Juízo competente, para fins de apuração dos índices contábeis previstos no edital.

d) Comprovação de patrimônio líquido mínimo de 10% (dez por cento) do valor total estimado da contratação ou do item pertinente.

17.4 Habilitação Técnica:

a) A Contratada deve apresentar: Atestado ou certidão de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, que comprove ter a licitante prestado de forma satisfatória, serviços análogos aos propostos no presente edital;

b) Atestado Comprovação de aptidão para o desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto desta licitação, por meio da apresentação de:

i. Atestado ou declaração de capacidade técnica de pessoa Jurídica Pública ou Privada, em nome da Licitante, que comprove a prestação de serviços de rede Corporativa IP MPLS ou SD-WAN para cliente abrangendo quantidade de circuitos previstos no Edital, velocidades e tecnologias.
ii. Atestado ou declaração de capacidade técnica, em nome da licitante, que comprove a prestação de serviços de acesso à internet abrangendo quantidade de tecnologias, acessos, velocidades e toda a infraestrutura necessária à prestação do serviço
iii. Declaração que comprove a capacidade de troca de tráfego do Backbone IP da Contratada com outros Backbones na banda especificada no Edital.
iv. Atestado ou declaração de capacidade técnica, em nome da licitante, que comprove os serviços de Segurança Gerenciada (MSS) PARA O LOTE 1;

c) Os recursos humanos a serem disponibilizados pela CONTRATADA deverão possuir as seguintes formações:

i. Diploma de Curso de Nível Superior na área de Tecnologia da Informação, Engenharia da Computação ou Análise de Sistemas;
ii. Certificação Avançada do fabricante para os equipamentos e softwares de rede fornecidos pela CONTRATADA;
iii. Conhecimento e experiência avançados em implementação de controles de segurança da informação de redes de telecomunicações, auditoria de logs, identificação de ameaças e vulnerabilidades, prevenção de ataques, e demais atribuições pertinentes;
iv. Experiência mínima de 5 anos, comprovada em carteira, atuando em redes de dados e infraestrutura de telecomunicações do fabricante da rede da CONTRATADA;
v. No ato da habilitação a licitante vencedora deverá apresentar declaração atestando que, **no momento da assinatura do contrato**, dispõe ou disporá de profissionais com os perfis e certificações descritos nesta alíenea.

d) Atestado ou declaração de capacidade técnica, em nome da licitante, que comprove a expertise para os serviços de Backbone Anti-DDoS nos moldes descrito neste termo.

e) A documentação que deverá ser apresentada visa garantir que as empresas vencedoras possuem capacidade plena para atendimento ao objeto, sem risco de incapacidade técnica para prestação dos serviços nos níveis exigidos na documentação técnica, o que na prática representaria parada completa no funcionamento da PGE-RJ em nível generalizado, que hoje depende da rede de telecomunicações em pleno funcionamento por conta dos sistemas corporativos e acesso à internet, no caso se a prestadora que se mostre incapaz de entregar o objeto na quantidade e qualidade exigidas.

18. DA FISCALIZAÇÃO

18.1 Por Fiscalização entende-se a atividade exercida de modo sistemático pela PGE e seus prepostos, objetivando a verificação do cumprimento das disposições contratuais, técnicas e administrativas, em todos os seus aspectos.

18.2 A PGE manterá, desde o início dos serviços, a seu critério exclusivo, uma equipe de Fiscalização constituída por profissionais habilitados que considerar necessários ao acompanhamento e controle dos trabalhos.

18.3 A CONTRATADA deverá facilitar, por todos os meios ao seu alcance, a ampla ação da Fiscalização, permitindo o acesso aos serviços em execução, bem como atendendo prontamente às solicitações que lhe forem efetuadas.

18.4 A atuação ou a eventual omissão da Fiscalização durante a realização dos trabalhos não poderá ser invocada para eximir a CONTRATADA da responsabilidade pela execução dos serviços.

18.5 A Fiscalização tem autonomia para exercer, dentre outras, as atividades descritas nos artigos 24 a 26 do Decreto Estadual nº 48.817/2023.

19. DAS CONDIÇÕES DE PAGAMENTO

19.1 O faturamento inicial será efetuado de acordo com os aceites das instalações nas localidades dos serviços – Tabela 1 - Tabela de Endereços das Localidades.

19.2 A fatura da prestação mensal dos serviços de acesso à rede deverá ser única e discriminada por tipo de serviço e acessos contratados, instalado e operacional (incluindo localidade, endereço, designação do circuito e velocidade de acesso).

19.3 A CONTRATADA deverá disponibilizar, mensalmente, o espelho da fatura detalhando os serviços referentes somente ao mês anterior, por meio eletrônico, em 10 (dez) dias úteis antes do faturamento para conferência e atesto.

19.4 A CONTRATADA deverá disponibilizar o Relatório de Nível de Serviço em meio digital e discriminado por unidade remota, localidade, tipo de serviço e acessos contratados.

19.5 A CONTRATADA só emitirá a segunda via das faturas após solicitação formal pela CONTRATANTE.

19.6 A CONTRATADA deverá disponibilizar as informações (tabelas e/ou demonstrativos) que identifiquem a metodologia empregada no cálculo dos custos de instalação e manutenção dos acessos e serviços.

19.7 As multas decorrentes das discrepâncias verificadas pelo não atendimento do nível de serviço acordado e o relatório do nível de serviço apurado, serão creditados na fatura do mês subsequente do respectivo órgão. Esses créditos deverão ser especificados por serviço e /ou ponto de acesso.

19.8 A CONTRATADA não poderá cobrar quaisquer valores para serviços de desinstalação.

19.9 Após a aceitação definitiva dos produtos e serviços, a CONTRATANTE autorizará a CONTRATADA a realizar a emissão da Nota Fiscal/Fatura, conforme as tabelas abaixo:

Tabela 1 - LOTE 1

ITEM	SERVIÇOS	UNIDADE	PRAZO	CONDIÇÕES DE PAGAMENTO
05	Plano de Projeto e Gerenciamento da Implantação completa da solução tecnológica	Unid.	Até 30 dias consecutivos do adimplemento do objeto	Parcela única - após a entrega e o aceite da comissão de fiscalização.
02	Licenciamento equipamento de segurança/SDWAN	Unid.	Até 30 dias consecutivos do adimplemento do objeto	Parcela única - após a entrega da licença do equipamento de segurança/SDWAN e o aceite da comissão de fiscalização
01 e 06	Rede IP Dedicado + SD-WAN Cluster (SEDE SD-WAN Principal)	Mensal	Até 30 dias consecutivos do adimplemento do objeto	**Pagamento realizado de forma mensal, em parcelas**. O primeiro pagamento mensal somente sera realizado apos o , após a realizacao de teste de verificacao do correto funcionamento do servico e do aceite pela Comissão de Fiscalização. Os demais pagamentos mensais serao realizados apos o aceite do correto funcionamento do servico pela comissao de fiscalizacao.
03, 08 até 22	Rede MPLS Principal SDWAN (Sede x Rede externa) + Links Principais Regionais	Mensal	Até 30 dias consecutivos do adimplemento do objeto	**Pagamento realizado de forma mensal, em parcelas**. O primeiro pagamento mensal somente sera realizado apos o , após a realizacao de teste de verificacao do correto funcionamento do servico e do aceite pela Comissão de Fiscalização. Os demais pagamentos mensais serao realizados apos o aceite do correto funcionamento do servico pela comissao de fiscalizacao.
04	Serviço de segurança MSS	Mensal	Até 30 dias consecutivos do adimplemento do objeto	**Pagamento realizado de forma mensal, em parcelas**. O primeiro pagamento mensal somente sera realizado apos o , após a realizacao de teste de verificacao do correto funcionamento do servico e do aceite pela Comissão de Fiscalização. Os

				demais pagamentos mensais serao realizados apos o aceite do correto funcionamento do servico pela comissao de fiscalizacao.

Tabela 2 - LOTE 2

ITEM	SERVIÇOS	UNIDADE	PRAZO	CONDIÇÕES DE PAGAMENTO
03	Plano de Projeto e Gerenciamento da Implantação completa da solução tecnológica	Unid.	Até 30 dias consecutivos do adimplemento do objeto	Parcela única - após a entrega e o aceite da comissão de fiscalização.
01	Rede IP Dedicado Secundário	Mensal	Até 30 dias consecutivos do adimplemento do objeto	**Pagamento realizado de forma mensal, em parcelas**. O primeiro pagamento mensal somente sera realizado apos o , após a realizacao de teste de verificacao do correto funcionamento do servico e do aceite pela Comissão de Fiscalização. Os demais pagamentos mensais serao realizados apos o aceite do correto funcionamento do servico pela comissao de fiscalizacao.
02, 4 até 19	Concentradora Rede Redundante MPLS com a Rede Externa + Links Redundantes Regionais	Mensal	Até 30 dias consecutivos do adimplemento do objeto	**Pagamento realizado de forma mensal, em parcelas**. O primeiro pagamento mensal somente sera realizado apos o , após a realizacao de teste de verificacao do correto funcionamento do servico e do aceite pela Comissão de Fiscalização. Os demais pagamentos mensais serao realizados apos o aceite do correto funcionamento do servico pela comissao de fiscalizacao.

19.10 A CONTRATADA deverá indicar na Nota Fiscal/Fatura o número do Contrato (empenho) firmado com a CONTRATANTE.

19.11 Satisfeitas as obrigações previstas nas cláusulas contratuais e cumpridos os requisitos constantes dos itens anteriores, a CONTRATADA deverá encaminhar as faturas à Comissão de Fiscalização da PGE/RJ para pagamento.

19.12 A Comissão de Fiscalização do Contrato terá o prazo de até 10 (dez) dias para atestar a nota fiscal e encaminhá-la para pagamento.

19.13 Os pagamentos serão efetuados por meio de crédito em conta corrente da

instituição financeira contratada pelo Estado do Rio de Janeiro – atualmente o Banco Bradesco S/A -, cujo número e agência deverão ser informados pela CONTRATADA até a assinatura do Contrato.

19.14 No caso de a CONTRATADA estar estabelecida em localidade que não possua agência da instituição financeira contratada pelo Estado do Rio de Janeiro, ou caso, verificada pelo Órgão Gestor a impossibilidade de a CONTRATADA, em razão de negativa expressa da instituição financeira contratada pelo Estado do Rio de Janeiro, abrir ou manter conta corrente naquela instituição financeira, o pagamento poderá ser feito mediante crédito em conta corrente de outra instituição. Nesse caso, eventuais ônus financeiros e/ou contratuais adicionais serão suportados exclusivamente pela CONTRATADA.

19.15 O prazo de pagamento das faturas será de 30 (trinta) dias, contados da data da entrada do documento de crédito na repartição competente, isenta de erros, previamente atestado por servidores, que não o ordenador de despesas, designados para a Fiscalização do Contrato.

19.16 O pagamento referente ao item concernente à prestação dos serviços será feito mensalmente, após a correlata disponibilização do serviço e da sua efetiva prestação.

19.17 Considera-se adimplemento o cumprimento da prestação com a execução do objeto, devidamente atestada pelo(s) agente(s) competente(s).

19.18 Caso se faça necessária a reapresentação de qualquer fatura por culpa da CONTRATADA, o prazo de 30 (trinta) dias ficará suspenso, prosseguindo a sua contagem a partir da data da respectiva reapresentação.

19.19 Os pagamentos eventualmente realizados com atraso, desde que, não decorram de ato ou fato atribuível à CONTRATADA, sofrerão a incidência de atualização financeira pelo Índice Nacional de Preços ao Consumidor – INPC, calculado e divulgado pelo Instituto Brasileiro de Geografia e Estatísticas – IBGE, e juros moratórios de 0,5% ao mês, calculado pro rata die.

19.20 Os pagamentos devidos à CONTRATADA não excederão os valores apresentados em sua proposta comercial e observarão eventuais descontos decorrentes da aplicação do Acordo de Níveis de Serviço – ANS, previsto neste instrumento.

19.21 Do Reajuste

Decorrido o prazo de 12 (doze) meses da data da apresentação da proposta ou do

orçamento a que essa proposta se referir, poderá a CONTRATADA fazer jus ao reajuste do valor contratual pelo Índice de Preços ao Consumidor Amplo - IPCA, apurado pelo Instituto Brasileiro de Geografia e Estatísticas (IBGE), que deverá retratar a variação efetiva do custo de execução do objeto contratual.

19.22 De acordo com o disposto no inciso I do art. 136 da Lei nº 14.133/2021, os reajustes ocorrerão por simples apostilamentos efetuados automaticamente e de ofício.

20. DA GARANTIA CONTRATUAL

20.1 Exigir-se-á da CONTRATADA, no prazo máximo de 10 (dez) dias consecutivos, contados da data constante no Memorando de Início de Serviços, a prestação de garantia durante toda a vigência do Contrato, em qualquer das modalidades previstas no art. 96, da Lei nº 14.133/2021, no montante de 5% (cinco por cento) do valor anual do Contrato, como condição de fiel cumprimento de todas as obrigações contratuais. A garantia prestada não poderá se vincular a outras contratações, salvo após sua liberação.

20.2 Caso o valor do Contrato seja alterado, nos termos do art. 125 da Lei nº 14.133/2021, a garantia deverá ser devidamente complementada pela CONTRATADA no prazo máximo de 72 (setenta e duas) horas, contadas da formalização do respectivo termo aditivo, de modo a manter o percentual de 5% (cinco por cento) do valor anual do Contrato.

20.3 O não atendimento a essa exigência poderá ensejar a suspensão dos serviços, a aplicação das penalidades contratuais e, se for o caso, a execução da garantia vigente, além de outras sanções cabíveis.

20.4 Nos casos em que valores de multas eventualmente aplicadas venham a ser descontados da garantia, seu valor original deverá ser recomposto no prazo máximo de 72 (setenta e duas) horas, sob pena de rescisão administrativa do Contrato.

21. DA FORMA DE SELEÇÃO E CRITÉRIO DE JULGAMENTO DA PROPOSTA

21.1 **Do prazo da Validade da Proposta**

21.1.1 O prazo de validade da proposta não será inferior a 60 (sessenta) dias

corridos, a contar da data de sua apresentação, podendo ser prorrogado, por igual período, salvo se houver justificativa para prazo diverso aceita pela Administração.

21.2 **Das Condições da Proposta**

21.2.1 O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

i. Valor Total do Lote;

ii. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência; e

iii. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

21.2.2 Devem ser apresentados em conjunto com a proposta os seguintes documentos:

a) Declaração de Garantia: Compromisso com a prestação de garantia técnica, incluindo manutenção on-site e suporte técnico especializado.

21.3 **Dos Critérios de Desempate**

21.3.1 Havendo eventual empate entre propostas, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

a) Disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

b) Avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos na Lei;

c) Desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento

d) Desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

e) Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

i. Empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

ii. Empresas brasileiras.

22. DA VISTORIA

22.1 É facultado aos interessados vistoriar as dependências da PGE/RJ, com o objetivo de conhecer o local e as condições para a prestação dos serviços, objeto desta contratação.

22.2 A opção pela vistoria constitui direito e ônus do interessado, com vistas à elaboração precisa e técnica de sua proposta, mas que não ostenta caráter eliminatório do certame para fins de exame de habilitação. Se, facultativamente, o interessado resolver não vistoriar os locais onde serão prestados os serviços, objeto da contratação, no caso de não contratação, não poderá alegar desconhecimento das condições dos locais como pretexto para eventual inexecução total ou parcial do Contrato ou atrasos em sua implementação.

22.3 O agendamento para a realização da vistoria poderá ser feito com a Gerência de Tecnologia da Informação da PGE/RJ, por meio do telefone (21) 2332-9401, no horário de 10h às 12h e 14h às 16h.

23. DA JUSTIFICATIVA DE PARCELAMENTO OU NÃO DA CONTRATAÇÃO

23.1 De acordo com o artigo 18, § 1°, inciso VIII da Lei 14.133/2021 o parcelamento ou não do objeto deve ser justificado. É sabido que o parcelamento do objeto em uma contratação é uma prática recomendada quando for tecnicamente viável, econômica e financeira vantajosa e, desde que não comprometa a execução do contrato.

No que tange a esta contratação, que compreende a contratação de empresa especializada para provimento de serviço de redes Multi Protocol Label Switching (MPLS) e circuitos de acesso à Internet com LINK DEDICADO, SDWAN, com o objetivo de otimizar o acordo, promover a competitividade, facilitar a gestão dos serviços e mitigar o risco de ponto único de falha havendo apenas um provedor de serviços, propõe-se a divisão do seu objeto em dois lotes distintos, quais sejam:

23.2. Lote 1 – Link dedicado de internet primário + SD-WAN + MSS + NGFW + DDoS

23.2.1 Este lote corresponde ao núcleo crítico da conectividade e da segurança da rede da PGE-RJ, fator determinante para a contratação conjunta desses serviços, uma vez que são tecnicamente integrados e interdependentes. Os serviços agregados (SD-WAN, MSS, NGFW e DDoS) devem estar totalmente compatíveis e interoperáveis com o link principal, exigindo que sejam fornecidos de forma integrada por uma única empresa ou consórcio, além dos seguintes resultados:

- Garantir a interdependência entre o link principal e os serviços de segurança e gerenciamento
- Facilitar a responsabilização contratual e o suporte técnico unificado
- Garantir performance e compatibilidade de ponta a ponta
- Reduzir riscos de incompatibilidade entre soluções de fornecedores distintos
- Gerenciar e garantir procedimentos de failover, switchover, HA e LB entre o link principal e o redundante.

23.3 Lote 2 – Link Secundário (Contingência)

23.3.1 O segundo lote trata exclusivamente da conectividade de contingência, ou seja, link secundário que funcionará como backup automático em caso de falha do principal. Este lote não exige a contratação conjunta de soluções avançadas como SD-WAN ou NGFW, permitindo que seja tratado de forma independente, além dos seguintes pontos:

- Permite maior abrangência de fornecedores, inclusive operadores menores ou regionais
- Amplia a concorrência no processo licitatório
- Evita dependência excessiva de um único fornecedor

24. DOS RECURSOS ORÇAMENTÁRIOS

24.1 Os recursos necessários à realização do objeto ora licitado correrão à conta do Fundo Especial da Procuradoria Geral do Estado do Rio de Janeiro – FUNPERJ e estarão vinculados à seguinte dotação orçamentária:

Programa de Trabalho	Natureza da Despesa	Fonte de Recurso
09610.1.03.126.0002.4918 (Operacionalização de tecnologia da informação e comunicação da PGE-RJ)	3.3.90.40.13 (Comunicação de dados e redes em geral)	1.501.230/1.760.232/2.501.230/2.753.232

25. DA SEGURANÇA DAS INFORMAÇÕES INSTITUCIONAIS, PROTEÇÃO DO DIREITO PATRIMONIAL E DA PROPRIEDADE INTELECTUAL

25.1 A CONTRATADA, por meio de seu representante legal, deverá assinar TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO (Anexo I), se comprometendo a manter sob o mais rigoroso sigilo todos dados, informações, documentos e especificações que venham a lhe ser confiados ou que venha a ter acesso em razão da execução dos serviços, não podendo, sob qualquer pretexto, revelá-los, divulgá-los, reproduzi-los ou deles dar conhecimento a quaisquer terceiros

25.2 Toda a documentação gerada na prestação dos serviços, objeto do presente Instrumento, com os dados sobre a solução da CONTRATANTE, bem como quaisquer outros dados inerentes ao ambiente computacional são de propriedade exclusiva da CONTRATANTE e devem ser mantidos em sigilo absoluto.

26. DA ESTIMATIVA DO VALOR DA CONTRATAÇÃO

26.1 A estimativa de valor da contratação foi elaborada com base em pesquisa realizada junto ao mercado, observando os critérios estabelecidos no artigo 23 da Lei nº 14.133/2021 e no Decreto 48.816/2023.

26.2 O valor estimado da contratação, para o período de 60 (sessenta) meses, encontra-se discriminado por lote conforme segue:

- **Lote 1:** R$ 4.283.780,00 (quatro milhões, duzentos e oitenta e três mil, setecentos e oitenta reais)
- **Lote 2:** R$ 1.964.216,00 (um milhão, novecentos e sessenta e quatro mil, duzentos e dezesseis reais)

O montante contempla a prestação de serviços de comunicação de dados, incluindo

conectividade entre a Sede e as Procuradorias Regionais, bem como acesso à internet.

A solução abrange links principais e de contingência, com infraestrutura totalmente independente entre os lotes, incluindo fornecimento, implantação, operação, gerenciamento e manutenção dos serviços, de modo a garantir conectividade segura, resiliente e de alta disponibilidade aos sistemas e serviços institucionais.

26.3 O custo estimado da contratação não possui caráter sigiloso, uma vez que sua divulgação é prevista pela legislação vigente, garantindo a transparência e o controle social sobre os atos administrativos.

27. DAS PENALIDADES E SANÇÕES ADMINISTRATIVAS

27.1 A inexecução dos serviços, total ou parcial, a execução imperfeita, a mora na execução ou qualquer inadimplemento ou infração contratual, sujeitará a CONTRATADA, sem prejuízo da responsabilidade civil ou criminal que couber, às sanções previstas na Lei n.º 14.133 /21 e demais normas pertinentes, assegurados, nos termos da lei, a ampla defesa e o contraditório.

27.2 A multa administrativa prevista no art. 156, II da Lei n. º 14.133/21, corresponderá ao valor de até 5% (cinco por cento) do Contrato, aplicada de acordo com a gravidade da infração e proporcionalmente às parcelas não executadas, e poderá ser aplicada cumulativamente a qualquer outra penalidade, não possuindo caráter compensatório, e o seu pagamento não exime a responsabilidade por perdas e danos das infrações cometidas.

27.3 Nas reincidências específicas, a multa corresponderá ao dobro do valor da que tiver sido inicialmente imposta, observando-se sempre o limite de 30% (trinta por cento), conforme preceitua o artigo 156, § 3º da Lei nº 14.133/21.

28. DAS CONSIDERAÇÕES FINAIS

28.1 O preço total proposto deverá considerar a consecução do objeto da presente contratação, englobando todos os custos diretos e indiretos.

28.2 Cabe à CONTRATADA consultar com antecedência os seus fornecedores quanto aos prazos de entrega, não cabendo, portanto, a justificativa de atraso do fornecimento devido ao não cumprimento da entrega por parte dos fornecedores.

28.3 Os casos omissos serão analisados pela Procuradoria Geral do Estado, à luz da legislação vigente, subsidiando posteriores decisões administrativas.

Rio de Janeiro, 30 de junho de 2026.

Responsável pela Demanda:
Wescley Barbosa de Paiva de Carvalho - ID: 50286820

Responsável Técnico:
Igor Almeida Borges - ID: 51210690

Responsável Administrativo:
Flávio Camara Carreiro - ID: 4323319-8

ANEXO I

TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO

PROCESSO ADMINISTRATIVO N.º	
PROCESSO LICITATÓRIO	
➢ **OBJETO**	
➢ **CONTRATO N.º**	

A PGE-RJ, com sede no Rio de Janeiro-RJ, inscrito no CNPJ sob o nº _____**,** e a **Empresa**_____, estabelecida à_____, CEP:_____, inscrita no CNPJ sob o nº_____, doravante denominada simplesmente **CONTRATADA**, representada neste ato pelo **Sr**_____, (cargo)_____ _____, (nacionalidade)_____, (estado civil)_____, (profissão) _____, portador da Cédula de Identidade nº_____, e do CPF nº _____, residente e domiciliado em_____, e, sempre que em conjunto referidas como PARTES para efeitos deste **TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO**, doravante denominado simplesmente TERMO.

CONSIDERANDO que, em razão do atendimento à exigência do Contrato Nº XX/20XX, celebrado pelas PARTES, doravante denominado **CONTRATO**, cujo objeto é a **<objeto do Contrato>**, mediante condições estabelecidas pelo CONTRATANTE;

CONSIDERANDO que o presente **TERMO** vem para regular o uso dos dados, regras de negócio, documentos, informações, sejam elas escritas ou verbais ou de qualquer outro modo apresentada, tangível ou intangível, entre outras, doravante denominadas simplesmente de **INFORMAÇÕES**, que a **CONTRATADA** tiver acesso em virtude da execução contratual;

CONSIDERANDO a necessidade de manter sigilo e confidencialidade, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse

da **PGE-RJ** de que a **CONTRATADA** tomar conhecimento em razão da execução do **CONTRATO**, respeitando todos os critérios estabelecidos aplicáveis às **INFORMAÇÕES**;

A PGE-RJ estabelece o presente **TERMO** mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste **TERMO** é prover a necessária e adequada **PROTEÇÃO ÀSINFORMAÇÕES** da **PGE-RJ**, principalmente aquelas classificadas como **CONFIDENCIAIS**, em razão da execução do **CONTRATO** celebrado entre as PARTES.

CLÁUSULA SEGUNDA - DAS INFORMACÕES CONFIDENCIAIS

Parágrafo Primeiro: As estipulações e obrigações constantes do presente instrumento serão aplicadas a todas e quaisquer **INFORMAÇÕES** reveladas pela **PGE-RJ**.

Parágrafo Segundo: A **CONTRATADA** se obriga a manter o mais absoluto sigilo e confidencialidade com relação a todas e quaisquer **INFORMAÇÕES** que venham a ser fornecidas pela **PGE-RJ**, a partir da data de assinatura deste **TERMO**, devendo ser tratadas como **INFORMACÕES CONFIDENCIAIS**, salvo aquelas prévia e formalmente classificadas com tratamento diferenciado pela **PGE-RJ**.

Parágrafo Terceiro: A **CONTRATADA** se obriga a não revelar, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que nenhum de seus diretores, empregados e/ou prepostos faça uso das **INFORMAÇÕES** da **PGE-RJ**.

Parágrafo Quarto: A **PGE-RJ**, com base nos princípios instituídos na Segurança da Informação, zelará para que as **INFORMAÇÕES** que receber e tiver conhecimento sejam tratadas conforme a natureza de classificação informada pela **CONTRATADA**.

CLÁUSULA TERCEIRA - DAS LIMITACÕES DA CONFIDENCIALIDADE

Parágrafo Único: As obrigações constantes deste **TERMO** não serão aplicadas às **INFORMAÇÕES** que:

I. Sejam comprovadamente de domínio público no momento da revelação ou após a revelação, exceto se isso ocorrer em decorrência de ato ou omissão das PARTES;

II. Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente **TERMO**;

III. Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo Estadual, somente até a extensão de tais ordens, desde que as

PARTES cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES ADICIONAIS

Parágrafo Primeiro: A **CONTRATADA** se compromete a utilizar as **INFORMAÇÕES** reveladas exclusivamente para os propósitos da execução do **CONTRATO**.

Parágrafo Segundo: A **CONTRATADA** se compromete a não efetuar qualquer cópia das **INFORMAÇÕES** sem o consentimento prévio e expresso da **PGE-RJ**.

I. O consentimento mencionado no Parágrafo segundo, entretanto, será dispensado para cópias, reproduções ou duplicações para uso interno das PARTES.

Parágrafo Terceiro: A **CONTRATADA** se compromete a cientificar seus diretores, empregados e/ou prepostos da existência deste **TERMO** e da natureza confidencial das **INFORMAÇÕES** da **PGE-RJ**.

Parágrafo Quarto: A **CONTRATADA** deve tomar todas as medidas necessárias à proteção das **INFORMAÇÕES** da **PGE-RJ**, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela **PGE-RJ**.

Parágrafo Quinto: Cada PARTE permanecerá como única proprietária de todas e quaisquer **INFORMAÇÕES** eventualmente reveladas à outra parte em função da execução do **CONTRATO**.

Parágrafo Sexto: O presente **TERMO** não implica a concessão, pela parte reveladora à parte receptora, de nenhuma licença ou qualquer outro direito, explícito ou implícito, em relação a qualquer direito de patente, direito de edição ou qualquer outro direito relativo à propriedade intelectual.

I. Os produtos gerados na execução do **CONTRATO**, bem como as **INFORMAÇÕES** repassadas à **CONTRATADA**, são única e exclusiva propriedade intelectual da **PGE-RJ**.

Parágrafo Sétimo: A **CONTRATADA** firmará acordos por escrito com seus empregados e consultores ligados direta ou indiretamente ao **CONTRATO**, cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente instrumento.

Parágrafo Oitavo: A **CONTRATADA** obriga-se a não tomar qualquer medida com

vistas a obter, para si ou para terceiros, os direitos de propriedade intelectual relativos aos produtos gerados e às **INFORMAÇÕES** que venham a ser reveladas durante a execução do **CONTRATO**.

CLÁUSULA QUINTA - DO RETORNO DE INFORMACÕES

Parágrafo Único: Todas as **INFORMAÇÕES** reveladas pelas PARTES permanecem como propriedade exclusiva da parte reveladora, devendo a esta retornar imediatamente assim que por ela requerido, bem como todas e quaisquer cópias eventualmente existentes.

I. A **CONTRATADA** deverá devolver, íntegros e integralmente, todos os documentos a ela fornecida, inclusive as cópias porventura necessárias, na data estipulada pela **PGE-RJ** para entrega, ou quando não mais for necessária a manutenção das Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias.

II. A **CONTRATADA** deverá destruir quaisquer documentos por ela produzidos que contenham Informações Confidenciais da **PGE-RJ**, quando não mais for necessária a manutenção dessas Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades previstas neste Termo.

CLÁUSULA SEXTA - DA VIGÊNCIA

Parágrafo Único: O presente **TERMO** tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até 5 (cinco) anos após o término do Contrato.

CLÁUSULA SÉTIMA - DAS PENALIDADES

Parágrafo Único: A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na **RESCISÃO DO CONTRATO** firmado entre as PARTES. Neste caso, a **CONTRATADA**, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela **PGE-RJ**, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 155 da Lei nº. 14.133/2021.

CLÁUSULA OITAVA - DAS DISPOSICÕES GERAIS

Parágrafo Primeiro: Este **TERMO** constitui vínculo indissociável ao **CONTRATO**, que é parte independente e regulatória deste instrumento.

Parágrafo Segundo: O presente **TERMO** constitui acordo entre as PARTES, relativamente ao tratamento de **INFORMAÇÕES**, principalmente as **CONFIDENCIAIS**, aplicando-se a todos e quaisquer acordos futuros, declarações, entendimentos e negociações escritas ou verbais, empreendidas pelas PARTES emações feitas direta ou indiretamente.

Parágrafo Terceiro: Surgindo divergências quanto à interpretação do pactuado neste **TERMO** ou quanto à execução das obrigações dele decorrentes, ou constatando-se nele a existência de lacunas, solucionarão as PARTES tais divergências, de acordo com os princípios da legalidade, da equidade, da razoabilidade, da economicidade, da boa-fé, e, as preencherão com estipulações que deverão corresponder e resguardar as **INFORMAÇÕES** da **PGE-RJ.**

Parágrafo Quarto: O disposto no presente **TERMO** prevalecerá sempre em caso de dúvida, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos legais conexos relativos à **CONFIDENCIALIDADE DE INFORMAÇÕES**.

Parágrafo Quinto: A omissão ou tolerância das PARTES, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo.

CLÁUSULA NONA - DO FORO

Parágrafo Único: Fica eleito o foro da Cidade do Rio de Janeiro, Comarca da Capital, para dirimir quaisquer dúvidas oriundas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, a **CONTRATADA** assina o presente **TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO**, em 2 (duas) vias de igual teor e um só efeito, na presença de duas testemunhas.

Rio de Janeiro/RJ,____de_____de 20__.

_____

Nome do Diretor ou representante legal da empresa

Cargo e CPF

_____	_____
Gestor do Contrato	Fiscal Técnico do Contrato

ANEXO II

PLANO DE TRABALHO: 999/AAAA

1. OBJETIVO

< Descrição do objetivo do plano de trabalho>

2. DETALHAMENTO DOS PRODUTOS FATURÁVEIS

<Detalhar os produtos/serviços a serem entregues e que estão associados ao faturamento.>

2.1 ATIVIDADE 1

<Descrição da Atividade (ex: Criação do campo Login Rede na tela de servidores do sistema XXX-PGE, para posteriormente uma carga popular o objeto schema.tabela.).>

2.1.1 DATA/PERÍODO DE EXECUÇÃO ESTIMADO:

<De dd/mm/aaa a dd/mm/aaa ou Dia>

Pré-requisitos	Evidências da entrega
<Identificar impeditivos ao início da atividade.	

3. APROVAÇÃO

Rio de Janeiro, **dd de <mês> de AAAA**.

Responsável Técnico pelo Plano de Trabalho:	Preposto do Contrato:
Nome **CPF** **CONTRATADA**	**Nome** **CPF** **CONTRATADA**

ANEXO III

Plano de Projeto (PP)			
Nome do Projeto:		**Contrato:**	
Patrocinador:		**Gerente:**	

1. JUSTIFICATIVA

<Descrever a justificativa, contendo um breve histórico, as motivações e os benefícios que levaram o órgão a propor o presente projeto.

2. OBJETIVO

< Descrição concreta do que o projeto quer alcançar, uma posição estratégica, um resultado a ser obtido, um produto a ser produzido ou um serviço a ser realizado. Os objetivos devem ser específicos, mensuráveis, realizáveis, realísticos e baseados no tempo.

3. DECLARAÇÃO DO ESCOPO

<Descrever a declaração do escopo, que inclui as principais entregas, fornece uma base documentada para futuras decisões do projeto e para confirmar ou desenvolver um entendimento comum do escopo do projeto entre as partes interessadas. Definir os procedimentos para aceitação formal das entregas concluídas do projeto. Descrever cada entrega do projeto em detalhes.

4. ESTRUTURA ANALÍTICA DE PROJETO (EAP)

<Inserir a imagem da EAP. A EAP é uma decomposição hierárquica orientada à entrega do trabalho a ser executado pela equipe do projeto para atingir os objetivos do projeto e criar as entregas necessárias.>

5. DICIONÁRIO DA EAP

<Descrever para cada entrega da EAP uma descrição do trabalho necessário para realizá-la.>

Entrega	Descrição da entrega

6. NÃO ESCOPO

<Descrever o que está excluído do projeto, para evitar que uma parte interessada possa supor que um produto, serviço ou resultado específico é um produto do projeto.

7. PREMISSAS

<Descrever as premissas do projeto. As premissas afetam todos os aspectos do planejamento do projeto e fazem parte da elaboração progressiva do projeto. Frequentemente, as equipes do projeto identificam, documentam e validam as premissas durante o processo de planejamento. Geralmente, as premissas envolvem um grau de risco.

8. RESTRIÇÕES

<Descrever as restrições do projeto. Uma restrição é uma limitação aplicável, interna ou externa ao projeto, que afetará o seu desempenho ou de um processo.

9. CRONOGRAMA DE MARCOS

<Inserir a imagem do cronograma de marcos. Caso não tenha ferramenta de gerenciamento de cronograma, preencher a tabela abaixo com os marcos e as respectivas datas.>

Nome do marco	**Data**

10. PLANO DE GERENCIAMENTO DA QUALIDADE

<Identificar os requisitos e padrões da qualidade do projeto e suas entregas.

Documentar o formato do gerenciamento e controle das conformidades com os requisitos de qualidade ao longo de todo o projeto.>

Entrega	Critérios de qualidade

11. PLANO DE GERENCIAMENTO DOS RECURSOS

<O Plano de Recursos contém os requisitos de recursos físicos e de equipe necessários para a conclusão do projeto.>

11.1. ORGANOGRAMA DO PROJETO

<Inserir a imagem do organograma do projeto. O organograma do projeto é a representação gráfica dos membros da equipe do projeto e seus inter-relacionamentos no projeto.>

11.2. EQUIPE DO PROJETO

<Definir os membros que irão compor a equipe do projeto.

Nome	Órgão	Cargo / Função	Telefone(s)	E-mail

11.3. PAPÉIS E RESPONSABILIDADES

<Definir o papel e a responsabilidade para o grupo do projeto.>

Nome	Papel	Responsabilidades

12. PLANO DE GERENCIAMENTO DA COMUNICAÇÃO

<O Plano de Comunicação documenta como as informações do projeto chegarão às partes interessadas de forma clara e no tempo adequado.>

12.1. DESCRIÇÃO DO PROCESSO DE COMUNICAÇÃO

<Descrever o processo de comunicação necessário para garantir a geração, coleta, distribuição, armazenamento, recuperação e destinação final das informações sobre o projeto. Este item pode conter informações, como: onde os arquivos do projeto serão armazenados, definição de nomenclatura de arquivos, se as reuniões deverão ser registradas em ata, necessidade de publicação de documento do Diário Oficial, modelos de relatórios/formulários que devem ser utilizados no projeto, etc.>

12.2. EVENTOS DE COMUNICAÇÃO

Evento	Objetivo	Responsável (is)	Partes Interessadas	Meio de Comunicação	Periodicidade	Formato	Materiais Relacionados
	<Preencher a tabela abaixo com as informações dos eventos de comunicação do projeto.>						

13. PLANO DE GERENCIAMENTO DO RISCO

<O Plano de Risco descreve como o gerenciamento de risco será estruturado e realizado.>

13.1. RISCOS

<Identificar eventos ou condições incertas que, se ocorrerem, provocarão efeitos positivos ou negativos nos objetivos do projeto.

13.2. DESCRIÇÃO DO PROCESSO DE GERENCIAMENTO DE RISCOS

<Descrever o processo de gerenciamento de risco do projeto. >

14. PLANO DE ENGAJAMENTO DAS PARTES INTERESSADAS

< Descrever o plano para envolver as partes interessadas do projeto, com base em suas necessidades, expectativas e interesses.>

15. CRONOGRAMA DE EXECUÇÃO

<Criar o cronograma com as tarefas, duração, sequência, datas planejadas de início e término para a conclusão das atividades, interdependências das atividades e marcos do projeto.>

16. PLANO DE GERENCIAMENTO DAS MUDANÇAS

< Descreve o processo para gerenciar todas as mudanças do projeto, documentar o seu impacto e formalizar as alterações>

17. PLANO DE GERENCIAMENTO DO CRONOGRAMA

<Descreve as políticas, os procedimentos e a documentação para o planejamento, desenvolvimento, gerenciamento, execução e controle do cronograma do projeto (ex: acompanhamento semanal entre o planejado (linha de base salva) com o realizado, comunicação dos indicadores através de Status Report semanal e etc.).

18. DESCRIÇÃO DO PROCESSO DE HOMOLOGAÇÃO DAS ENTREGAS

<Descreve o processo de homologação do produto, os componentes e artefatos a serem homologados, quem são os envolvidos da equipe técnica, da parte do cliente e/ou usuários e a documentação comprobatória da homologação. Estas informações podem ser agrupadas nas subseções a seguir.

19. O PROCESSO DE HOMOLOGAÇÃO

<O processo de homologação descreve as etapas a serem executados para aprovação dos produtos do projeto. Esses produtos podem envolver, por exemplo, a documentação do usuário, os artefatos produzidos durante o desenvolvimento do produto, os testes de aceitação, etc.>

19.1. EQUIPE DE HOMOLOGAÇÃO

<Descrever os participantes do processo de homologação: técnicos responsáveis pelos testes, pela documentação e pelos artefatos gerados, os gerentes de ambas as partes e demais stakeholders que se façam necessários. Indicar quem são os

responsáveis por criar e por homologar cada artefato.>

19.2. PRODUTOS A SEREM HOMOLOGADOS

<Lista quais produtos serão submetidos à homologação. Por exemplo, a documentação de análise e projeto, especificações dos casos de uso, os componentes da aplicação, manuais de instalação, utilização do produto e etc.>

19.3. DOCUMENTAÇÃO COMPROBATÓRIA

<Especifica os documentos que constituirão o termo de homologação do produto.>

20. APROVAÇÃO

Rio de Janeiro, dd de <mês> de AAAA.

Responsável Técnico pelo Plano de Projeto:	Preposto do Contrato:
_____ **Nome CPF** **CONTRATADA**	_____ **Nome CPF** **CONTRATADA**