1 OBJETO (ART. 18, § 3º, I)

Registro de Preços para contratação de Serviços Especializados de Comunicação Digital, incluindo links remotos com segurança da informação ponta a ponta e serviço de WiFi gerenciado, para as comarcas do Poder Judiciário do Estado da Bahia PJBA, respeitados os níveis de serviço especificados no presente instrumento, pelo período de 24 (vinte e quatro) meses.

2 FUNDAMENTAÇÃO DA CONTRATAÇÃO (ART. 18, § 3º, II)

2.1 Motivação (Art. 18, § 3º, II, a)

O Poder Judiciário do Estado da Bahia (PJBa) mantém em atividade uma Rede Corporativa com o objetivo de permitir que os computadores das suas Unidades, tanto da capital como do interior do estado, possam se conectar ao seu Data Center e à Internet.

No total, centenas de computadores, na capital e no interior, conectados ao Data Center, viabilizam o acesso aos sites e sistemas internos e também à internet, sendo tal solução de fundamental importância para as atividades dessas unidades.

Atualmente os serviços de interligação das unidades judiciárias do interior do estado são prestados pela operadora Telemar Norte Leste através do contrato emergencial nº 020/19-S, com vigência de 180 (cento e oitenta) dias, expirando em 30/09/2019.

Tendo em vista a proximidade da expiração desse contrato, é de fundamental importância a abertura de processo licitatório para nova contratação, de forma a manter a continuidade dos serviços, possibilitando o acesso das unidades do interior à Rede Corporativa e garantindo a segurança e integridade dos dados trafegados nesta rede.

2.2 Objetivos (Art. 18, § 3º, II, b)

- Gerenciar e dar suporte tecnológico na implantação e operacionalização de todos os serviços de comunicação de dados contratados de forma segura.
- Oferecer solução de segurança da informação ponta a ponta, tanto durante o trânsito das informações a partir das diversas unidades quanto na centralização das comunicações no *Data Center* do CONTRATANTE.
- Assegurar que os incidentes e problemas sejam prontamente identificados e solucionados.
- Oferecer serviço de infraestrutura de acesso.
- Manter os enlaces de dados.
- Disponibilizar informações dos serviços contratados, relatórios, status e utilização da rede.
- Manter acessibilidade aos sistemas.
- Provisionar serviço de WiFi gerenciado.

2.3 Benefícios (Art. 18, § 3º, II, c)

A eficácia da solução será alcançada garantindo-se ao jurisdicionado a disponibilidade e continuidade do acesso à rede corporativa em todo o interior do Estado.

A eficiência na prestação dos serviços será dada pelo apoio técnico necessário por parte da CONTRATADA, a qual deverá garantir a segurança de rede na comunicação entre as unidades do interior e o *Data Center* e solucionar quaisquer demandas técnicas relacionadas aos serviços estabelecidos, dentro dos prazos acordados, incluindo falhas e serviços de manutenção.

Todos esses benefícios, espera-se, deverão prover um acesso de qualidade à rede corporativa e minimizar a probabilidade de interrupção.

2.4 Alinhamento Estratégico (Art. 18, § 3º, II, d)

O presente processo encontra aderência estratégica no item 15 do Planejamento Estratégico do Poder Judiciário do Estado da Bahia para o período de 2015-2020: "*Perspectiva dos Recursos*", macro desafio "*Melhoria da Infraestrutura e da TIC*", nos seguintes objetivos:

- "*Garantir a Infraestrutura de TIC apropriada às atividades judiciais, extrajudiciais e administrativ*
o qual encontra-se alinhado com o indicador homônimo, item 47 na Cesta de Indicadores.
- "*Garantir a Disponibilidade de sistemas essenciais de TIC*", alinhado com o indicador homônimo, item 48 na Cesta de Indicadores.
- Esta demanda está prevista na Relação de Serviços constante do Plano de Contratações de STIC exercício de 2019 da SETIM / PJBA , em observância à Resolução nº182/2013, Art. 7º,§ 4º.

2.5 Referência aos Estudos Preliminares (Art. 18, § 3º, II, e)

Este Termo de Referência foi elaborado com base nas informações contidas no Documento de Oficialização da Demanda (DOD) encaminhado pela Coordenação de Produção e Comunicação (CPROD) para a Secretaria de Tecnologia da Informação e Modernização (SETIM) e no conteúdo dos Estudos Preliminares desenvolvidos pela equipe de planejamento da contratação. Todos os documentos encontram-se no Processo Administrativo TJ-ADM-2018/56286, em tramitação no SIGA.

2.6 Relação entre a Demanda Prevista e a Contratada (Art. 18, § 3º, II, f)

O serviço a ser contratado, em conformidade com os requisitos definidos, deverá atender integralmente à demanda, visto que contempla todos os serviços necessários para manter o acesso das unidades do interior ao *Data Center* do Tribunal de Justiça.

O dimensionamento da quantidade de circuitos encontra-se detalhado no tópico a seguir.

As solicitações de instalação serão feitas de acordo com a necessidade do CONTRATANTE, não necessariamente significando a contratação da totalidade dos circuitos até o final do contrato. As informações que complementam a configuração dos circuitos, tais como Unidade, nome e informações de contato do responsável no local de instalação, ligação ao *backbone*, informações adicionais, número de classes e configuração do roteador (SNMP, ROTAS, Endereço IP da LAN) e DHCP (Faixa de Exclusão, *Gateway*, Máscara, IP e DNS) serão entregues à CONTRATADA após assinatura do Contrato.

2.6.1 Quantificação e Distribuição:

Os quadros a seguir especificam a quantidade de circuitos, por tipo, a serem disponibilizadas sob demanda durante a vigência contratual, cujas taxas serão atualizadas no decorrer do contrato até a configuração disposta na última coluna, onde não haverá mais circuitos de 2 Mbps.

Os quantitativos são meramente estimativos, não constituindo compromisso de o CONTRATANTE requisitar efetivamente todos os circuitos aqui estimados.

Do mesmo modo, a distribuição entre o primeiro e o segundo ano de contrato visa apenas estabelecer um parâmetro uniforme para a comparação das propostas e determinação do valor global. Sendo um contrato sob demanda, poderão ser demandados novos circuitos ou atualizada a velocidade dos existentes em qualquer momento do contrato. Da mesma maneira, a requisição de serviços complementares poderá variar sob demanda ao longo do contrato.

Em todos os casos, os quantitativos efetivamente usados poderão variar, para mais ou para menos, ao longo do contrato, desde que o valor global do contrato não seja ultrapassado.

Caso necessidades futuras exijam alterar o valor global, o mesmo poderá ser aumentado ou reduzido nos limites definidos pela legislação em vigor.

Evolução das necessidades conforme a Taxa e Nível de Segurança			
Links Remotos	**Demanda inicial[1]**	**Previsão 1º ano[2]**	**Previsão 2º ano**
LR Básico 10 Mbps	---	10	15
LR Básico 20 Mbps	---	8	22
LR Básico 50 Mbps	---	15	20
LR Básico 100 Mbps	---	1	2
LR Básico 200 Mbps	---	0	1
Total Básicos ⇨	***---***	***34***	***60***
LR Avançado 2 Mbps + SLR[3] + SDC[4]	49	60	30

1 Entende-se por demanda inicial a substituição dos circuitos atualmente em uso. Posteriormente, ao longo do contrato, esses circuitos poderão sofrer desativação, upgrade, downgrade ou mudança de endereço respondendo a solicitação do CONTRATANTE, bem como poderá ser solicitada a instalação de novos circuitos em unidades ainda não contempladas.

2 As colunas Previsão 1º Ano e Previsão 2º Ano são meramente informativas, apresentando a estimativa atual de alterações quantitativas ao longo desses períodos sem, no entanto, constituir compromisso efetivo de o CONTRATANTE requisitar tais alterações nos quantitativos previstos.

LR Avançado 5 Mbps + SLR + SDC	174	150	105
LR Avançado 10 Mbps + SLR + SDC	7	55	120
LR Avançado 20 Mbps + SLR + SDC	16	26	36
LR Avançado 50 Mbps + SLR + SDC	2	4	7
LR Avançado 100 Mbps + SLR + SDC	---	0	2
LR Avançado 200 Mbps + SLR + SDC	---	0	1
Total Avançados ⇨	***248***	***295***	***301***
LR Plus 5 Mbps + SLR + SDC	---	5	8
LR Plus 10 Mbps + SLR + SDC	---	5	8
LR Plus 20 Mbps + SLR + SDC	---	5	10
LR Plus 50 Mbps + SLR + SDC	---	1	2
LR Plus 100 Mbps + SLR + SDC	---	0	1
LR Plus 200 Mbps + SLR + SDC	---	0	1
Total Plus ⇨	***---***	***16***	***30***
Total de Links Remotos ⇨	**248**	**345**	**391**

Serviço de Wi-Fi Gerenciado	**Demanda inicial**	**1º ano**	**2º ano**
Unidades judiciárias a serem atendidas	---	20	30
Total Wi-Fi Gerenciado ⇨	**---**	**20**	**30**

2.7 Análise do Mercado de TIC (Art. 18, § 3º, II, g)

2.7.1 Soluções disponíveis no mercado (Art. 18, § 3º, II, g)

Não existem soluções eficazes, a não ser a terceirização dos serviços mediante a contratação de operadoras privadas de telecomunicações. Soluções próprias, tais como a utilização de links de rádio ou fibras privadas, só têm aplicação em pequenas distâncias, tornando-se ineficazes ou excessivamente onerosas para interligar unidades remotas.

Alternativamente, existe a possibilidade de criação de redes próprias. Porém, ela exige um alto investimento inicial, dificilmente acessível para órgãos isolados como o Tribunal de Justiça. Uma tentativa de viabilizar esse investimento é a Rede Nacional de Ensino e Pesquisa (RNP), uma infraestrutura avançada e compartilhada iniciada pelos Ministérios da Ciência e Tecnologia e da Educação e sob a denominação de ReMeSSa (Rede Metropolitana de Salvador) gestionada localmente pela Universidade Federal da Bahia, com a qual o Tribunal de Justiça já tem um convênio para atendimento às unidades de Salvador. Porém, ainda não tem cobertura suficiente no interior do Estado da Bahia.

2.7.2 Soluções Contratadas por outros Órgãos (Art. 18, § 3º, II, g)

Entre as mais recentes, foram encontradas as seguintes contratações de serviços de comunicação de dados com alguma similaridade aos serviços demandados neste Termo de Referência:

- Órgão: Ministério da Agricultura, Pecuária e Abastecimento PE 23/2017
  Objeto: Contratação de serviços de acesso à internet e comunicação de dados via MPLS (Multi Protocol Label Switching) para a rede WAN (Wide Area Network) do Ministério da Agricultura, Pecuária e Abastecimento MAPA, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos(Lote 2).
  Vigência: 12 meses
  Número de circuitos: 58
  Valor global: R$ 808.210,34
- Órgão: Banco Central do Brasil PE 85/2017
  Objeto: Prestação de serviços de comunicação multimídia por meio de uma rede MPLS/VPN.
  Vigência: 36 meses
  Número de circuitos: 70
  Valor global: R$ 699.520,86
- Órgão: Justiça Federal de 1ª Instância PE 17/2017
  Objeto: Serviços de Telecomunicações para implantação (instalação e configuração), operação, manutenção e gerenciamento de uma Rede IP Multisserviços, com uso da Tecnologia MPLS,

3 SLR – Segurança do Link Remoto, conforme definido no item 4.6.8.
4 SDC – Segurança de Acesso ao Data Center, conforme definido no item 4.6.9.

objetivando a interligação das redes locais de computadores da Seção Judiciária do Tocantins Palmas e das Subseções Judiciárias de Araguaína e Gurupi-TO.
Vigência: 12 meses
Número de circuitos: 3
Valor global: R$ 300.000,00

As duas primeiras contratações diferem notavelmente do contexto deste Termo de Referência, pois têm escopo de abrangência nacional. A primeira, PE 23/2017, Lote 2, consiste na contratação de serviços de comunicação entre Brasília e 58 (cinquenta e oito) unidades regionais localizadas em todos os estados do país e as taxas são limitadas a 8, 16 e 32 Mbps. A segunda PE 85/2017, embora possua também abrangência em todo o território nacional, define a vigência contratual de 36 meses, enquanto a contratação do TJBA define 24 meses. Já a terceira contratação, a PE 17/2017, possui escopo mais restrito e contrata apenas os circuitos de comunicação para 3 (três) localidades: Palmas, Araguaína e Gurupi, como se pode observar no objeto, nas taxas de 15 e 30 Mbps.

Por outra parte, todas essas contratações tratam apenas dos serviços de comunicação, podendo, em alguns casos, incluir segurança na ponta (no link remoto). Porém, nenhuma delas inclui o serviço de segurança ponta a ponta (desde o data center até o link remoto e vice-versa). Mesmo a Rede Governo III, que até 2018 atendeu às necessidades do Tribunal de Justiça, e o contrato emergencial atualmente em curso, só contemplam segurança na ponta.

Considerando as diferenças de escopo com essas contratações, pode-se perceber a ineficácia de uma comparação de valores entre eles e sua utilização como valores de referência para esta contratação.

2.7.2 Definição e Justificativa da Solução Adotada (Art. 18, § 3º, II, g)

O Modelo Funcional desta contratação compreende a execução de uma solução integrada para todas as unidades do interior do Estado da Bahia, disponibilizando infraestrutura corporativa convergente e segura para comunicação de dados, voz e vídeo com tecnologia digital, acesso à Internet, serviços de Gerenciamento, Service-Desk e de TIC, e manutenção e operação dos recursos envolvidos na solução.

O objeto desse Termo será a Contratação de Solução de Comunicação de dados, voz e vídeo estruturada em rede privativa com segurança e serviços adicionais. Os elementos deste termo podem ser divididos em:

- Ponto Principal: Backbone da rede, localizado no *Data Center* do Tribunal de Justiça, onde serão instalados equipamentos de conectividade de rede, Internet e segurança de data center.
- Links Remotos (LRs): Circuitos de comunicação de dados e acesso banda larga que interligarão as unidades operacionais ao *Data Center*. Os LRs deverão possuir solução de segurança na ponta.
- Solução de Gerenciamento: Serviços de caráter obrigatório para monitoramento e relatórios dos circuitos e equipamentos dos Pontos Principais e dos Link Remotos.
- Service Desk: Serviço de caráter obrigatório para atuar como canal de relacionamento para registro de incidentes e solicitações de serviço, atuando como ponto único de contato (PUC).
- Serviços de WiFi Gerenciado: Complementares aos Link Remotos, porém de contratação opcional.

O diagrama do Modelo Funcional é mostrado na Figura 1.

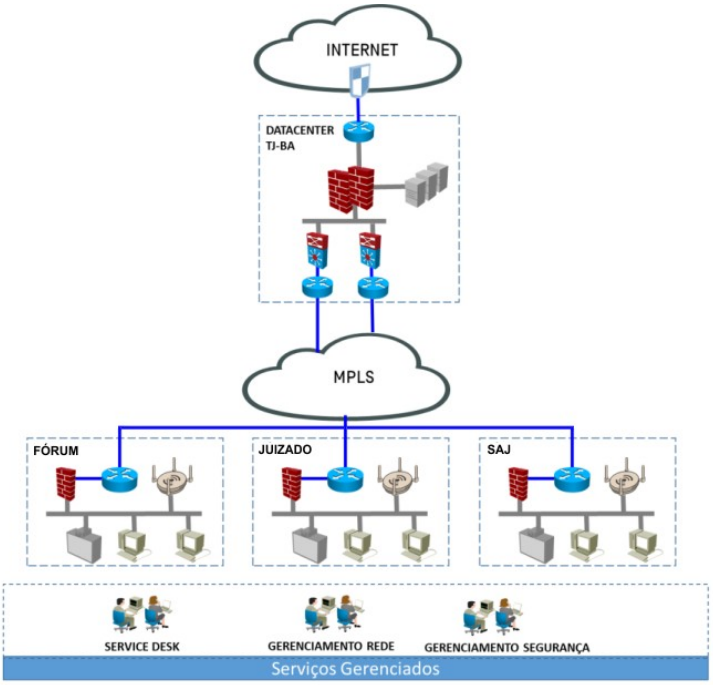

Figura 1 Modelo Funcional

2.8 Natureza do Objeto (Art. 18, § 3º,II, h)

Trata-se de contratação de serviços continuados e de natureza comum durante a vigência do contrato, podendo se estender por mais de um exercício financeiro.

2.9 Parcelamento e Adjudicação do Objeto (Art. 18, § 3º, II, i)

Como se trata do mesmo serviço para todas as unidades do interior do estado, a concentração em um mesmo contrato mostra-se mais vantajosa, tanto no aspecto econômico como no operacional.

No aspecto econômico, a vantagem se apresenta na formação de preços, pois o licitante poderá construir uma logística mais eficiente na alocação dos recursos humanos e de hardware.

Do ponto de vista operacional o contrato único representa maior eficiência de gestão por parte do CONTRATANTE.

Considerando a existência de lote único, a adjudicação será por um fornecedor apenas. No entanto, a fim de preservar e garantir a competitividade do certame, serão admitidas a formação de consórcio e a subcontratação.

2.9.1 Consórcio

A participação de interessados sob a forma de Consórcio deverá respeitar o disposto no art. 105 da Lei Estadual nº 9.433/05. As empresas consorciadas deverão participar de apenas um Consórcio, estendendo-se tal restrição às empresas pertencentes a um mesmo grupo econômico (coligadas, controladas ou controladoras).

A empresa líder do Consórcio deverá apresentar o instrumento de constituição ou de compromisso de constituição do Consórcio, o qual deverá obedecer aos seguintes requisitos:

1. Conter indicação da empresa líder do Consórcio, conforme o disposto no artigo 105, parágrafo 5º, da Lei Estadual nº 9.433/2005, que será responsável perante o CONTRATANTE, pelo cumprimento das obrigações das consorciadas.
2. Conferir, à empresa líder, amplos poderes para representar as consorciadas no procedimento licitatório e no Contrato, quanto ao preço do Serviço, dar quitação, responder administrativa e judicialmente, inclusive receber notificação, intimação e citação.
3. Regular a participação de cada consorciada na execução dos serviços, bem como a participação percentual de cada consorciada no Preço.
4. Regular a responsabilidade de cada consorciada quanto ao cumprimento das obrigações contratuais e/ou técnicas, devendo as integrantes do Consórcio ser obrigatoriamente responsáveis solidárias pelo cumprimento de todas as obrigações decorrentes do procedimento licitatório e do Contrato.

5. Conter compromisso tácito dos consorciados de que não terão sua constituição ou composição alteradas ou modificadas sem a prévia e expressa anuência da Administração, até o cumprimento do objeto da licitação ou enquanto perdurar o contrato de prestação de serviço.

2.9.2 Subcontratação

A Subcontratação será admitida, eximindo-se CONTRATANTE de quaisquer compromissos assumidos pela CONTRATADA com a(s) SUBCONTRATADA(S). Para tanto, deverão ser respeitados os seguintes requisitos:

1. Será permitida a subcontratação apenas de atividades acessórias e complementares, desde que isso não implique em transferência da prestação do serviço contratado, em perda de economicidade ou em detrimento de sua qualidade.
2. Entendem-se como atividades acessórias e complementares aquelas atividades de apoio para montagem ou manutenção do item de serviço.
3. Será permitida a subcontratação de última milha de acesso terrestre (fibra ótica ou par metálico) no limite de 10% do total de links.
4. Será permitida a subcontratação de acesso satélite no limite de 5% dos pontos conectados para cada órgão.
5. 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.

2.10 Modalidade, Tipo de Licitação e Critérios de Aceitabilidade da Proposta (Art. 18, § 3º, II, j)

Considerando a natureza comum do objeto, sugere-se o emprego da modalidade de Pregão Eletrônico.

2.10.1 Limites Máximos de Preços (Art. 18, § 3º, II, j)

Considerando o orçamento estimado apurado nos Estudos Preliminares desta contratação, tomando como base as propostas apresentadas por fornecedores, o limite máximo de preço aceitável será de R$ 44.646.624,00 (quarenta e quatro milhões, seiscentos e quarenta e seis mil, seiscentos e vinte e quatro reais) pelo período de 24(vinte e quatro) meses.

Deverão ser respeitados, ainda, os limites referenciais por item conforme detalhamento abaixo:

Item	Descrição	Unidade	Limite de Preço
1	LR Básico 10 Mbps	LR/Mês[5]	1.592,53
2	LR Básico 20 Mbps	LR/Mês	2.031,04
3	LR Básico 50 Mbps	LR/Mês	3.306,37
4	LR Básico 100 Mbps	LR/Mês	4.785,71
5	LR Básico 200 Mbps	LR/Mês	7.789,19
6	LR Avançado 2 Mbps + SLR[6] + SDC[7]	LR/Mês	3.902,65
7	LR Avançado 5 Mbps + SLR + SDC	LR/Mês	4.395,44
8	LR Avançado 10 Mbps + SLR + SDC	LR/Mês	5.646,27
9	LR Avançado 20 Mbps + SLR + SDC	LR/Mês	6.846,88
10	LR Avançado 50 Mbps + SLR + SDC	LR/Mês	8.918,37
11	LR Avançado 100 Mbps + SLR + SDC	LR/Mês	22.310,28
12	LR Avançado 200 Mbps + SLR + SDC	LR/Mês	39.101,31
13	LR Plus 5 Mbps + SLR + SDC	LR/Mês	5.378,31
14	LR Plus 10 Mbps + SLR + SDC	LR/Mês	6.616,17
15	LR Plus 20 Mbps + SLR + SDC	LR/Mês	8.604,00
16	LR Plus 50 Mbps + SLR + SDC	LR/Mês	10.103,70
17	LR Plus 100 Mbps + SLR + SDC	LR/Mês	23.535,69
18	LR Plus 200 Mbps + SLR + SDC	LR/Mês	45.652,80
19	Serviços de Wi-Fi Gerenciado	UJ/Mês[8]	618,94

Todas e quaisquer despesas necessárias ao cumprimento do objeto desta licitação, tais como mão de obra (deslocamento, hospedagem, alimentação, seguros, etc.) impostos, tributos, encargos e contribuições sociais, fiscais, parafiscais, fretes, seguros, transporte, estadia, alimentação e demais despesas inerentes, correrão por conta da CONTRATADA, não cabendo ao CONTRATANTE, o reembolso de despesas com

5 LR/Mês: Custo mensal de um link remoto.
6 SLR: Segurança do Link Remoto, conforme definido no item 4.6.8.
7 SDC: Segurança de Acesso ao Data Center, conforme definido no item 4.6.9.
8 UJ/Mês: Custo mensal dos serviços de Wi/Fi Gerenciado para uma Unidade Judiciária.

transporte, hospedagem e outros custos operacionais, não previstos neste termo de referência, que deve ser de exclusiva responsabilidade da CONTRATADA.

2.10.2 Qualificação Técnica (Art. 18, § 3º, II, j)

A qualificação técnica do licitante será aferida com base nos seguintes documentos:

- Atestado(s) ou declaração(ões) de capacidade técnica, fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, comprovando atividade pertinente e compatível, em características, quantidades e prazos, com o objeto desta licitação, incluindo:
    - Prestação de serviços de Comunicação com características compatíveis com o objeto desta licitação.
    - Prestação de serviços de Segurança Gerenciada contemplando a disponibilização de equipamentos UTMs monitorados 24 x 7.
    - Prestação de serviços de Service Desk, em regime de funcionamento 24 x 7, com processos baseados nas melhores práticas do ITIL e fornecimento de portal WEB para abertura ou consulta de tickets.
    - Prestação de serviços de Rede Sem Fio (Access Points indoor, incluindo equipamentos, Captive Portal e acessórios).
- Comprovação de que a empresa licitante é concessionária ou autorizada pela ANATEL para prestação de serviços de telecomunicações no estado da Bahia.
- Apresentação de contrato de utilização compartilhada de pontos de fixação de cabos de fibra óptica e recursos de telecomunicações em poste da concessionária do serviço público de distribuição de energia elétrica (Companhia de Eletricidade do Estado da Bahia – COELBA). Caso contrário, a licitante deverá comprovar a existência de postes próprios, redes enterradas, ou ainda compartilhamento de infraestruturas com outras operadoras, como também as devidas autorizações das entidades para tal propriedade.

Para comprovar suficientemente a aptidão da empresa licitante, os atestados deverão conter informações detalhadas sobre os serviços prestados, tais como tempo de execução efetiva e grau de satisfação do contratante.

A Administração se resguarda o direito de efetuar diligência junto à pessoa jurídica emissora dos atestados, visando obter informação sobre o serviço prestado e cópias dos respectivos contratos e aditivos e/ou outros documentos comprobatórios do conteúdo declarado.

No caso de atestados emitidos por pessoa jurídica de direito privado, não serão considerados aqueles emitidos por empresa pertencente ao mesmo grupo empresarial da licitante, sua subsidiária, controlada ou controladora ou por empresa na qual haja pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da licitante.

Todos os documentos emitidos em língua estrangeira deverão ser acompanhados da correspondente versão em português, assinada por tradutor juramentado.

Sempre que julgar necessário, o CONTRATANTE poderá solicitar a apresentação do original dos documentos, não sendo aceitos “protocolos de entrega” ou “solicitações de documentos” em substituição aos comprovantes exigidos no presente Edital.

O CONTRATANTE poderá, se julgar necessário, realizar inspeções e diligências no ambiente da CONTRATADA a fim de garantir que a mesma esteja em condições de fornecer os serviços pretendidos de acordo com a qualidade exigida.

2.11 Adequação do Ambiente (Art. 18, § 3º, II, k)

Em todos os locais em que a CONTRATADA execute serviços, deverão sempre ser mantidas as mesmas condições estéticas do local. Os serviços de instalação não devem obstruir o andamento das rotinas de trabalho nos ambientes objetos de intervenção. Quando houver intervenção nestes ambientes, é de responsabilidade da CONTRATADA, a recomposição total dos mesmos deixando os locais totalmente limpos e arrumados inclusive com relação a algum dano a eles causado quando da execução dos serviços, isso inclui quando necessário, recomposição de gesso e pintura das áreas afetadas pela intervenção realizada.

2.12 Conformidade Técnica e Legal (Art. 18, § 3º, II, l)

A contratação deverá estar de acordo com a Lei Estadual nº 9.433, de 01 de março de 2005, e, no que couber, com a Lei Federal nº 8.666/93 e demais normas correlatas.

Todos os equipamentos e enlaces a serem fornecidos, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área e pelas entidades de padronização reconhecidas internacionalmente, tais como:

- ABNT (Associação Brasileira de Normas Técnicas);
- ANATEL (Agência Nacional de Telecomunicações);
- ITU-T (*International Telecommunication Union*);
- ISO (*International Standardization Organization*);
- IEEE (*Institute of Electrical and Electronics Engineers*);
- EIA/TIA (*Electronics Industry Alliance and Telecomumnication Industry Association*).

2.13 Obrigações da Contratada (Art. 18, § 3º, II, m)

2.13.1 Prestar os serviços conforme especificações, quantidades, prazos e demais condições estabelecidas no Edital e seus anexos, na Proposta e no Contrato.

2.13.2 Participar da reunião de alinhamento a ser realizada em data e horário a ser definido pelo CONTRATANTE. Nesta reunião, designar e apresentar o preposto do contrato.

2.13.3 Estar disponível para realizar reuniões periódicas com o CONTRATANTE, podendo este último, em atenção a circunstâncias específicas, dispensar reuniões programadas ou convocar, em caso de necessidade, reuniões extraordinárias, às que um representante da CONTRATADA deve comparecer no prazo máximo de dois dias úteis.

2.13.4 Seguir as instruções e observações efetuadas pelo Gestor do Contrato, bem como reparar, corrigir, remover, reconstruir ou substituir às suas expensas, no todo ou em parte, serviços efetuados em que se verificarem vícios, defeitos ou incorreções.

2.13.5 Utilizar as melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço e o atendimento às especificações contidas no Contrato, Edital e seus Anexos.

2.13.6 Reportar formal e imediatamente ao Gestor do Contrato quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução do(s) serviço(s).

2.13.7 Adotar critérios adequados para o processo seletivo dos profissionais, com o propósito de evitar a incorporação de pessoas com características e/ou antecedentes que possam comprometer a segurança ou credibilidade do CONTRATANTE.

2.13.8 Responder perante o CONTRATANTE, pela conduta dos seus empregados designados para execução dos serviços objeto do contrato, nos aspectos de segurança, disciplina e demais regulamentos vigentes no CONTRATANTE, bem como atentar para as regras de cortesia no local onde serão executados os serviços.

2.13.9 Pagar os salários e encargos sociais devidos pela sua condição de única empregadora do pessoal designado para execução dos serviços contratados, incluindo indenizações decorrentes de acidentes de trabalhos, demissões, vales-transporte, entre outros, obrigando-se, ainda, ao fiel cumprimento das legislações trabalhistas e previdenciárias, sendo-lhes defeso invocar a existência deste contrato para eximir-se destas obrigações ou transferi-las para o CONTRATANTE.

2.13.10 Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do CONTRATANTE.

2.13.11 Responsabilizar-se integralmente pelos recursos técnicos e humanos, primando pela qualidade, desempenho, eficiência, disponibilidade e produtividade, visando à execução dos trabalhos durante toda a vigência do Contrato, dentro dos prazos e condições estipulados, sob pena de ser considerado infração passível de aplicação de penalidades previstas contratualmente, caso os prazos e condições não sejam cumpridos.

2.13.12 Promover, por sua conta e risco, o transporte de seus empregados, equipamentos, peças, insumos e utensílios necessários à execução dos serviços objeto do contrato, até as instalações do CONTRATANTE.

2.13.13 Facilitar por todos os meios a seu alcance a ampla ação fiscalizadora dos prepostos designados pelo CONTRATANTE, atendendo prontamente as observações e exigências que lhe forem dirigidas.

2.13.14 Responder por quaisquer prejuízos que seus profissionais causarem ao patrimônio da CONTRATANTE ou a terceiros, por ocasião da prestação dos serviços, procedendo imediatamente aos reparos ou indenizações cabíveis e assumindo o ônus decorrente.

2.13.15 Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do Contrato, respeitando todos os critérios estabelecidos.

2.13.16 Manter sigilo total de todos os dados ou informações a que tiver acesso, não podendo, em hipótese alguma, divulgar resultados, parciais ou totais, ou fazer qualquer comentário sobre as informações a que tenha tido acesso, o levantamento realizado e o conteúdo dos produtos gerados.

2.13.17 Somente divulgar quaisquer informações a que tenha acesso, em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, com autorização, por escrito, do CONTRATANTE.

2.13.18 Quando da assinatura do contrato, por meio de seu representante, assinar Termo de Sigilo em que se responsabilizará pela manutenção de sigilo e confidencialidade das informações a que possa ter acesso em decorrência da contratação. O termo visa assegurar que a CONTRATADA manterá sigilo, sob pena de responsabilidade Cível, penal e administrativa acerca de informações consideradas como de interesse restrito ou confidencial, e não podem ser de conhecimento de terceiros, como por exemplo:

2.13.18.1 Programas de computador, seus códigos-fonte e códigos-objeto, bem como suas listagens e documentações.

2.13.18.2 Toda a informação relacionada a programas de computador existentes ou em fase de desenvolvimento no âmbito do CONTRATANTE e rotinas desenvolvidas por terceiros, incluindo fluxogramas, estatísticas, especificações, avaliações, resultado de testes, arquivo de dados, versões “beta” de quaisquer programas, dentre outros.

2.13.18.3 Documentos relativos à lista de usuários do CONTRATANTE e seus respectivos dados, armazenados sob qualquer forma.

2.13.18.4 Metodologias e ferramentas de serviços, desenvolvidas pelo CONTRATANTE.

2.13.18.5 Parte ou totalidade dos modelos de dados que subsidiam os sistemas de informações do CONTRATANTE, sejam eles executados interna ou externamente.

2.13.18.6 Parte ou totalidade dos dados ou informações armazenadas nas bases de dados que subsidiam os sistemas de informações do CONTRATANTE sejam elas residentes interna ou externamente.

2.13.18.7 Circulares e comunicações internas do CONTRATANTE.

2.13.18.8 Quaisquer processos ou documentos classificados como RESTRITO ou CONFIDENCIAL pelo CONTRATANTE.

2.13.19 O fornecedor não poderá armazenar consigo qualquer documento técnico que contemple configurações e regras de segurança aplicadas nos equipamentos implantados na rede do TJBA.

2.13.20 Todos os perfis de acesso e caixas postais eventualmente concedidos ao fornecedor deverão ser imediatamente excluídos após o término do contrato.

2.13.21 O TJBA terá propriedade sobre todos os dados, documentos e procedimentos operacionais produzidos no escopo da presente contratação.

2.13.22 O fornecedor deverá respeitar as normas de segurança estabelecidas pelo TJBA durante a realização de atividades nas dependências do CONTRATANTE.

2.13.23 Não será permitida intervenção nas bases de dados, a menos que haja autorização expressa e formal da área gestora dos sistemas.

2.13.24 A inclusão de componentes de software proprietários sem prévia e expressa autorização do Poder Judiciário da Bahia é vedada em qualquer das etapas de execução dos serviços.

2.14 Obrigações do Contratante (Art. 18, § 3º, II, m)

2.14.1 Efetuar mensalmente os pagamentos devidos à Contratada.

2.14.2 Disponibilizar todas as informações necessárias para o desenvolvimento dos trabalhos.

2.14.3 Fornecer a infraestrutura necessária para o pleno funcionamento dos Serviços, seguindo as especificações técnicas fornecidas pela CONTRATADA e dentro das normas ABNT relacionadas. Entende-se como infraestrutura:

2.14.3.1 Alimentação (disponibilização de energia elétrica estabilizada e aterrada) para Equipamentos de Comunicação necessários à implantação da rede.

2.14.3.2 Infraestrutura do ambiente (cabeamento lógico da rede interna e rack para instalação dos equipamentos, certificado de acordo com as normas nacionais e internacionais).

2.14.3.3 Aterramento da rede elétrica relativa aos equipamentos de interconexão e telecomunicações (modem, rádio ou interface de fibras ótica com rede externa, etc.).

2.14.4 Validar e aprovar os serviços executados, em conformidade com as regras e requisitos estabelecidos no ANS (Acordo de Níveis de Serviço).

2.14.5 Providenciar o acesso controlado dos profissionais da CONTRATADA ao ambiente de TI, incluindo bibliotecas de programas, políticas, normas, procedimentos, metodologias, bases de dados, ferramentas, de acordo com pré-requisitos definidos nas comunicações formais de demanda.

2.14.6 Responsabilizar-se pela guarda e integridade dos equipamentos recebidos. No momento da instalação, deve ser fornecida uma relação dos equipamentos de comunicação que serão instalados na unidade, com todas as informações estabelecidas no processo de ativação. Esta ordem de serviço deve ser assinada pelo representante do CONTRATANTE que acompanhou o processo de instalação.

2.14.7 Aplicar as sanções conforme previsto no contrato.

3 DETALHAMENTO DO OBJETO (ART. 18, § 3º, III)

3.1 Modelo de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a)

O CONTRATANTE será responsável pela gestão do contrato e pelo atesto quanto à aderência aos padrões de qualidade exigidos dos produtos e serviços entregues.

A CONTRATADA será responsável pela execução dos serviços e gestão dos recursos humanos, físicos e tecnológicos inerentes ao escopo da contratação.

3.2 Principais Papéis (Art. 18, § 3º, III, a, 1)

- Gestor do Contrato: Servidor do quadro permanente do CONTRATANTE, a ser designado oportunamente mediante portaria, com as seguintes responsabilidades:
    - Planejar e orientar a contratação, especialmente para estabelecer diretrizes para a contratação e condução dos vínculos contratuais.
    - Manter fluxo de comunicação e administrar as relações com a CONTRATADA.
    - Acompanhar o andamento do contrato, especialmente no referente aos cumprimentos e descumprimentos contratuais.
    - Manter-se sempre informado de todas as ocorrências contratuais e repassar às autoridades, proativamente, aquelas que interfiram na prestação dos serviços.
    - Paralisar a execução do contrato no caso de estar em desacordo com o pactuado ou diante de graves descumprimentos pelo fornecedor ou riscos para a Administração.
    - Promover as pertinentes penalizações e fazer os contatos necessários em nome do Contratante.
    - Promover os pertinentes ajustes no contrato.
    - Conduzir o encerramento do contrato.
- Fiscais do Contrato: Servidores do quadro permanente do CONTRATANTE, a serem oportunamente designados mediante portaria, responsáveis pela fiscalização do contrato sob os pontos de vista funcional, técnico e administrativo, aos quais competirá:
    - Verificar os recursos materiais e humanos empregados na execução do contrato.
    - Verificar a forma de execução do objeto do contrato.
    - Avaliar o cumprimento de todas as obrigações contratuais.
    - Cobrar da CONTRATADA o cumprimento do contrato.
    - Promover o registro documentado de todas as ocorrências contratuais diretamente relacionadas às obrigações assentadas no contrato.

- Manter contato com a CONTRATADA de modo a promover todo o tipo de interlocução operacional em nome do Tribunal.
- Comunicar ao Gerente do contrato as ocorrências de cumprimento e de descumprimento contratual detectadas.

- Preposto da CONTRATADA: Como anexo ao contrato, deverá a CONTRATADA indicar, formalmente, o seu preposto como responsável pela execução, nos termos do artigo 1561, da Lei n° 9.433/05.
  - O representante nomeado pela CONTRATADA deverá ter condições de coordenar a execução do contrato e ter poderes expressos para representá-la em todos os atos do contrato, especialmente para ajustes obrigacionais registrados em atas de reuniões, termos de recebimento ou recusa de objeto a ser entregue, notificações, ofícios, e demais atos relacionados à execução do contrato.
  - Esta designação será escrita, assinada pelo representante da CONTRATADA (outorgante) e pelo próprio preposto indicado, devendo conter, no mínimo, as disposições do "Termo de Nomeação de Preposto", Modelo III deste Termo de Referência.
  - No ato da designação, a Contratada deverá apresentar todas as informações de contato do preposto escolhido (endereço, telefone, celular, WhatsApp, e-mail etc.), bem como os canais específicos para o registro de solicitações, consultas, intimações, etc.
  - Havendo necessidade de realizar reuniões de planejamento e/ou ajuste da execução dos serviços, o Gestor do Contrato poderá convocar reuniões específicas, as quais o Preposto da Contratada deverá comparecer no prazo máximo de 2 (dois) dias úteis[9].

3.3 Dinâmica da Execução (Art. 18, § 3º, III, a, 2)

Os serviços a serem prestados são de natureza técnica, sob demanda, e serão solicitados pelo CONTRATANTE por meio de Chamado, conforme detalhado mais adiante neste tópico.

Para a realização dos serviços deve-se cumprir os procedimentos descritos a seguir, mantendo-se, ainda, a conformidade com o tópico 13.1, Modelo de Execução e atendendo ao Acordo de Nível de Serviço (ANS) definido no tópico 13.3.2.3:

3.4 Instrumentos Formais de Solicitação (Art. 18, § 3º, III, a, 3)

Todos os Incidentes e Requisições de Serviço objeto desta contratação serão administrados pelo Sistema de Service Desk a ser disponibilizado pela CONTRATADA, devendo armazenar todas as informações necessárias ao pleno funcionamento dos circuitos, permitindo a abertura de solicitações e incidentes e o acompanhamento global dos serviços prestados.

3.5 Atendimento aos Prazos de Garantia (Art. 18, § 3º, III, a, 4)

A garantia dos serviços será assegurada por três vias: Garantia Contratual, Serviços de Manutenção e Acordo de Níveis de Serviços.

3.5.1 Garantia Contratual

Em garantia de plena, fiel e segura execução de tudo o que se há obrigado, a CONTRATADA prestará caução correspondente a 2% (dois por cento) sobre o valor global do objeto contratado, em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, cuja liberação ou restituição dar-se-á após a expiração deste instrumento contratual.

A garantia será obrigatoriamente revista e complementada quando houver redução da sua representatividade percentual por variação econômica do contrato ou descontos de valores devidos ao CONTRATANTE, a exemplo de multas, quando for o caso.

A garantia responderá pelo inadimplemento das obrigações contratuais e pelas multas impostas, independentemente de outras cominações legais.

O cálculo da atualização monetária do valor caucionado em dinheiro será feito aplicando-se o índice mais vantajoso para a Administração entre a data de retenção da caução e da devolução do seu valor.

A garantia deverá ser apresentada no prazo máximo de 15 (quinze) dias corridos, contados da assinatura do Contrato.

9 A critério do Gestor do Contrato e concordância da CONTRATADA, essas reuniões poderão ser realizadas em forma presencial ou remota, mediante conferências telefônicas, videoconferência o similar.

3.5.2 Manutenção

A CONTRATADA deverá realizar a manutenção preventiva e corretiva do Ambiente de Comunicação Digital disponibilizado para o CONTRATANTE, através de equipe técnica especializada, visando atender ao disposto no Acordo de Nível de Serviço (ANS), para plena disponibilidade do serviço em operação.

A prestação do serviço de manutenção deverá ser realizada por profissional da empresa CONTRATADA, cabendo-lhe efetuar os ajustes na solução, conserto ou troca de peças defeituosas por novas, sem nenhum tipo de ônus para o CONTRATANTE.

Caso haja a necessidade de realizar manutenção preventiva de qualquer serviço, a CONTRATADA deve solicitar ao CONTRATANTE com 5 (cinco) dias úteis de antecedência da data proposta para a realização do serviço. A CONTRATADA só poderá realizar este procedimento com a anuência do CONTRATANTE. O tempo gasto na manutenção programada, nos moldes do disposto neste item, não será registrado como serviço indisponível.

3.5.3 Acordo de Nível de Serviço (ANS)

Para o acompanhamento e avaliação dos serviços da CONTRATADA será estabelecido e utilizado entre as partes o Acordo de Níveis de Serviços (doravante chamado ANS). O ANS deve ser considerado e entendido pela CONTRATADA como um compromisso de qualidade que assumirá junto ao CONTRATANTE.

A CONTRATADA deverá acompanhar os Indicadores para que seja possível uma avaliação da qualidade do serviço entregue. A partir das informações obtidas nestes indicadores será possível a aplicação do ANS (Acordo de Níveis de Serviço) no processo de pagamento.

Caso ocorra, a qualquer tempo, a não aceitação, por parte do CONTRATANTE, de quaisquer aspectos necessários à declaração da fatura, os prazos para ateste serão descontinuados e reiniciados após a correção necessária. O CONTRATANTE pode, a qualquer momento, recusar-se a declarar a fatura, caso constate:

- Falhas sistemáticas ou intermitentes, decorrentes de defeitos ou vícios nos equipamentos ou nos serviços.
- Descumprimento dos requisitos técnicos e funcionalidades estabelecidos neste Edital e/ou indicados na proposta e demais documentos que a integram.
- Problemas decorrentes de falha de projeto.

O valor a ser pago pela realização dos serviços objeto deste contrato será apurado em razão do cumprimento do ANS, podendo diante de eventuais imperfeições em sua execução, resultar em glosa no seu pagamento.

Entretanto, eventuais falhas e descumprimentos contratuais verificados serão devidamente apurados em processos administrativos próprios, podendo resultar em aplicação de penalidade, sem prejuízo de possível rescisão do contrato, na forma prevista na lei.

A CONTRATADA terá até 05 (cinco) dias úteis do mês posterior ao mês faturado para justificar situações imprevistas que tenham gerado uma informação inadequada de faturamento, bem como para comprovar eventuais ocorrências decorrentes de força maior, alheias ao seu controle, que tenham prejudicado o atendimento às condições aqui definidas. Após esse período de justificativa por parte da CONTRATADA, o CONTRATANTE terá até 05 (cinco) dias úteis para análise das justificativas, acatando-as ou não. Após estes 10 (dez) dias úteis, a fatura deve ser recalculada, se for o caso, e encaminhada para o pagamento.

Para o estabelecimento da remuneração mensal da CONTRATADA define-se:

- **Nível de Serviço Contratado (NSC) [unidade]**: valor estabelecido pelo CONTRATANTE, como limite superior que pode ser atingido pela CONTRATADA para cada Indicador, conforme apresentado nos Quadros 1 e 2.
- **Nível de Serviço Apurado (NSA) [unidade]:** valor apurado para cada Indicador no período em análise.
- **Não Conformidade (NC) [%]:** percentual calculado a partir das regras estabelecidas no Quadro 5, considerando as informações de NSC e NSA.
- **O *Pagamento Individual do Serviço* (PIS):** é o valor de referência acordado com a CONTRATADA para o pagamento de um serviço específico, Link Remoto (LR) ou Serviço de Wi-Fi.
- **Valor Devido do Serviço (VDS) [R$]:** valor devido pela CONTRATADA ao CONTRATANTE, em função de não ter atingido o Nível de Serviço estabelecido pelo CONTRATANTE no Acordo de Nível de Serviço (ANS) de um Serviço Específico, LR ou Wi-Fi. O Valor devido terá como base as informações estabelecidas de Não Conformidade (**NC**) e Pagamento Individual do Serviço (**PIS**).

- **Pagamento Completo (PC) [R$]:** valor de referência acordado com a CONTRATADA para pagamento de todos os serviços prestados. Será o valor adotado quando a CONTRATADA tiver como resultante do cálculo do Valor Devido (**VD**) um número igual a zero.
- **Valor Devido (VD) [R$]:** valor devido pela CONTRATADA ao CONTRATANTE, em função de não ter atingido o Nível de Serviço estabelecido pelo CONTRATANTE no Acordo de Nível de Serviço (ANS), considerando todos os serviços prestados. O Valor devido terá como base as informações estabelecidas no **Valor Devido do Serviço (VDS)**.
- **Pagamento Efetivo (PE) [R$]:** valor efetivo a ser pago à CONTRATADA pelo CONTRATANTE referente ao mês de apuração do NSA.

A CONTRATADA se compromete a prestar o serviço com os *Indicadores* **de tempo máximo de atendimento,** a partir da abertura do Chamado, apresentados nos Quadros 1 e 2. Estes Indicadores serão consolidados mensalmente, durante a execução do CONTRATO, gerando o cálculo do ANS. A condição Não Funcional ou Indisponível de um determinado *Indicador* será determinada a partir do procedimento estabelecido nos quadros 3 e 4.

Considera-se ***Dia Útil do Mês*** para efeito do ANS, a quantidade de dias do mês subtraindo os finais de semana, feriados nacionais, estaduais e municipais da Bahia. A CONTRATADA deverá identificar, por localidade a ser atendida, quais são os feriados municipais.

Indicadores de Serviço	NSC
Ativação de LR	45 dias corridos
Desativação de LR ou Wi-Fi	1 dia corrido
Mudança de Endereço de LR ou Wi-Fi	45 dias corridos
Alteração de Taxa de Comunicação	30 dias corridos
Alteração de Configuração (exceto solicitações de Segurança)	1 dia útil
Alteração de Configuração de Segurança de LR[10]	4 horas
Requisição de logs ou relatórios de Segurança de LR	1 dia útil
Análise e investigação / troubleshooting de Segurança de LR	2 horas
Instalação da Solução de Segurança Data Center	60 dias corridos
Instalação de Wi-Fi Gerenciado	30 dias corridos

Quadro 1 Indicadores de Serviço e seus NSCs

Indicadores de Operação	NSC Não Funcional	NSC Indisponível
Operação LR Básico	2 dias úteis	1 dia útil
Operação de LR Avançado até 5 Mbps	1 dia útil	1 dia útil
Operação de LR Avançado a partir de 10 Mbps	Mesmo dia Chamado aberto até 12:00 inclusive. 1 dia útil Chamado aberto após as 12:00	Mesmo dia Chamado aberto até 12:00 inclusive. 1 dia útil Chamado aberto após as 12:00
Operação de LR Plus	Mesmo dia Chamado aberto até 12:00 inclusive. 1 dia útil Chamado aberto após as 12:00	Mesmo dia
Operação da Solução de Segurança do Data Center	2 dias corridos	1 dia corrido
Operação de Wi-Fi Gerenciado	2 dias úteis	1 dia útil

Quadro 2 Indicadores de Operação e seus NSCs

Para o estabelecimento de uma condição Não Funcional ou Indisponível deverá ser realizada uma medição dos Indicadores de Desempenho nos termos estabelecidos de Periodicidade conforme o Quadro 3. Poderão ocorrer três situações para o LR:

- Funcional O valor medido está dentro do limite estabelecido no Quadro 4.
- Não Funcional Caso o valor medido esteja acima do valor estabelecido no Quadro 4, o LR será considerado Não Conforme. Por exemplo, caso um LR de um circuito de 10 MBps esteja com um Jitter superior a 50 ms, ele será considerado Não Funcional. Uma vez detectada a condição de Não Funcional será aberto um Chamado que contabilizará o tempo.
- Indisponível Caso nenhum dos pings obtenha resposta, o LR será considerado Indisponível.

10 Aplicável apenas para LR Avançado e Plus

O critério para definição da situação de Não Funcional ou Indisponível para o serviço de Wi-Fi Gerenc será o mesmo do LR definido no Quadro 4, exceto no parâmetro de Vazão Mínima e Jitter que não aplicam.

Para o serviço de Solução de Segurança Data Center, os critérios, considerando os equipamentos que compõem a solução, serão os seguintes:

- Funcional: quando não existir nenhuma falha nos equipamentos.
- Não Funcional: quando ocorrer qualquer falha que afete o funcionamento parcial em um dos equipamentos. Por exemplo: quando falhar apenas uma fonte ou queimar uma das portas de rede.
- Indisponível: Quando qualquer equipamento apresente um problema que afete o seu funcionamento por completo. Por exemplo: quando apenas um dos equipamentos da solução queime.

Indicadores de Desempenho do LR	Periodicidade e Quantidade de ping's
Vazão	20 ping's a qualquer momento para qualquer circuito *[11]
Tempo de Resposta	
Perda de Pacotes	
Jitter	

Quadro 3 – Periodicidade de Medição dos Indicadores de Desempenho

	LR Básico	Circuito Terrestre LR Avançado e Plus				Circuito Satélite LR Avançado				
Indicadores de Desempenho	Perda de Pacotes	Tempo de Resposta (ms)	Jitter (ms)	Perda de Pacotes (pacotes)	Vazão Mínima	Tempo de Resposta (ms)	Jitter (ms)	Perda de Pacotes (pacotes)	Vazão Mínima	
									Upload	Download
Até 5 Mbps	< 5%	< 130	< 50	< 1,00 %	Taxa contratada	< 900	< 100	< 5,00 %	20% da Taxa contratada	50% da Taxa contratada
Acima de 5 Mbps	< 5%	< 50	< 50	< 1,00 %	Taxa contratada	-	-	-	-	-

Quadro 4 – Parâmetros para Medição de Funcionalidade dos LR's

Para o atendimento da prestação de serviço e cálculo do Valor Devido (**VD**) para fins de pagamento, o Quadro 5 apresenta a respectiva forma de cálculo da Não Conformidade (**NC**). O Valor de referência de **NSC** para os diversos Indicadores encontra-se no Quadro 4.

Item	Indicadores	Nível de Serviço Apurado NSA [un]	Forma de Cálculo da Não Conformidade NC [%]
1	Ativação de LR Básico e LR Avançado Ativação de LR Plus Desativação de LR ou Wi-Fi Mudança de Endereço de LR ou Wi-Fi Instalação da Solução de Segurança do Data Center Instalação de Wi-Fi Gerenciado	Dias corridos entre a abertura do chamado e a entrega	Quando NSA > NSC: NC =(NSA-NSC) [%]
2	Alteração de Taxa de Comunicação	Dias corridos entre a abertura do chamado e a entrega	Quando NSA > NSC: NC = (NSA-NSC)*0,3[%]
3	Alteração de Configuração (exceto solicitação de Segurança).	Dias úteis entre a abertura do chamado e a entrega	Quando NSA > NSC: NC = NSA*0,3 [%]
4	Alteração de Configuração de Segurança de LR Requisição de logs ou relatórios de Segurança de LR Análise e investigação / troubleshooting de Segurança de LR	Tempo corrido em horas entre a abertura do chamado e a entrega	Quando NSA > NSC: NC = NSA*0,0125 [%]
5	Operação de LR Básico Não Funcional Operação de LR Avançado até 5 Mbps Não Funcional Operação de LR Avançado a partir de 10 Mbps Não Funcional Operação de LR Plus Não Funcional Operação de Wi-Fi Gerenciado Não Funcional	Dias úteis entre a abertura do chamado e a entrega.	Quando NSA > NSC: NC = (NSA / 23)*0,3 [%]
6	Operação de LR Básico Indisponível Operação de LR Avançado até 5 Mbps Indisponível Operação de LR Avançado a partir de 10 Mbps Indisponível Operação de LR Plus Indisponível Operação de Wi-Fi Gerenciado Indisponível	Dias úteis entre a abertura do chamado e a entrega.	Quando NSA > NSC: NC = (NSA / 23)[%]
7	Operação de Solução de Segurança Não Funcional	Tempo corrido em horas entre a abertura do chamado e a entrega	Quando NSA > NSC: NC = (NSA / 744)*0,6 [%]

11 O teste de ping para os LRs Avançado e Plus será realizado a partir do Data Center do CONTRATANTE para o roteador LR, através do Ponto Principal. Para o LR Básico, o teste será feito a partir do Data Center, através da Internet, para o IP do equipamento do LR Básico.

Item	Indicadores	Nível de Serviço Apurado NSA [un]	Forma de Cálculo da N Conformidade NC [%]
1	Operação de Solução de Segurança Indisponível	Tempo corrido em horas entre a abertura do chamado e a entrega	Quando NSA > NSC: NC = (NSA / 744) [%]

Quadro 5 – Níveis de Serviço Contratados (NSC) e Cálculo do NC a partir do NSA.

O CONTRATANTE pagará mensalmente pelos serviços efetivamente prestados pela CONTRATADA, proporcionalmente aos valores cotados na proposta vencedora, considerando que:

O ***Valor Devido do Serviço*** **(VDS)**, será o resultado da multiplicação do somatório de todas as ***Não Conformidades*** **(NC)**, obtido *com b*ase em todos os Indicadores associados ao serviço conforme fórmula de cálculo definida no Quadro 5, pelo ***Pagamento Individual do Serviço*** **(PIS)**:

$$VDS = (\sum NC) \times PIS$$

O **Valor Devido (VD)** será o resultado do somatório dos **Valores Devidos dos Serviços (VDS),** referente a todos os serviços prestados:

$$VD = \sum VDS$$

O ***Pagamento Completo*** **(PC)** será o resultado do somatório dos ***Pagamentos Individuais dos Serviços*** **(PIS)**, referente a todos os serviços prestados:

$$PC = (\sum PIS)$$

O *Pagamento Efetivo* pelos serviços prestados pela CONTRATADA (PE) será o resultado da seguinte fórmula:

$$PE = PC - VD$$

Caso o VD apurado no mês seja maior do que 30% do Pagamento Completo (PC), serão aplicadas as penalidades previstas no contrato e na legislação em vigor.

3.6 Acompanhamento da Execução (Art. 18, § 3º, III, a, 5)

O Preposto, indicado pela CONTRATADA através do Termo de Nomeação de Preposto (Modelo III), será corresponsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual. Este serviço, de gerenciamento do contrato e dos diversos serviços nele contemplados, será prestado sem ônus específico.

Da parte do CONTRATANTE, o gestor e o fiscal do contrato, através de ferramentas próprias, serão encarregados do monitoramento dos Indicadores de Serviço estabelecidos no Acordo de Níveis de Serviço. Neste mesmo tópico, além de ser especificado o Indicador de Serviço, também estão estabelecidos o período de medição e a forma de medição para obtenção do Nível de Serviço Apurado do Mês.

Como meios de comunicação oficiais entre a CONTRATANTE e a CONTRATADA, poderão ser utilizados os seguintes:

- E-mail
- Relatório de Nível de Serviço
- Termo de Notificação
- Relatórios gerados pelo Sistema de Informação utilizado na prestação dos serviços.

Os documentos relacionados acima terão validade legal para fins de aferição de resultados, comprovação, contestação, pagamentos, entre outros.

Mensalmente, a CONTRATADA deverá entregar um relatório consolidando todas as informações relativas aos indicadores do mês anterior até o 5º dia útil de cada mês.

3.7 Recebimento Provisório e Definitivo (Art. 18, § 3º, III, a, 6)

O Aceite dos serviços será feito mensalmente com base em relatório dos serviços prestados a ser apresentado pela CONTRATADA.

Esse relatório será Aceito:

- Provisoriamente, pelo prazo de 15 (quinze) dias corridos, para efeito de posterior verificação da conformidade com os requisitos exigidos no edital.
- Definitivamente, após verificação da qualidade e quantidade dos serviços prestados, podendo o CONTRATANTE glosar o faturamento com base nas regras definidas no Acordo de Níveis de Serviços.

Para todos os fins, será considerado o mês de atividade referente ao serviço realizado a partir de 00:00 1º dia até as 23:59 h do último dia do mês.

O faturamento de um circuito ativado no mês de referência será calculado proporcionalmente à quantidade de dias de prestação do serviço entre a data de ativação efetiva e o final do mês.

O faturamento de um circuito desativado no mês de referência será calculado proporcionalmente ao tempo transcorrido entre o primeiro dia do mês e a data de abertura da ordem de serviço que solicitou a sua desativação.

A efetivação e aceite de quaisquer serviços não previstos só poderá acontecer mediante aprovação formal do CONTRATANTE.

A(s) nota(s) fisca(l)is / fatura(s) somente deverá(ao) ser apresentada(s) para pagamento após a conclusão da etapa do Aceite Definitivo, indicativo da satisfação pela Contratada de todas as obrigações pertinentes, acompanhadas da documentação probatória pertinente, relativa ao recolhimento dos impostos relacionados com a obrigação.

Tratando-se de um contrato de serviços sob demanda, não haverá faturamento nos meses em que nenhum circuito estiver em atividade.

O aceite dos serviços pelo Contratante não exime a Contratada da responsabilidade pela correção dos erros porventura identificados em faturamentos anteriores.

O Recebimento Definitivo da totalidade dos serviços, habilitando a CONTRATADA a requerer a devolução da caução, será emitido após o encerramento do contrato mediante constatação de que todas as obrigações da CONTRATADA foram satisfatoriamente executadas.

3.8 Forma de Pagamento (Art. 18, § 3º, III, a, 7)

A Contratada deverá apresentar nota fiscal correspondente ao objeto fornecido, reservando-se o Contratante o direito de não a atestar para o pagamento se os dados nela constantes estiverem em desacordo com os valores apurados com base no Acordo de Níveis de Serviços, ficando o pagamento suspenso até a regularização.

No caso de consórcio, não serão aceitas notas fiscais emitidas separadamente pelas empresas consorciadas, devendo todo o faturamento ser realizado em nome do consórcio.

Nos casos de subcontratação, não serão aceitas notas fiscais emitidas pelas empresas subcontratadas, devendo todo o faturamento ser realizado em nome da empresa contratada.

O atesto na nota fiscal é condição indispensável para o pagamento desta. Na ausência do gestor, o atesto será dado por gestor substituto.

O pagamento será efetuado no prazo de 8 (oito) dias úteis, contados a partir da apresentação da nota fiscal ao gestor do contrato ou substituto.

O CNPJ constante da nota fiscal deverá ser o mesmo indicado na proposta, nota de empenho e vinculado à conta-corrente da Contratada.

3.9 Locais de Prestação dos Serviços

Os Pontos Principais deverão ser instalados em Salvador/BA, no Data Center do Tribunal de Justiça, 5ª Avenida do CAB, Nº 560, CEP 41745-971.

Os Links Remotos (LRs) serão inicialmente instalados nos endereços listados no Anexo VI, podendo o CONTRATANTE solicitar, sob demanda, a instalação de novos LRs e/ou a transferência dos existentes para novos endereços.

Os serviços de Wi-Fi serão prestados sob demanda, nos endereços que o CONTRATANTE indicar.

3.10 Reunião de Alinhamento

Reuniões de Alinhamento entre representantes do CONTRATANTE e da CONTRATADA serão realizadas com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus Anexos e esclarecer possíveis dúvidas acerca da execução dos serviços.

A Reunião de Alinhamento realizar-se-á no endereço do CONTRATANTE, em até 10 (dez) dias úteis após a publicação do contrato, conforme agendamento a ser efetuado pelo Gestor do Contrato.

Nessa reunião, a CONTRATADA deverá:

- Apresentar oficialmente seu Preposto.

- Apresentar um Projeto Técnico Detalhado da Solução, a ser aprovado pelo CONTRATANTE, mostrando a topologia detalhada, o Cronograma de Instalação, os serviços oferecidos e as tecnologias de rede de acesso/transporte que serão utilizadas na solução, de maneira a demonstrar o atendimento a todos os requisitos exigidos neste Termo de Referência.

Todos os entendimentos durante a reunião de alinhamento deverão constar da Ata de Reunião a ser lavrada pelo Gestor do Contrato e assinada por todos os participantes.

3.11 Acompanhamento da Execução

O Preposto, indicado pela CONTRATADA como seu representante na reunião de alinhamento, será o responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual. Este serviço, de gerenciamento do contrato e dos diversos serviços nele contemplados, será prestado sem ônus específico.

Da parte do CONTRATANTE, o Gestor e os Fiscais do contrato, através de ferramentas próprias, serão encarregados do monitoramento dos Indicadores de Serviço estabelecidos no Acordo de Níveis de Serviço. No mesmo tópico estão estabelecidos o período e a forma de medição para obtenção do Nível de Serviço Apurado do Mês.

Como meios de comunicação oficiais entre a CONTRATANTE e a CONTRATADA, poderão ser utilizados os seguintes:

- E-mail
- Relatório de Nível de Serviço
- Termo de Notificação
- Relatórios gerados pelo Sistema de Informação utilizado na prestação dos serviços.

Os documentos relacionados acima terão validade legal para fins de aferição de resultados, comprovação, contestação, pagamentos, entre outros.

3.12 Vigência do Contrato

O Contrato terá vigência de 24 (vinte e quatro) meses a contar da data de sua assinatura, admitida a prorrogação nos termos da legislação em vigor.

3.13 Transferência de Conhecimento (Art. 18, § 3º, III, a, 8)

A CONTRATADA deverá efetuar o registro de todos os atendimentos de suporte e atualizações realizadas, bem como dos eventos relacionados à monitoração remota, e disponibilizar esse registro ao CONTRATANTE sempre que solicitado.

3.14 Transição Contratual

No encerramento do contrato, a CONTRATADA deverá promover transição contratual e repassar para o CONTRATANTE e/ou para a nova CONTRATADA todos os dados, documentos e elementos de informação utilizados na execução dos serviços.

Para melhor estruturar a transição, o CONTRATANTE promoverá uma Reunião de Alinhamento de Expectativas com a nova CONTRATADA, quando terá início formal à transferência de conhecimentos entre as empresas.

Os meios utilizados para essa transferência serão previamente acordados entre CONTRATADA e CONTRATANTE, podendo consistir em um ou uma combinação dos seguintes meios:

- Divulgação eletrônica.
- Base de conhecimentos.
- Registro de lições aprendidas.
- Registro de soluções alternativas utilizadas.
- Registro de ocorrências, conhecimentos e procedimentos.
- Documentação de melhores práticas.
- Reuniões e suas respectivas atas.
- Relatórios periódicos.

- Ferramentas de comunicação em geral: videoconferência, chat, e-mail.

A participação ativa da CONTRATADA nas atividades de transição contratual será condição indispensável para a devolução da Garantia Contratual.

3.15 Encerramento Abrupto do Contrato

Em caso de encerramento abrupto do contrato não haverá como manter a continuidade dos serviços em razão do caráter altamente especializado da infraestrutura necessária.

Portanto, competirá ao TJBA:

- Efetuar imediata contratação emergencial para evitar a paralisação das atividades das unidades do interior do estado que dependam de serviços hospedados no *Data Center*.
- Iniciar de imediato o planejamento da nova contratação para substituir a contratação emergencial.

3.16 Direitos de Propriedade Intelectual (Art. 18, § 3º, III, a, 9)

A CONTRATADA deverá entregar ao CONTRATANTE toda e qualquer documentação gerada como resultado da prestação de serviços, objeto da contratação.

Entende-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, fontes dos códigos dos programas em qualquer mídia, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica.

A utilização de soluções ou componentes proprietários da CONTRATADA ou de terceiros na execução dos serviços relacionados ao presente contrato, que possam afetar a propriedade do produto, deve ser formal e previamente autorizada pelo TJBA.

3.17 Descumprimento das Obrigações Contratuais (Art. 18, § 3º, III, a, 11)

Constituem ilícitos administrativos as condutas previstas nos artigos 184 e 185 da Lei nº 9.433/05, sujeitando-se os infratores às cominações legais, especialmente as definidas no art. 186 do mesmo diploma, garantida a prévia e ampla defesa em processo administrativo, bem como as condutas previstas na legislação específica, especialmente a Lei nº 10.520/02, art. 7º e Decretos Judiciários nº 12/2003 e 44/2003.

4 REQUISITOS TÉCNICOS ESPECÍFICOS (ART. 18, § 3º, IV)

4.1 Requisitos Técnicos Gerais

4.1.1 Adotar o protocolo TCP/IP para o tráfego de dados, voz e imagem em toda a rede, utilizando a tecnologia MPLS (Multi Protocol Label Switching) na rede de transporte entre o Backbone da CONTRATADA e os Pontos Principais.

4.1.2 Os serviços devem obrigatoriamente ser prestados por uma rede IP Multiserviços que permita a criação de VPN (Virtual Private Network) através de MPLS (Multiprotocol Label Switching) e que possibilite a configuração de QoS (Quality of Service) conforme cada caso.

4.1.3 Deverão ser criadas Redes Privadas Virtuais (VPNs) entre os LRs (Links Remotos), e entre LRs e os Pontos Principais , garantindo um isolamento completo do tráfego.

4.1.4 Deverá ser provida a facilidade de LRs de uma mesma VPN se comunicar diretamente sem passar pelos Pontos Principais e sem ônus para o CONTRATANTE.

4.1.5 Quando solicitado deverá ser provida facilidade de comunicação de determinado(s) LR(s) de uma ou mais VPNs para o Data Center.

4.1.6 A solução do Ponto Principal deverá ser capaz de bloquear tráfego de determinados LRs no ambiente com múltiplas VPNs de modo granular.

4.1.7 O serviço de VPN deve estar contemplado conforme exigência de cada categoria de LRs.

4.1.8 Prover integração e interoperabilidade de todos os recursos tecnológicos para o atendimento ao mecanismo de reconhecimento, classificação e priorização do tráfego (QoS) conforme cada categoria de LRs.

4.1.9 Suportar os protocolos IPv4 e IPv6 em todos os equipamentos utilizados na solução, devendo a rede suportar IPv6, promovendo a migração de IPv4 para IPv6, quando solicitado mediante apresentação de cronograma, e sem ônus para o CONTRATANTE.

4.1.10 Adotar o plano de endereçamento IP de LAN hoje existente. A alocação e o gerenciamento destes endereços serão feitos pelos órgãos.

4.1.11 A CONTRATADA deverá garantir o isolamento completo do tráfego para os LRs dos demais clientes existentes na rede IP Multiserviços.

4.1.12 O Backbone da CONTRATADA deverá adotar o protocolo TCP/IP e suportar os protocolos IPv4 e IPv6 em todos os equipamentos utilizados na solução, devendo a rede suportar IPv6, promovendo a migração de IPv4 para IPv6, quando solicitado, e sem ônus para o CONTRATANTE.

4.1.13 A CONTRATADA deve disponibilizar a técnicos indicados por cada órgão CONTRATANTE um acesso do tipo “somente leitura” a todos os equipamentos que compõem a solução, excluindo o backbone da operadora.

4.1.14 Deverá assegurar pleno acesso em consonância ao regimento do Marco Civil da Internet, e ao o princípio da neutralidade de rede.

4.1.15 Os recursos de hardware e suporte dos equipamentos envolvidos devem ser atualizados tecnologicamente nos termos de uma manutenção programada durante a vigência do contrato, visando a garantia do ANS (Acordo de Nível de Serviço) contratado e o adequado funcionamento dos serviços, sem ônus adicional para os clientes. A CONTRATADA deve apresentar um relatório de intervenção contendo todos os detalhes relacionados à atualização tecnológica, que deve ser submetido ao CONTRATANTE para que seja analisado e aprovado antes da sua efetiva implementação

4.1.16 As manutenções programadas deverão ser avisadas com no mínimo 5 (cinco) dias de antecedência e só poderão ser realizadas com a concordância do órgão CONTRATANTE.

4.1.17 Deverá ser fornecido Service Desk acessível por número telefônico com DDG (Discagem Direta Gratuita 0800) e site web para abertura de serviços e reparos conforme especificações do tópico Service Desk.

4.2 Requisitos Técnicos Gerais para as categorias de LR´s

4.2.1 Os serviços de acessos denominados como Links Remotos (LRs), serão classificados em 3 (três) categorias: LR Básico, LR Avançado e LR “Plus”.

4.2.2 Os serviços de acessos denominados como Links Remotos (LRs) deverão estar disponíveis 24 horas por dia, nos sete dias da semana.

4.2.3 A CONTRATADA deverá projetar, implantar, ativar, operacionalizar e manter, ao longo do contrato, os meios de acesso (metálico, óptico, radiofrequência, satélite) e redes de telecomunicações utilizadas no serviço dos LRs.

4.2.4 A CONTRATADA deverá realizar o fornecimento, instalação, configuração, suporte técnico e manutenção, ao longo do contrato, dos equipamentos de conectividade (modem, modem ótico, rádio, roteadores, Firewall, entre outros) utilizados no serviço dos LRs.

4.2.5 A CONTRATADA deverá apresentar preços fixos unitários mensais para todos os serviços de Links Remotos nas suas respectivas velocidades e localidades previstas na abrangência deste Termo. O volume de dados, voz e imagem trafegados não terá impacto na precificação, bem como, o tempo de utilização dos serviços e informações trafegadas.

4.2.6 Em caso de utilização de sistema de radiofrequência nos Links Remotos, devem ser utilizadas frequências licenciadas pela ANATEL, não sendo permitido o uso de rádios de frequência aberta. Neste caso, as localidades atendidas neste item deverão ser informadas aos CONTRATANTES. Não será permitido o uso de rede com tecnologia celular como GSM, EDGE, 3G, LTE, ou qualquer outra.

4.2.7 O CONTRATANTE será responsável pela infraestrutura necessária para instalação dos LRs, tais como energia elétrica, aterramento, climatização, espaço físico, racks, rede interna e cabeamento estruturado.

4.2.8 Deverão estar inclusos na composição de preços dos LRs os serviços de instalação.

4.2.9 Os endereços de instalação dos LRs, assim como possíveis mudanças de endereços, estarão localizados em áreas urbanas, em localidades constantes nos Planos Diretores Municipais ou disponíveis no Censo mais atual do IBGE.

4.2.10 Alternativamente, poderá ser utilizado atendimento por satélite para o LR Avançado, de acordo com as seguintes características:

4.2.10.1 Adotar uma solução sem duplo salto para comunicação, exceto nas comunicações entre dois LRs atendidos via satélite.

4.2.10.2 O acesso poderá ser disponibilizado com velocidades assimétricas, desde que a velocidade de dowstream seja a mesma velocidade nominal CONTRATADA.

4.2.10.3 A banda de download garantida deve ser de pelo menos 50% (cinquenta por cento) da velocidade nominal e 20% (vinte por cento) da garantia de upload.

4.2.10.4 Para o acesso por satélite, haverá apenas 2 (duas) Classe de Serviços a saber: Dados Prioritários e Dados não Prioritários.

4.2.10.5 O Tempo de Retardo médio (latência) fim-a-fim admitido deverá ser de, no máximo, 900 ms, já incluindo o tempo de propagação do satélite.

4.2.10.6 Fica estabelecido o percentual máximo de pontos conectados por tecnologia de acesso para cada órgão:

- 5% para satélite.
- 5% para radiofrequência.

4.2.11 Eventuais demandas de atendimentos a novos LRs localizados em zona rural e às margens de rodovias poderão ser atendidas por acesso satélite, excluindo-se esses atendimentos da limitação de 5% para satélite.

4.2.12 Os endereços, localidades, categorias e quantitativos dos LRs para instalação inicial, em até 90 dias, na ordem a ser definida pelo CONTRATANTE, estão listados neste Modelo de Proposta.

4.2.13 O aumento da velocidade, quando solicitado, deverá ser implementado com, no máximo, 2 (duas) horas de interrupção do serviço.

4.2.14 O serviço de mudança de endereço de LR, quando solicitado, deverá ser implementado sem causar descontinuidade dos serviços, e sem que haja repasse de custos adicionais.

4.2.15 O serviço de desativação de LR, quando solicitado, deverá ser realizado sem que haja repasse de custos adicionais. A CONTRATADA deverá realizar a retirada dos equipamentos com prévio agendamento com o CONTRATANTE. O pagamento do link será proporcional até a data agendada para cancelamento.

4.2.16 Executar as configurações de serviços e protocolos tais como ACL, DHCP, SNMP, roteamento, entre outros, de acordo com o acionamento do órgão.

4.2.17 Deverá ser fornecido um serviço de gerenciamento web-based dos LRs, conforme especificado no tópico Gerenciamento de Ambiente. Este serviço deve ser hospedado na infraestrutura da CONTRATADA sem custos adicionais.

4.3 Requisitos Técnicos Gerais dos Serviços de WiFi Gerenciado

4.3.1 Os serviços de WiFi Gerenciado são itens de contratação facultativa que podem ser agregados aos LRs de acordo com o interesse e necessidade do CONTRATANTE.

4.3.2 Os serviços de WiFi Gerenciado deverão estar disponíveis 24 horas por dia, nos sete dias da semana.

4.3.3 A CONTRATADA deverá realizar o fornecimento, instalação, configuração, suporte técnico, e manutenção dos equipamentos utilizados na prestação dos serviços de WiFi Gerenciado.

4.3.4 O CONTRATANTE será responsável pela infraestrutura necessária para instalação dos equipamentos, tais como energia elétrica, aterramento, espaço físico, rede interna e cabeamento estruturado, entre outros.

4.3.5 Os serviços de instalação deverão estar inclusos na composição de preços dos serviços de WiFi Gerenciado.

4.3.6 Será considerada como unidade de precificação dos serviços a plena cobertura WiFi de um único endereço de instalação com superfície máxima de 400 m².

4.3.7 As solicitações de mudança de endereço deverão ser atendidas, sem ônus adicional, no prazo de até 05 (cinco) dias úteis, contados a partir da emissão da Ordem de Serviço.

4.3.8 As solicitações de desativação de serviço, deverão ser atendidas, sem ônus adicional, limitado o faturamento à data da Ordem de Serviço que determinou a desativação. Após a desativação, a CONTRATADA poderá realizar a retirada dos equipamentos prévio agendamento com o Gestor do Contrato.

4.3.9 Visando viabilizar a amortização dos investimentos a serem realizados pela CONTRATADA, cada unidade instalada deverá permanecer ativa pelo período mínimo de 12 (doze) meses.

4.4 Serviços a Serem Executados

4.4.1 Fornecer os componentes da solução Ponto Principal, contemplando infraestrutura para instalação dos equipamentos de transmissão, necessária à prestação dos serviços e à integração com o ambiente operacional do Data Center. Os Pontos Principais deverão ser instalados no Data Center do CONTRATANTE.

4.4.2 Fornecer os componentes da solução Links Remotos (LR).

4.4.3 Fornecer os componentes dos Serviços de Wi-Fi Gerenciado.

4.4.4 Efetuar, para todos os elementos fornecidos, a instalação, configuração, manutenção e gerenciamento.

4.5 Sistema de Gestão de Contas

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

a) Ser acessível via WEB e compatível com navegadores padrão de mercado, tais como Internet Explorer, Microsoft Edge, Google Chrome e Mozilla Firefox.

b) Deverá utilizar o protocolo HTTPS para acesso ao portal.

c) Deverá ser em idioma português do Brasil.

d) Deverá possuir, no próprio portal, manual de utilização para auxílio dos usuários.

e) Deverá possuir alerta para acesso à área exclusiva de notificações para o usuário.

f) Deverá possuir recurso de enviar notificações de novas contas para o e-mail dos usuários.

g) Deverá armazenar os dados históricos de contas pelo período mínimo de 60 meses.

h) Deverá permitir visualizar as contas de todos os serviços contratados.

i) A plataforma deverá possibilitar a criação de usuários, sendo que cada novo usuário deverá receber uma notificação por e-mail para completar seu cadastro e ser ativado na plataforma.

j) Deverá permitir a exportação de contas, inclusive várias simultaneamente, no formato PDF.

k) Deverá oferecer visualização de, no mínimo, os seguintes campos: Tipo do Documento, CNPJ, Razão Social do Cliente, Data de Vencimento, Data de Disponibilização da Conta, Valor Total e Mês de Referência da Conta.

l) Deverá apresentar, sempre, a conta atual válida. Caso haja mudança na conta/fatura em virtude de contestações, o portal deve apresentar a conta ajustada com um flag para diferenciação.

4.5.2 O portal ofertado deverá substituir as contas físicas, que não precisarão ser enviadas para o CONTRATANTE.

4.5.3 A CONTRATADA deverá enviar as contas detalhadas por meio digital, via e-mail ou aplicativo instalado no computador do CONTRATANTE.

4.6 Serviços Técnicos Específicos

4.6.1 Service Desk

4.6.1.1 A CONTRATADA deverá disponibilizar, como Service Desk, uma Central de Atendimento especializada para atendimento aos usuários do CONTRATANTE, acessível por número telefônico de Discagem Direta Gratuita (DDG 0800) e portal web.

4.6.1.2 Este serviço telefônico 0800 pode ser um número compartilhado com opção de seleção (a árvore de atendimento não poderá ter mais que duas opções no primeiro nível), para que os usuários façam registros de ocorrências e acompanhamento dos chamados em atendimento.

4.6.1.3 Todo o acionamento ao Service Desk deve ser registrado em portal web, dedicado à solução e fornecido pela CONTRATADA, com geração de ticket a ser informado ao usuário no momento do atendimento. Este ticket será utilizado pelos usuários para acompanhamento das solicitações.

4.6.1.4 O Service Desk deve estar disponível 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, durante todo o ano. A CONTRATADA deverá sempre propor melhorias no atendimento da Central, visando atender satisfatoriamente às demandas do CONTRATANTE.

4.6.1.5 A abertura de chamados através da Internet, pelos usuários do CONTRATANTE, deverá ser através de um portal disponível na web, com recursos de autenticação e requisitos de segura, que garantam a confidencialidade das informações do CONTRATANTE.

4.6.1.6 A CONTRATADA deve manter, em sua base de dados, o cadastro atualizado de todos os serviços vigentes nos contratos, para que possa haver a correlação de serviços e incidentes com todos os ativos contratados, a fim de garantir ações corretivas que permitam a operação dentro dos limites estabelecidos no acordo de qualidade de serviço.

4.6.1.7 Haverá duas modalidades de chamado que poderão ser abertas:

a) Serviços: chamados para demandas como ativação e desativação de LR e Wi-Fi, mudança de endereço de instalação, alteração de velocidade, remanejamento de equipamentos, configuração de rede e roteadores, entre outros.

b) Incidentes: chamados decorrentes de indisponibilidade total e/ou parcial de LR ou Wi-Fi, defeito e/ou sinistro de equipamentos, e perda de desempenho.

4.6.1.8 Todo serviço ou incidente deve ser associado ao ativo previamente cadastrado na base de dados do portal.

4.6.1.9 Ao receber uma solicitação para abertura de chamado, o atendente deverá registrar as seguintes informações: Nome da Unidade, Nome do responsável, Número de telefone de contato, Endereço da Unidade, Nome da Contratada, Categoria (LR ou Wi-Fi), Número de designação do ativo e Descrição do chamado/serviço.

4.6.1.10 A depender da categoria requerida (serviço ou incidente), deverão ser registradas outras informações adicionais da solicitação. Exemplificando, caso a solicitação seja de mudança de endereço do circuito, deverá ser registrado o novo endereço de instalação do LR; caso a solicitação seja de alteração de velocidade, deverá ser registrada a nova velocidade requerida para o LR. A categorização dos chamados e a estruturação das informações adicionais deverão ser definidas em comum acordo com a CONTRATADA.

4.6.1.11 Após o registro deverá ser fornecido ao solicitante o número da ocorrência que lhe foi atribuído (por telefone, correio eletrônico ou pela web).

4.6.1.12 Para os chamados da modalidade de Incidente, a CONTRATADA deverá promover atualizações no sistema com periodicidade máxima de 30 minutos durante o tempo necessário para solução do incidente, permitindo o acompanhamento das ações adotadas para sua resolução. Quando solucionado, deverá ser validado pelo responsável do chamado para ser encerrado.

4.6.1.13 Para os chamados da modalidade de Serviços ainda em andamento, a CONTRATADA deverá promover atualizações no sistema em periodicidade a ser definida com a CONTRATADA, mostrando o status do atendimento da solicitação. Quando concluído o Serviço, deverá ser validado e homologado pelo responsável do chamado para ser encerrado.

4.6.1.14 A CONTRATADA deverá acompanhar os chamados tanto de Incidente quanto de Serviços.

4.6.1.15 A CONTRATADA deverá arcar com todos os custos operacionais do Service Desk, inclusive de mão de obra (atendentes, supervisores, gerentes, etc), equipamentos (microcomputadores dos atendentes, PABX, roteadores, etc.), mobiliários e espaço físico. A estrutura deste atendimento deve ser em ambiente externo ao CONTRATANTE e não é exigida exclusividade.

4.6.1.16 Este serviço deverá obedecer às melhores práticas de Gerenciamento de Serviços, adotando-se como modelo o ITIL (Information Technology Infrastructure Library).

4.6.1.17 A CONTRATADA deverá disponibilizar relatórios e arquivos que permitam ao CONTRATANTE avaliar e auditar a performance do serviço.

4.6.1.18 A CONTRATADA deverá fornecer ao CONTRATANTE, mensalmente ou sob demanda, relatórios de atendimento técnico contendo, no mínimo, as seguintes informações: Unidade afetada, Nome da Contratada, Categoria (LR ou WiFi), Número de designação do ativo, Data e hora do registro da ocorrência, Problema reportado, Data e hora da resolução do problema, Solução apresentada ao problema, Fonte do incidente, Causa raiz e Ação de mitigação.

4.6.1.19 As informações referentes aos chamados efetuados deverão estar disponíveis para consulta durante todo o contrato, pelo prazo mínimo de 1 (um) ano a partir da data do chamado para consulta on-line e indefinidamente para consultas sob demanda, que deverão ser respondidas em até 3 (três) dias úteis.

4.6.1.20 O Service Desk deverá possuir uma base de dados contendo o roteiro e o checklist que serão seguidos no atendimento aos clientes, assim como o registro de problemas mais frequentes com suas respectivas soluções. A base de dados deverá ser disponibilizada para o CONTRATANTE em formato eletrônico.

4.6.1.21 Visando melhorias no nível de serviço prestado, o CONTRATANTE poderá, quando oportuno, solicitar melhorias no sistema de gestão do Service Desk. Tais implementações não estão relacionadas com arquiteturas da solução ou características estruturantes do sistema, mas a mudanças de leiautes de relatórios, tabelas e gráficos, visando atender necessidades específicas.

4.6.1.22 Na data de expiração do contrato, todo o registro de ocorrências, conhecimentos e procedimentos relacionados aos atendimentos atualizado até as últimas atividades efetuadas deverá ser transferido ao CONTRATANTE, sendo esta condição indispensável para a devolução da garantia contratual. Estas informações deverão ser entregues em mídia digital, formato texto, com todos os campos sendo nomeados e discriminados.

4.6.2 Gerenciamento de Ambiente

4.6.2.1 Deve contemplar módulos de gerência de falhas, desempenho, disponibilidade, relatórios e gestão de nível de serviço.

4.6.2.2 A solução deverá disponibilizar portal web para visualização de informações on-line, de forma gráfica, para o acompanhamento e monitoração do estado global e detalhado do ambiente.

4.6.2.3 O serviço de gerenciamento de acessos da CONTRATADA deverá atuar de forma proativa, antecipando-se aos problemas na rede e garantindo o cumprimento do Acordo de Nível de Serviço (ANS), realizando abertura, acompanhamento e fechamento de chamados de falhas relacionadas com indisponibilidade, operando em regime 24x7, todos os dias do ano.

4.6.2.4 O portal web a ser disponibilizado deve permitir o acesso a todos os recursos e módulos através de única autenticação, sem a necessidade de realizar outros logins para acessar qualquer outro recurso de gerenciamento.

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

4.6.2.6 Deverá permitir acessos de usuários com perfis diferenciados, com limitação de acesso a consoles, dispositivos, menus, alarmes e indicadores, entre outros.

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

4.6.2.8 A solução deverá permitir a criação de grupos de perfis de acesso, que serão associados a tipos de usuários.

4.6.2.9 Os perfis deverão prever configurações em níveis de alertas, equipamentos, interfaces, aplicações, funcionalidades de monitoração, inventário, entre outros.

4.6.2.10 O Portal web deve ser acessível sem necessidade de instalação de *clients* específicos. Portanto, não serão aceitas soluções que não sejam nativas em web ou que requeiram a instalação de agentes nos desktops dos colaboradores do CONTRATANTE.

4.6.2.11 O acesso deverá ser via web, padrão HTTP/HTTPS, e em português, portanto não serão aceitas soluções que não possuam interface de usuário em português do Brasil.

4.6.2.12 A solução deverá ser acessível através dos principais browsers do mercado, tais como, Internet Explorer, Firefox, Google Chrome e Safari.

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

4.6.2.14 A solução de gerenciamento de rede deverá gerar alertas quando os thresholds “limites” configurados para um componente monitorado sejam excedidos, como, por exemplo, utilização de CPU, memória, interfaces, volume de erros ou tempo de resposta de serviços.

4.6.2.15 A solução deverá fornecer, através do portal, visualização de informações da rede, on-line (em intervalos de 5 minutos e de forma gráfica), apresentando, no mínimo, os seguintes itens para cada um dos elementos monitorados:

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

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

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

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

e) Ocupação de memória e CPU dos roteadores.

f) Retardo dos enlaces, separados por dia e mês.

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

h) Taxa de erros, em erros por segundo.

i) Latência, em milissegundos.

4.6.2.16 A solução de gerenciamento de rede deverá permitir a apresentação de indicadores que reflitam o ANS (Acordo de Nível de Serviço) dos serviços contratados.

4.6.2.17 A solução deve fornecer o inventário dos equipamentos e enlaces da rede contendo, no mínimo, as seguintes informações:

a) Enlace: designação, tecnologia e nível de serviço.

b) Roteador: fabricante, modelo e configuração física (interfaces, memória, slots, dentre outros).

c) Endereçamento lógico: endereços IP e máscaras.

4.6.2.18 A solução deve possuir funcionalidade de backup de configuração dos elementos gerenciados, alarmes para alterações realizadas e relatório de mudanças.

4.6.2.19 A solução deverá permitir adicionar a nomenclatura conhecida pelo CONTRATANTE para os recursos gerenciados.

4.6.2.20 A solução de Gerenciamento deverá realizar registro de todas as ocorrências de alarmes/eventos em log de históricos e/ou em base de dados, contendo informações de data e hora de ocorrência, identificando os recursos gerenciados e armazenando os dados pelo período mínimo de 6 (seis) meses.

4.6.2.21 A solução de Gerenciamento deverá permitir a criação de Relatórios. Tais relatórios devem poder ser exportados conforme os principais métodos como: pdf, csv, xls. A seguir são apresentados os relatórios desejados:

a) Relatórios de desempenho sumarizado por período especifico.

b) Relatórios de desempenho classificados em uma visão TOP N, como exemplo, Top N Roteadores % de utilização de CPU, Top N Interfaces % de utilização, Top N Interfaces com descartes, dentre outros.

c) Relatórios de disponibilidade com períodos específicos.

d) Dashboards relacionando falhas, desempenho e disponibilidade.

e) Dashboards executivos com visões sumarizadas de indicadores operacionais (Taxa de Reincidência, Reparos no Prazo e Taxa de Falha).

4.6.3 Gerenciamento da Solução de Segurança

4.6.3.1 O serviço deve contemplar a monitoração, em regime 24 x 7, dos dispositivos de segurança mencionados, através de Centro de Operações de Segurança da CONTRATADA.

4.6.3.2 A monitoração pelo Centro de Operações de Segurança deve atuar de modo proativo e deverá mitigar possíveis problemas de segurança.

4.6.3.3 O Centro de Operações de Segurança deverá possuir gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos.

4.6.3.4 Deverá ser realizado o gerenciamento dos equipamentos de segurança fornecidos, administrando-os e configurando-os de forma a minimizar possíveis incidentes de Segurança.

4.6.3.5 A implantação de novas regras ou alteração de regras nos equipamentos de segurança deve sempre ocorrer mediante prévia solicitação e/ou anuência do CONTRATANTE.

4.6.3.6 Sempre que detectadas vulnerabilidades em regras que possam comprometer a segurança do ambiente, a CONTRATADA deve sugerir ao CONTRATANTE alterações nas configurações dos equipamentos de modo a melhorar a proteção da rede.

4.6.3.7 As soluções de segurança fornecidas devem ser atualizadas (Firmware e SO), sempre que o fabricante informar sobre a necessidade, seja por questões de segurança ou melhorias sistêmicas.

4.6.3.8 O gerenciamento da solução de segurança deve realizar a coleta de estatísticas de desempenho e falhas de segurança em todos os equipamentos da plataforma.

4.6.3.9 Os logs devem ser armazenados pelo período mínimo de 60 (sessenta) dias.

4.6.3.10 Em caso de incidentes ou falhas, o Centro de Operações de Segurança deverá classificá-los por severidade.

4.6.3.11 Deverá ser fornecido um conjunto de relatórios, acessados via Portal Web, para permitir gerenciamento e acompanhamento online da segurança, do desempenho da rede e a gestão ANS contratado, com as seguintes características:

a) Disponibilizar informações gerenciais de desempenho relativas aos serviços contratados.

b) Permitir visualização online de relatórios de Firewall: conexões ativas, conexões rejeitadas e utilização de CPU e memória do(s) CPE (Equipamento de Segurança).

c) Permitir a visualização online de relatórios de IDS/IPS.

d) Permitir a visualização das políticas de segurança aplicadas aos equipamentos da Solução de Segurança dos Links Remotos.

e) Apresentar informações sobre o histórico de relatórios de segurança e de desempenho do serviço (busca por data, designação de circuito, tipo de relatório).

4.6.4 Ponto Principal

4.6.4.1 Conexão permanente e dedicada ao Backbone da CONTRATADA, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante toda a vigência do contrato, para comunicação de dados entre os data centers dos órgãos e suas respectivas unidades.

4.6.4.2 Deverá ser usada a tecnologia MPLS, integrada a VPN, e de caráter simétrico (velocidade upstream = velocidade downstream) com banda garantida de 100% (cem por cento).

4.6.4.3 Os Pontos Principais de Rede deverão ser integrados e compatíveis aos ambientes operacionais existentes.

4.6.4.4 A redundância deve operar de modo automático, ou seja, sem intervenção manual, utilizando os encaminhamentos físicos distintos instalados entre os data centers dos órgãos e as estações prediais distintas da CONTRATADA.

4.6.4.5 A implantação inicial do Ponto Principal de Rede deverá ser concluída em até 60 (sessenta) dias após a data de assinatura do Contrato.

4.6.4.6 A solução completa do Ponto Principal de Rede deverá contemplar o fornecimento de, no mínimo, dois roteadores, dois equipamentos de acesso e meios de acessos redundantes de conexões físicas utilizando meio ótico, com dupla abordagem por estações prediais distintas, as quais deverão possuir pontos de roteamento que se interligam ao backbone da CONTRATADA, garantindo a contingência automática dos serviços contratados, devendo ser implementado pela CONTRATADA no prazo de até 60 (sessenta) dias após a assinatura do contrato.

4.6.4.7 Os Pontos Principais de Rede deverão contemplar plano de continuidade e contingência com a descrição dos recursos e meios envolvidos, visando à garantia da disponibilidade mensal maior ou igual a 99,9%.

4.6.4.8 Os Pontos Principais de Rede deverão possuir média mensal de perda de pacotes inferior ou igual a 1%.

4.6.4.9 A solução dos Pontos Principais de Rede deverão ter, a qualquer tempo, capacidade suficiente para acomodar o pico (somatório) das demandas impostas pelos acessos dos LRs, sem que haja estrangulamento do tráfego de qualquer aplicação. A largura de banda do Ponto Principal deve ser capaz de suportar o tráfego do somatório de todos os Links Remotos do órgão.

4.6.4.10 Deverão ser disponibilizadas, obrigatoriamente, 2 (duas) interfaces no padrão Gigabit Ethernet com conector RJ45, em cada roteador, para conexão com a rede interna (LAN). Caso a demanda de tráfego exceda essa capacidade, a solução dos Pontos Principais de Rede deverá disponibilizar adicionalmente 2 (duas) interfaces 10 Gigabit Ethernet.

4.6.4.11 Os equipamentos dos Pontos Principais de Rede deverão possuir capacidade de suportar o tráfego com banda completamente ocupada, sem que os limites de 80% de utilização da memória e 80% de utilização da CPU sejam excedidos. A CONTRATADA deverá informar estas estatísticas diariamente no Sistema de Gerenciamento.

4.6.4.12 O CONTRATANTE será responsável pela infraestrutura necessária para instalação dos acessos, tal como energia elétrica, aterramento, climatização, espaço físico, racks 19 polegadas e cabeamento estruturado.

4.6.5 Link Remoto Básico

4.6.5.1 O Link Remoto Básico (LRB) é um acesso para navegação na Internet de caráter assimétrico (velocidade upstream ≠ velocidade downstream), com banda garantida de no mínimo 20%.

4.6.5.2 Por se tratar de um link de Internet, não se aplicam os requisitos do item 4.1 REQUISITOS TÉCNICOS GERAIS.

4.6.5.3 Deverá ser fornecido, no mínimo, nas seguintes velocidades:

Sentido Downstream	Sentido Upstream
10 Mbps	1 Mbps
20 Mbps	3 Mbps
50 Mbps	5 Mbps
100 Mbps	10 Mbps
200 Mbps	20 Mbps

4.6.5.4 Deverá ser oferecida garantia de banda conforme resolução nº 575 da ANATEL.

4.6.5.5 Será fornecido mediante análise prévia de viabilidade técnica.

4.6.5.6 A CONTRATADA deve informar o prazo de instalação ou de rejeição do pedido em até 5 (cinco) dias após a solicitação formal, não podendo exceder a 15 (quinze) dias para entrega do acesso.

4.6.5.7 O equipamento de roteamento fornecido para o LR Básico deverá possuir pelo menos 1 (uma) porta Ethernet.

4.6.5.8 O equipamento de roteamento fornecido para o LR Básico deverá ser compatível com protocolo SNMP v2.

4.6.5.9 Deverá ser configurada comunidade de leitura nos roteadores para gerar logs e/ou traps SNMP para um ou mais endereços IP a serem definidos pelo CONTRATANTE.

4.6.5.10 Não será aplicável nenhuma configuração de QoS nessa categoria.

4.6.5.11 Deverá ser fornecido, pelo menos, 1 (um) endereço IP fixo roteável na internet.

4.6.6 Link Remoto Avançado

4.6.6.1 O Link Remoto Avançado (LRA) é caracterizado por um circuito de acesso MPLS, integrado à VPN e de caráter simétrico (velocidade upstream = velocidade downstream).

4.6.6.2 Deverá ser fornecido com tecnologia de acesso metálico até a velocidade de 2 Mbps e fibra ótica a partir de 5 Mbps.

4.6.6.3 Deverá ser fornecido com banda garantida de 100% (cem por cento) da velocidade nominal do LRA.

4.6.6.4 O LRA terá as seguintes opções de velocidades: 2Mbps, 5Mbps, 10Mbps, 20Mbps, 50Mbps, 100 Mbps, 200 Mbps.

4.6.6.5 Existência da necessidade de diferenciação de tráfego de dados.

4.6.6.6 A priorização de tráfego deverá ser permitida com, no mínimo, 04 (quatro) classes de serviço:

a) Classe 1 Dados não prioritários.

b) Classe 2 Dados prioritários.

c) Classe 3 Voz.

d) Classe 4 Vídeo.

4.6.6.7 Quando as aplicações de maior prioridade não estiverem em uso, os recursos do link deverão ser utilizados pelas de menor prioridade.

4.6.6.8 Deverá ser configurado o endereçamento IP LAN definido pelos órgãos.

4.6.6.9 Para o LRA, deverão ser fornecidos equipamentos para segurança da informação com as seguintes características:

a) Funcionalidades de Roteamento, Redes e Segurança, Filtro de Conteúdo, VPN (Virtual Private Network), Autenticação, Registros de Logs, Qualidade de Serviço (QoS) e Modelagem de tráfego, Balanceamento de Carga (SD-WAN) e Controladora de Wi-Fi que devem ser gerenciadas de forma centralizada, compatível com o equipamento da solução adotada (CPE).

b) Os equipamentos fornecidos pela solução para a funcionalidade de segurança devem ter uma arquitetura específica e dedicada (appliance), não podendo ser utilizados equipamentos do tipo servidor de uso genérico. O sistema operacional deve estar integrado à solução, ou seja, hardware e software devem ser integrados em um único equipamento.

c) Garantir que um único equipamento possa atender à totalidade das capacidades exigidas, não sendo aceitos somatórios para atingir os limites mínimos.

d) Devem possuir fonte de alimentação com seleção automática nas tensões 110/220V.

e) Possuir quantidade de memória e processamento suficientes para atendimento de todas as funcionalidades e desempenho, de acordo com a velocidade do LR contratado, solicitados neste Termo de Referência.

f) Garantir que a solução disponibilize, nos equipamentos, acesso a gerência, monitoração, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall NGFW).

g) Garantir que não haja restrição por número de usuários da solução disponibilizada.

h) Permitir monitorar na solução, via protocolo SNMP, falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede.

i) Garantir o envio dos logs para os sistemas de monitoramento do CONTRATANTE de forma simultânea ou programada, caso requerido.

j) Garantir que o gerenciamento da solução suporte acesso via SSH, software cliente ou interface web (HTTPS).

k) Na proteção combinada contra ameaças, a solução instalada deverá ter, de maneira ativa, as funcionalidades de firewall, IPS, antivírus e controle de aplicações especificadas neste termo de referência, com todo o tráfego suportado pelo LR (considerando as métricas de mundo real) e processos automáticos configurados.

l) Para as instâncias virtuais, os equipamentos da solução devem ser disponibilizados com apenas 01 (uma) instância virtual ativa, sendo as demais instâncias ativadas mediante solicitação do CONTRATANTE.

m) A solução de segurança instalada deverá ser compatível com a velocidade CONTRATADA dos LRs, possuir todos os recursos (memória, processamento, I/O e portas de comunicação) necessários ao pleno funcionamento com todas as funcionalidades exigidas pelo CONTRATANTE, com o desempenho satisfatório para atendimento de todo o tráfego gerado na rede local onde o LR esteja instalado, não podendo ultrapassar 80% da sua capacidade operacional (uso de CPU e memória) com todas as funcionalidades habilitadas simultaneamente: últimas assinaturas atualizadas de IPS, Políticas de Segurança implementadas e ativas; Tráfegos diversos, tais como DNS, HTTP, SMTP, HTTPS, FTP e outros protocolos; Ambientes de usuários, tais como redes sociais, plataforma de colaboração e outras aplicações; Recursos de NAT e Logs habilitados.

n) A implantação de novas regras ou alteração das regras existentes nos equipamentos de segurança deve sempre ocorrer mediante prévia solicitação e/ou anuência do gestor de segurança dos órgãos.

o) O CONTRATANTE poderá solicitar a interligação de um link de Internet, seja um LR Básico ou um link de Internet de terceiros, na solução de segurança do LR para que seja possível realizar configurações de gerenciamento de tráfego dos links. O equipamento de segurança deve ser capaz de manter a comunicação com serviços hospedados no Data Center do CONTRATANTE através do LR Avançado ou Plus e o acesso à Internet através do LR Básico.

p) A solução de segurança deve ser capaz de criar VPN, utilizando o link de Internet, com o Data Center do CONTRATANTE para ser utilizado como uma alternativa em caso de queda do link principal, seja ele LR Avançado ou Plus.

4.6.7 Link Remoto Plus

4.6.7.1 O Link Remoto Plus (LRP) é caracterizado por ser um serviço para atendimento a Ponto Remoto com maior criticidade e menor tolerância a paralisações.

4.6.7.2 O LRP deverá possuir dois acessos redundantes de conexões físicas distintas.

4.6.7.3 Os acessos redundantes podem ser entregues através de uma das seguintes alternativas:

a) Dupla abordagem com cabos óticos por caminhos distintos.

b) 1º acesso por cabo ótico e 2º acesso por equipamento de radiofrequência.

4.6.7.4 A taxa de comunicação de ambos os acessos deve ser a mesma.

4.6.7.5 O LRP deverá contemplar o fornecimento de equipamentos redundantes, no mínimo, dois roteadores, dois equipamentos de acesso e dois dispositivos de segurança, de modo que seja garantida a contingência automática em caso de falha de alguns dos equipamentos (failover).

4.6.7.6 Deverá possuir recursos de proteção do tráfego por criptografia através de túneis VPN IPSec e otimização do uso da rede por balanceamento inteligente do tráfego.

4.6.7.7 O LRP terá as seguintes opções de velocidades: 5Mbps, 10Mbps, 20Mbps, 50Mbps, 100 Mbps, 200 Mbps.

4.6.7.8 O LRP deve possuir as mesmas características técnicas do LRA, tais como utilizar tecnologia MPLS, ser integrado a uma VPN, ser de caráter simétrico, ser fornecido com 100% de garantia de banda da velocidade nominal do LR, dentre outros.

4.6.7.9 Para o LRP, em caráter excepcional e caso seja conveniente ao órgão solicitante, os serviços que estiverem publicados na Internet devem ser acessados diretamente através de um link dedicado Internet em substituição a um dos links MPLS previstos nessa categoria.

4.6.7.10 O LRP deverá possuir a mesma priorização de tráfego com, no mínimo, 04 (quatro) classes de serviços:

a) Dados não prioritários;

b) Dados prioritários;

c) Classe de voz;

d) Classe de vídeo.

4.6.7.11 O LRP deverá ser fornecido com solução de segurança de informação com as mesmas características do LRA.

4.6.7.12 A solução de segurança de informação no LRP deve ser entregue em topologia de Alta Disponibilidade (HA), ou seja, deverão existir dois dispositivos de segurança garantindo a contingência automática em caso de falha de um dos equipamentos.

4.6.7.13 Para este tipo de link não será permitido que o acesso seja atendido através de satélite.

4.6.8 Segurança dos Links Remotos – SLR

4.6.8.1 Devem ser disponibilizados 4 (quatro) tipos de equipamentos com os seguintes requisitos técnicos:

a) Solução de segurança TIPO 1 Para LRs com velocidade 2 (dois) até 10 (dez) Mbps:

- Possuir, no mínimo, 5 (cinco) interfaces RJ45 GigabitEthernet.
- Throughput de Firewall de, no mínimo, 2,5 Gbps
- Throughput de IPsec de, no mínimo, 90 Mbps
- Throughput para proteção combinada de ameaças de, no mínimo, 150 Mbps.
- Suportar, no mínimo, 1.800.000 conexões simultâneas.
- Suportar, no mínimo, 20.000 novas conexões por segundo.
- Suportar, no mínimo, 3 instâncias virtuais.

b) Solução de segurança TIPO 2 Para LRs com velocidade de 20 (vinte) Mbps:

- Possuir, no mínimo, 5 (cinco) interfaces RJ45 GigabitEthernet.
- Throughput de Firewall de, no mínimo, 3 Gbps
- Throughput de IPsec de, no mínimo, 2 Gbps
- Throughput para proteção combinada de ameaças de, no mínimo, 180 Mbps.
- Suportar, no mínimo, 1.200.000 conexões simultâneas.
- Suportar, no mínimo, 30.000 novas conexões por segundo.
- Suportar, no mínimo, 3 instâncias virtuais.

c) Solução de segurança TIPO 3 Para LRs com velocidade de 50 (cinquenta) até 100 (cem) Mbps:

- Possuir, no mínimo, 5 (cinco) interfaces RJ45 GigabitEthernet.
- Throughput de Firewall de, no mínimo, 7 Gbps
- Throughput de IPsec de, no mínimo, 4 Gbps
- Throughput para proteção combinada de ameaças de, no mínimo, 240 Mbps.

- Suportar, no mínimo, 2.000.000 conexões simultâneas.
- Suportar, no mínimo, 30.000 novas conexões por segundo.
- Suportar, no mínimo, 3 instâncias virtuais.

d) Solução de segurança TIPO 4 Para LRs com velocidade de 200 (duzentos) Mbps:

- Possuir, no mínimo, 5 (cinco) interfaces RJ45 GigabitEthernet.
- Throughput de Firewall de, no mínimo, 20 Gbps
- Throughput de IPsec de, no mínimo, 8 Gbps
- Throughput para proteção combinada de ameaças de, no mínimo, 1 Gbps.
- Suportar, no mínimo, 2.000.000 conexões simultâneas.
- Suportar, no mínimo, 130.000 novas conexões por segundo.
- Suportar, no mínimo, 3 instâncias virtuais.

4.6.8.2 As funcionalidades de Roteamento, Redes e Segurança da solução de segurança para os Links Remotos devem atender, no mínimo, os seguintes requisitos:

a) Ter tecnologia de firewall do tipo Statefull.

b) Ser otimizada para análise de conteúdo de aplicações em camada 7.

c) Permitir, para o gerenciamento da solução, interface de administração via web no próprio dispositivo, integrada com bases de usuários LDAP, LDAP/AD.

d) Realizar VLAN com tags padrão 802.1q.

e) Possuir suporte a agregação de links 802.3ad e LACP.

f) Realizar política baseada em roteamento (policy based routing) ou política baseada em encaminhamento (policy based forwarding).

g) Realizar roteamento multicast (PIM-SM e PIM-DM).

h) Realizar DHCP Relay e DHCP Server.

i) Possuir suporte a sub-interfaces ethernet lógicas.

j) Funcionar com tradução de endereços de rede (NAT) dinâmica (Many-to-1 e Many-to-Many).

k) Funcionar com NAT estática (1-to-1, Many-to-Many, bidirecional 1-to-1).

l) Funcionar com tradução de porta (PAT).

m) Funcionar com NAT de Origem e NAT de Destino simultaneamente.

n) Suportar NAT64 e NAT46.

o) Suportar NAT66, e implementar quando solicitado pelo Contratante.

p) Implementar o protocolo ICMP.

q) Implementar balanceamento de link por hash do IP de origem, como também por hash do IP de origem e destino.

r) Suportar o balanceamento de no mínimo dois circuitos (links), implementando balanceamento de carga, sendo possível definir o percentual de tráfego que será escoado por cada um dos links.

s) Possuir proteção contra falsificação de endereços (anti-spoofing).

t) Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).

u) Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3).

v) Suportar OSPF gracefulrestart.

w) Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

x) Ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3).

y) Suportar Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação.

z) Suportar Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas.

aa) Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

ab) Possuir suporte à criação de sistemas virtuais no mesmo equipamento (appliance).

ac) Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente.

ad) Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolação das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos).

ae) Operar em caráter permanente para as funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, de-criptografia SSL ou SSH, e protocolos de roteamento dinâmico.

af) Realizar controles de políticas por porta e protocolo.

ag) Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

ah) Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança.

ai) Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS).

aj) Realizar controle, inspeção e descriptografia de SSL por política, para tráfego de entrada (Inbound) e Saída (Outbound).

ak) Realizar offload de certificado em inspeção de conexões SSL de entrada (Inbound).

al) Descriptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2.

am) Realizar controle de inspeção e descriptografia de SSH ou SSL por política.

an) Implementar objetos e regras, inclusive para protocolos de roteamento multicast.

ao) Realizar, no mínimo, três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com notificação do bloqueio ao usuário, Drop com opção de envio de ICMP para máquina de origem do tráfego, TCP-Reset para o cliente, TCP-Reset para o server ou para os dois lados da conexão.

ap) Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

aq) Possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

ar) Realizar a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

as) Reconhecer, no mínimo, 2.000 aplicações diferentes, incluindo (mas não limitado a) tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail, entre outros.

at) Inspecionar o payload de pacote de dados com o objetivo de detectar, através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo.

au) Detectar aplicações através de análise comportamental do tráfego observado, incluindo (mas não limitado a) Bittorrent criptografado e aplicações VOIP que utilizam criptografia proprietária.

av) Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da deep web (ex.: rede Tor).

aw) Descriptografar pacotes, para tráfego criptografado SSL, a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

ax) Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo (mas não limitado a) aplicações usando HTTP. A decodificação de protocolo também

deve identificar funcionalidades específicas dentro de uma aplicação, incluindo (mas limitado a) compartilhamento de arquivos.

ay) Atualizar a base de assinaturas de aplicações automaticamente.

az) Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD.

ba) Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários.

bb) Possibilitar a adição de controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente à possibilidade de habilitar controle de aplicações em algumas regras.

bc) Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos.

bd) Manter a segurança da rede eficiente, realizando o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

be) Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE.

bf) Criar assinaturas personalizadas com o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP ou usando decodificadores de, pelo menos, os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL.

bg) Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

bh) Permitir a configuração de alertas quando uma aplicação for bloqueada.

bi) Possibilitar que o controle de portas seja aplicado para todas as aplicações.

bj) Possibilitar a diferenciação de tráfegos Peer-to-Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos.

bk) Possibilitar a diferenciação de tráfegos de mensageiros instantâneos (AIM, Hangouts, Facebook Chat, etc.), possuindo granularidade de controle/políticas para os mesmos.

bl) Possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o “Hangouts chat” e bloquear a chamada de vídeo.

bm) Possibilitar a diferenciação de aplicações Proxies (psiphon3, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos.

bn) Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pelo CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol, etc.), nível de risco, categoria, uso de técnicas evasivas utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos) etc.

bo) Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance.

bp) Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).

bq) Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo.

br) Implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Anti-spyware e Antivírus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo.

bs) Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração.

bt) Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança.

bu) Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do Contratante Aderente, para aplicações de políticas baseadas nesses grupos.

bv) Possibilitar a configuração de diferentes políticas de controle de ameaças e ataq baseados em políticas do firewall, considerando usuários, grupos de usuários, local ou b de usuários externas (LDAP, LDAP/AD).

bw) Permitir o uso de exceções por IP de origem ou de destino nas regras e assinatura.

bx) Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

by) Permitir o bloqueio de vulnerabilidades.

bz) Permitir o bloqueio de programas exploradores de vulnerabilidades (exploits) conhecidos.

ca) Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo. Análise para detecção de anomalias de protocolo. Análise heurística. Desfragmentação de IP. Remontagem de pacotes de TCP. Bloqueio de pacotes malformados.

cb) Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood, etc..

cc) Detectar e bloquear a origem de programas de varredura de portas (portscans).

cd) Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões.

ce) Possuir assinaturas para bloqueio de ataques de buffer overflow.

cf) Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações.

cg) Permitir o bloqueio de vírus e spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.

ch) Identificar, alertar e bloquear comunicação com botnets.

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

cj) Suportar a captura de pacotes (PCAP), por assinatura de IPS ou ACL e controle de aplicação ou anti-malware.

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

cl) Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.

cm) Identificar nos eventos o país de onde partiu a ameaça.

cn) Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

co) Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.

4.6.8.3 As funcionalidades de Filtro de Conteúdo da solução de segurança para os Links Remotos devem atender, no mínimo, os seguintes requisitos:

a) Possuir, no mínimo, 50 (cinquenta) categorias ou subcategorias de classificação de URL.

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

c) Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.

d) Criar políticas baseadas na visibilidade e controle de acesso que permitam identificar usuários versos URL's, através da integração com serviços de diretório (LDAP/Active Directory) e base de dados local.

e) Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.

f) Permitir a criação de categorias de URLs customizadas.

g) Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs.

h) Deve possuir a função de exclusão de URLs do bloqueio, por categoria.

i) Permitir a customização de página de bloqueio.

4.6.8.4 As funcionalidades de Balanceamento de Carga (SD-WAN) para os Links Remotos devem atender, no mínimo, os seguintes requisitos:

a) A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

b) A solução SD-WAN deve suportar micro-segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

c) A solução SD-WAN deve suportar NAT em contexto de saída (NAT Outbound) para um pool de IPs públicos.

d) Na solução deve ser provida gerência centralizada pela CONTRATADA.

e) A solução dever ser capaz de prover função Zero Touch Provisioning com suporte a endereçamentos estáticos e dinâmicos, e que sejam suportados múltiplos links WAN.

f) A função de Zero Touch Provisioning deve ser escalável, suportando um mínimo de 15 (quinze) dispositivos em uma mesma comunidade VPN neste contexto.

g) A solução deve suportar RFC7018 ADVPN entre Ponto Central e Unidades Remotas com autenticação baseada em padrão x.509 Certificados Digitais e também PSK.

h) A solução deve ser capaz de criar VPN Full-Mesh, de forma automática, e sem que o administrador precise configurar site por site.

i) A configuração VPN IPSec deverá oferecer suporte para versão IKE v2.0.

j) A configuração VPN IPSec deverá oferecer suporte para DH Group 14 e 15.

k) A solução deve ser capaz de prover uma arquitetura onde em uma comunicação Ponto Central x Unidade Remota, em que a Unidade Remota também esteja utilizando seu acesso de Internet local para se comunicar com outro elemento de SD-WAN em nuvem pública e caso este circuito venha a falhar, que seja utilizado o túnel VPN com Matriz, para possibilitar a comunicação da Unidade Remota com esta máquina na Nuvem Pública.

l) A solução deve suportar aos seguintes protocolos: IPv6, VRRP ou Equivalente, VRF, BGP, OSPF, RIPv2, 802.1Q, BFD, Dynamic Multipath, Policy Based Routing.

m) Reconhecimento em camada 7 totalmente segregado da camada 4.

n) Deve, de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP ou range de IPs de destino.

o) O reconhecimento de aplicações, deve ser atualizado de forma dinâmica e totalmente transparente para o dispositivo.

p) O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados.

q) Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de, pelo menos, mais de 1.000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, entre outros).

r) A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.

s) A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e packet loss, onde seja possível configurar um valor de theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

t) A solução deve permitir modificar configuração de tempo de checagem em segundos para cada um dos links.

u) A solução deve permitir a configuração de regras onde o failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja x% (com x variando de 10 à 50) do seu valor de Saúde melhor que o link atual.

v) A solução deve permitir a configuração de regras onde o failback (retorno à condição ini apenas ocorra dentro de um espaço de tempo de x segundos, configurável pelo administra do sistema.

w) A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

x) A solução deve permitir a configuração de políticas de QoS em valores onde o máximo corresponda à totalidade de largura de banda disponível no equipamento.

y) A solução deve permitir a consulta via SNMPv2/v3 referente aos seguintes dados: Estado atual dos links SD-WAN. Latência. Jitter. Packet Loss. Pacotes enviados / Pacotes Recebidos. Link Bandwitdh.

z) VRF associada.

aa) A solução deve possibilitar a distribuição de peso em cada um dos links que compõe o SD-WAN, a critério do usuário, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em: Número de Sessões. Volume de Tráfego. IP de Origem e Destino. Transbordo de Link (Spillover).

ab) A solução física deve apresentar compatibilidade com modens USB (3G/4G), onde estes sejam capazes de funcionar como circuito Ativo x Ativo em relação à saída principal de internet, e também alternativamente funcionar em uma arquitetura Ativo x standby, onde apenas seja acionado na eventualidade de falha no link principal.

ac) A solução deve possuir capacidade de autenticar usuários para administração do Equipamento, através de base de dados: Local. Integrada a servidor TACACS+. Integrada a servidor LDAP.

ad) Provisionamento de templates SD-WAN que considere critérios relacionados a: que interfaces seriam consideradas SD-WAN (combinação: wan1 e wan2, etc), Jitter, Latência e Packet Loss para mensuração de saúde dos links.

ae) Criação de Regras SD-WAN.

af) A Alta Disponibilidade provida pela solução de SD-WAN, independente em suas modalidades físicas ou virtual, deverá obedecer os seguintes critérios: Suportar Balanceamento Ativo Ativo, Suportar Balanceamento Ativo Passivo, Suportar Balanceamento de até 4 peers, Suportar Balanceamento distribuído geograficamente.

ag) A solução SD-WAN deve oferecer troubleshooting em console de linha de comando ou gráfica, onde seja possível: executar Packet sniffer do tráfego interessante, filtrando por: IP e Porta, Realizar debug detalhado das fases de negociação VPN.

ah) A Solução SD-WAN deve oferecer relatórios de: aplicações mais utilizadas com respectiva largura de banda, Shapping de Tráfego SD-WAN, IPs de Destino mais utilizados com respectivo número de Sessões e Largura de Banda associados.

ai) A solução SD-WAN deve suportar marcação de pacotes DSCP nas definições e regras para tráfego.

4.6.8.5 As funcionalidades de Qualidade de Serviço (QoS) e Modelagem de Tráfego da solução de segurança para os Links Remotos devem atender, no mínimo, os seguintes requisitos:

a) Realizar Traffic Shaping para a solução de segurança dos Acessos Dedicados.

b) Criar políticas de QoS e Traffic Shaping por endereço de origem e destino.

c) Realizar a criação de políticas de QoS e Traffic Shaping por porta.

d) Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade.

e) Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI(Command Line Interface).

f) Realizar QoS (Traffic Shapping) em interfaces agregadas ou redundantes.

4.6.8.6 As funcionalidades de Filtro de Dados da solução de segurança para os Links Remotos devem atender, no mínimo, os seguintes requisitos:

a) Identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos.

b) Identificar arquivos criptografados e aplicar políticas sobre esses tipos de arquivos.

c) Identificar e prevenir a transferência de informações definidas como sensíveis CONTRATANTE (por exemplo, número de cartão de crédito, etc.) possibilitando a criação novos tipos de dados via expressão regular

4.6.8.7 As funcionalidades de Redes Virtuais Privadas (VPNs) da solução de segurança para os Links Remotos devem atender, no mínimo, os seguintes requisitos:

a) Criar VPN dos tipos Site-to-Site.

b) Criar IPSec VPN e SSL VPN.

c) Suportar nativamente a criação de VPN IPSec utilizando 3DES.

d) Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128, 192 ou 256 bits.

e) Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1.

f) Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.

g) Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2).

h) Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI.

i) Possuir interoperabilidade com, no mínimo, os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

j) Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting).

k) Criar políticas de controle de aplicações, IPS, Antivírus, Anti-spyware e filtro de URL para tráfego das unidades remotas conectados na VPN.

l) Permitir autenticação via AD/LDAP, Secure id, certificado e base de usuários local.

m) Aplicar políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

4.6.9 Segurança do Data Center – SDC

4.6.9.1 Além das exigências contidas no item precedente, o serviço de Links Remotos para o Tribunal de Justiça deverá incluir uma solução de segurança de acesso ao Data Center, assim garantindo a proteção integral do tráfego entre as diversas unidades e o Data Center.

4.6.9.2 A CONTRATADA deverá fornecer, instalar e manter todos os recursos (hardware, software, atualizações) envolvidos e necessários para a operação da Solução de Segurança da Data Center.

4.6.9.3 Todo o tráfego de entrada e saída para os serviços de Internet via Ponto de Troca de Tráfego será inspecionado de forma integral, ou seja, fazendo todos os filtros de segurança contratados neste serviço: Firewall, IPS e Controle de Aplicação e Prevenção de Ameaças.

4.6.9.4 O Serviço de Segurança do Data Center deve disponibilizar todos os recursos da solução adotada para garantir as seguintes funcionalidades detalhadas neste termo de referência:

a) Solução de Rede e Firewall.

b) Solução de Filtro de Conteúdo.

c) Solução de Controle de Aplicações.

d) Solução de Prevenção de Ameaças.

e) Solução de Autenticação Centralizada (identificação do usuário e técnicos).

f) Solução de Qualidade de Serviço (QoS) e Modelagem de Tráfego.

g) Solução de Filtro de Dados.

h) Solução de Redes Virtuais Privadas (VPNs).

4.6.9.5 Caberá à CONTRATADA fornecer a solução que abrange todas as funcionalidades deste Serviço e ao CONTRATANTE a operacionalização de atividades de configuração, implementação de regras de segurança, disponibilização de acessos e dentre outros).

4.6.9.6 Os equipamentos que compõem a Solução de Segurança Data Center devem atender seguintes requisitos gerais:

a) Serem fornecidas atualizações, durante a vigência do contrato, dos softwares/firmwares que compõem a solução, para suas versões estáveis e livres de vulnerabilidades conhecidas, com janelas de manutenção combinadas, e sob a anuência do CONTRATANTE.

b) Fornecer ao CONTRATANTE credenciais de acesso de leitura e escrita a toda a solução, e a todos os seus recursos, que compõem este serviço.

c) Garantir o funcionamento total dos recursos de segurança, assim como as atualizações de bases de dados de todas as funcionalidades, durante a vigência do contrato, com toda a documentação disponível no site do fabricante.

d) Possuir interface de administração via web no próprio dispositivo, permitindo configurá-lo diretamente através de um navegador web.

e) Possuir interface de administração via linha de comando CLI (Command Line Interface).

f) Possuir bases de dados, assinaturas e funcionalidades (engines) de segurança desenvolvidas pelo mesmo fabricante ou parceiros, desde que atendam a todas as especificações solicitadas e não haja perda de funcionalidades.

g) Garantir e suportar acesso para gerenciamento da solução via SSH e cliente WEB (HTTPS).

h) Permitir a aplicação de políticas de senhas de acesso na solução adotada.

i) Todos os dispositivos disponibilizados para uso devem ser acessados por protocolos seguros e os usuários devem estar cadastrados em uma base de dados LDAP ou LDAP/AD, disponibilizada pelo CONTRATANTE.

j) A Solução deve prover exportação de dados via formato csv.

k) Todos os equipamentos disponibilizados para o Serviço de Segurança Data Center devem ter capacidade de funcionar em alta disponibilidade (HA High Availability) ativo/ativo ou ativo/passivo de modo transparente.

l) Os equipamentos disponibilizados para o Serviço de Segurança Data Center devem ser fornecidos sempre aos pares, ou seja, dois equipamentos idênticos, de modo que possam funcionar em alta disponibilidade.

m) Ser fornecido em plataforma com funcionalidades de Next Generation Firewall (NGFW), e console de gerência. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

n) Deve ser fornecido hardware com arquitetura específica e dedicada para funcionalidades de segurança (appliance), não podendo ser utilizado servidor de uso genérico. O sistema operacional deve estar embutido no hardware proposto, ou seja, hardware e software devem ser integrados em um único equipamento.

o) Garantir que um único equipamento possa atender a totalidade das capacidades exigidas, não sendo aceitos somatórios para atingir os limites mínimos.

p) Possuir quantidade de recursos (memória, processamento, I/O e portas) suficientes para atendimento de todas as funcionalidades solicitadas, com desempenho (performance) satisfatório para suportar todo o tráfego sem ultrapassar 70% da capacidade de uso de CPU e memória, com todas as funcionalidades habilitadas simultaneamente, como:

- Últimas assinaturas atualizadas de IPS.
- Políticas de segurança implementadas e ativas.
- Tráfegos diversos, tais como: DNS, HTTP, SMTP, HTTPS, FTP e outros protocolos.
- Ambientes de usuários (como por exemplo: redes sociais e plataforma de colaboração) outras aplicações.
- Recursos de NAT e Logs habilitados.
- Garantir que não haja restrição por número de usuários da solução disponibilizada.

4.6.9.7 Suportar o protocolo de gerenciamento SNMP compatível, no mínimo, nas versões 2 e 3.

4.6.9.8 Deve permitir monitorar, via protocolo SNMP, falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede.

4.6.9.9 Enviar log para sistemas de monitoração externos, de forma simultânea ou programada.

4.6.9.10 O gerenciamento da solução deve suportar acesso via SSH, software cliente, WEB (HTTPS) e API aberta.

4.6.9.11 Possibilitar a criação de administradores que tenham acesso a todas as instâncias de virtualização.

4.6.9.12 Possuir a capacidade de virtualização, possibilitando a delegação de controle, para que administradores, definidos pelo CONTRATANTE, possam gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado.

4.6.9.13 A solução deverá englobar dois tipos de equipamentos: Data Center 1 e Data Center 2, operando cada um deles com dois equipamentos idênticos.

4.6.9.14 A seguinte tabela apresenta as especificações mínimas para cada equipamento componente da Solução de Segurança do Data Center Tipo 1:

Item	Especificação	Valores
1	Throughput de Firewall (Gbps)	80
2	Conexões simultâneas (milhões)	50
3	Novas conexões por segundo (mil)	380
4	Throughput de IPSec (Gbps)	45
5	Proteção combinada contra ameaças (Gbps)	14
6	Quantidade mínima de interfaces (1 Gbps)	2
7	Quantidade mínima de interfaces (10 Gbps)	48
9	Quantidade de Instâncias Virtuais	200

4.6.9.15 A seguinte tabela apresenta as especificações mínimas para cada equipamento, componentes da Solução de Segurança do Data Center Tipo 2:

Item	Especificação	Valores
1	Throughput de Firewall (Gbps)	70
2	Conexões simultâneas (milhões)	10
3	Novas conexões por segundo (mil)	280
4	Throughput de IPSec (Gbps)	40
5	Proteção combinada contra ameaças (Gbps)	5
6	Quantidade mínima de interfaces (1 Gbps)	16
7	Quantidade mínima de interfaces (10 Gbps)	8
9	Quantidade de Instâncias Virtuais	200

4.6.9.16 Na proteção combinada contra ameaças, a solução instalada deverá ter, de maneira ativa, as funcionalidades de firewall, IPS, Antivírus e controle de aplicações especificadas neste termo de referência, com todo o tráfego suportado pelo equipamento (considerando as métricas de mundo real) e processos automáticos configurados.

4.6.9.17 Requisitos Mínimos para Solução de Rede e Firewall:

a) Ter tecnologia de firewall do tipo *Statefull.*

b) Ser otimizada para análise de conteúdo de aplicações em camada 07 (sete).

c) Permitir, para o gerenciamento da solução, interface de administração via web no próprio dispositivo integrada com bases de usuários LDAP, LDAP/AD.

d) Realizar VLAN com *tags* padrão 802.1q.

e) Possuir suporte a agregação de links 802.3ad e LACP.

f) Realizar política baseada em roteamento (*policy based routing*) ou política baseada em encaminhamento (*policy based forwarding*).

g) Realizar roteamento *multicast* (PIM-SM e PIM-DM).

h) Realizar DHCP Relay e DHCP Server.

i) Possuir suporte a sub-interfaces ethernet lógicas.

j) Funcionar com tradução de endereços de rede (NAT) dinâmico (*Many-to-1* e *Many-to-Many*).

k) Funcionar com NAT estático (1-to-1, *Many-to-Many*, bidirecional 1-to-1).

l) Funcionar com tradução de porta (PAT).

m) Funcionar com NAT de Origem e NAT de Destino simultaneamente.

n) Suportar o *Network PrefixTranslation* (NPTv6) ou NAT66, prevenindo problemas roteamento assimétrico.

o) Suportar NAT64 e NAT46.

p) Implementar o protocolo ICMP.

q) Implementar balanceamento de link por *hash* do IP de origem, como também por *hash* do IP de origem e destino.

r) Implementar balanceamento de link por peso, sendo possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, dois links.

s) Possuir proteção contra falsificação de endereços (*anti-spoofing*).

t) Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).

u) Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3).

v) Suportar OSPF *graceful restart*.

w) Suportar Modo *Sniffer*, para inspeção via porta espelhada do tráfego de dados da rede.

x) Ter a capacidade de operar de forma simultânea em uma única instância de *firewall*, mediante o uso de suas interfaces físicas nos seguintes modos: modo *sniffer* (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3).

y) Suportar Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação.

z) Suportar Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como *default gateway* das redes protegidas.

aa) Suportar Modo misto de trabalho *Sniffer*, L2 e L3 em diferentes interfaces físicas.

ab) Suportar configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: em modo transparente.

ac) Possuir suporte à criação de sistemas virtuais no mesmo equipamento (*appliance*).

ad) Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente.

ae) Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (*Inbound*) e Saída (*Outbound*), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolação das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos).

af) Operar em caráter permanente para as funcionalidades de controle de aplicações, VPN IPSec e SSL, QoS, de-criptografia SSL ou SSH, e protocolos de roteamento dinâmico.

ag) Realizar controles por zona de segurança.

ah) Realizar controles de políticas por porta e protocolo.

ai) Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

aj) Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança.

ak) Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS).

al) Criar políticas por geolocalização, permitindo que o tráfego de determinado Pais/Países seja(m) bloqueados.

am) Realizar a visualização dos países de origem e destino nos logs dos acessos.

an) Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.

ao) Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (*Inbound*) e Saída (*Outbound*).

ap) Realizar offload de certificado em inspeção de conexões SSL de entrada (*Inbound*).

aq) De-criptografar tráfego *Inbound* e *Outbound* em conexões negociadas com TLS 1.2.

ar) Realizar controle de inspeção e de-criptografia de SSH ou SSL por política.

as) Implementar objetos e regras IPV6.

at) Implementar objetos e regras *multicast*.

au) Realizar no mínimo três tipos de negação de tráfego nas políticas de firewall: *Drop* sem notificação do bloqueio ao usuário, *Drop* com notificação do bloqueio ao usuário, *Drop* com opção de envio de ICMP *Unreachable* para máquina de origem do tráfego, TCP-Reset para o cliente, TCP-Reset para o server ou para os dois lados da conexão.

av) Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

4.6.9.18 Requisitos mínimos para Solução de Filtro de Conteúdo:

a) Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL.

b) Possuir a funcionalidade de cota de tempo de utilização ou definir horários específicos para acesso por categoria.

c) Possibilitar a criação de categorias personalizadas.

d) Possibilitar a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

e) Possibilitar a categorização e reclassificação de sites web, tanto por URL quanto por endereço IP.

f) Possibilitar a criação de listas de URL específicas para serem bloqueadas ou liberadas.

g) Possibilitar, nas listas de URL personalizadas, a inserção de novas listas por expressão regular, permitindo adicionar domínios, subdomínios ou caminhos completos de sites.

h) Possibilitar o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual.

i) Possibilitar a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP, endereço IP e sub-rede.

j) Possibilitar a criação de regras para acesso/bloqueio por endereço IP de origem e sub-rede de origem.

k) Ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP.

l) Possibilitar *Proxy* Transparente.

m) Implementar roteamento WCCP e ICAP, ou outra solução para realizar roteamento de manipulação de tráfego WEB (*proxy* transparente).

n) Prover o funcionamento mínimo do mecanismo (*engine*) de filtragem web mesmo que a comunicação com o site do fabricante esteja fora de operação.

o) Possibilitar filtragem e categorização das URLs, mesmo sem conectividade com a Internet.

p) Possuir integração com serviços de diretório LDAP e Microsoft *Active Directory* para autenticação de usuários.

q) Possibilitar a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft *Active Directory*.

r) Possibilitar a criação de quotas de utilização ou limite de banda por usuários e grupos de usuários por Aplicação (facebook, youtube, etc.).

s) Ter a capacidade de exibir mensagens de bloqueio customizável pelos administradores para resposta aos usuários, na tentativa de acesso a recursos proibidos ou restringidos pela política de segurança do órgão.

t) Possibilitar o bloqueio de páginas web por meio da construção de filtros específicos com mecanismo de busca textual.

u) Possibilitar o bloqueio de URLs inválidas cujo campo CN ou DN do certificado SSL não contenha um domínio válido.

v) Possibilitar o bloqueio de páginas web por classificação, como páginas que facilitam a busca de áudio, vídeo, imagem, URLs originadas de spam e sites de *proxys* anônimos.

w) Possibilitar e forçar pesquisas seguras em sistemas de buscas, contemplando no mínimo, Google, Bing e Yahoo.

4.6.9.19 Requisitos mínimos para Solução de Controle de Aplicações:

a) Possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

b) Realizar a liberação e bloqueio somente de aplicações sem a necessidade de liberação portas e protocolos.

c) Reconhecer no mínimo 2.000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a *peer-to-peer*, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, *proxy*, mensageiros instantâneos, compartilhamento de arquivos, e-mail, entre outros.

d) Inspecionar o *payload* de pacote de dados com o objetivo de detectar, através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo.

e) Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent “encriptado” e aplicações VOIP que utilizam criptografia proprietária.

f) Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da *deep web* (ex.: rede Tor).

g) De-criptografar, para tráfego criptografado SSL, pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.

h) Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos.

i) Atualizar a base de assinaturas de aplicações automaticamente.

j) Limitar a banda (*download*/*upload*) usada por aplicações (*traffic shaping*), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD.

k) Possuir a capacidade de identificar usuários de rede com integração ao LDAP, LDAP/Microsoft *Active Directory*, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários.

l) Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

m) Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos.

n) Manter a segurança da rede eficiente, realizando o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

o) Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE.

p) Criar assinaturas personalizadas com o uso de expressões regulares, contexto (sessões ou transações), usando posição no *payload* dos pacotes TCP e UDP ou usando decodificadores de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL.

q) Possibilitar a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

r) Possibilitar a configuração de alertas quando uma aplicação for bloqueada.

s) Possibilitar que o controle de portas seja aplicado para todas as aplicações.

t) Possibilitar a diferenciação de tráfegos *Peer-to-Peer* (Bittorrent, emule, neonet, etc) possuindo granularidade de controle/políticas para os mesmos.

u) Possibilitar a diferenciação de tráfegos de mensageiros instantâneos (AIM, Hangouts, Facebook Chat, etc), possuindo granularidade de controle/políticas para os mesmos.

v) Possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o “Hangouts chat” e bloquear a chamada de vídeo.

w) Possibilitar a diferenciação de aplicações *Proxies* (psiphon3, freegate, etc) possuindo granularidade de controle/políticas para os mesmos.

x) Permitir a criação de grupos estáticos e dinâmicos de aplicações, informadas pela CONTRATANTE, baseados em características das mesmas, tais como: Tecnologia utilizada (*Client-Server*, *BrowseBased*, *Network Protocol*, etc), Nível de risco, Categoria, uso de técnicas evasivas, utilizadas por *malwares* (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.

4.6.9.20 A solução deverá atender, ainda, às seguintes condições:

a) Garantir o funcionamento com módulos de IPS, Antivírus e *Anti-Spyware* integrados no próprio *appliance* de Firewall.

b) Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e *Anti-Spyware*).

c) Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, *Anti-Spyware* quando implementado em alta disponibilidade ativo/ativo e ativo/passivo.

d) Implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, *Anti- spyware* e Antivirus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo.

e) Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração.

f) Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança.

g) Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do *firewall*, considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc..

h) Permitir o uso de exceções por IP de origem ou de destino nas regras e assinatura.

i) Suportar granularidade nas políticas de IPS, Antivírus e *Anti-Spyware*, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

j) Permitir o bloqueio de vulnerabilidades.

k) Permitir o bloqueio de programas exploradores de vulnerabilidades (*exploits*) conhecidos.

l) Possuir no mínimo os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo. Análise para detecção de anomalias de protocolo. Análise heurística. Desfragmentação de IP. Remontagem de pacotes de TCP. Bloqueio de pacotes malformados.

m) Ser imune e capaz de impedir ataques básicos como: *Synflood*, ICMP *flood*, UDP *flood*, etc..

n) Detectar e bloquear a origem de programas de varredura de portas (*portscans*).

o) Bloquear ataques efetuados por *worms* conhecidos, permitindo ao administrador acrescentar novos padrões.

p) Possuir assinaturas para bloqueio de ataques de *buffer overflow*.

q) Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e *anti-spyware*, permitindo a criação de exceções com granularidade nas configurações.

r) Permitir o bloqueio de vírus e *spywares* em, pelo menos, dois dos seguintes protocolos: FTP, SMB, SMTP e POP3, e obrigatoriamente em HTTP.

s) Identificar, alertar e bloquear comunicação com *botnets*.

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

u) Suportar a captura de pacotes (PCAP), por assinatura de IPS e controle de aplicação ou *anti-malware*.

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

w) Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de *botnets* conhecidas.

x) Identificar nos eventos o país de onde partiu a ameaça.

y) Incluir proteção contra vírus em conteúdo HTML e *javascript*, *software* espião (*spyware*) e *worms*.

z) Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.

4.6.9.21 Requisitos mínimos para Solução do Serviço de Autenticação Centralizada:

a) Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, *E-directory* e base de dados local.

b) Possuir integração com LDAP, LDAP/Microsoft *Active Directory* para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando *single sign-on*. essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso, não limitado a utilização de sistemas virtuais, segmentos de rede, etc..

c) Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

d) Permitir o controle de acesso, para saída de Internet, sendo habilitado o *Captive Portal*, de forma integrada com a solução proposta.

e) Permitir o recurso de bloqueio e continuação, possibilitando que o usuário acesse um site potencialmente bloqueado, informando ao mesmo, na tela de bloqueio, e possibilitando, a utilização de um botão “Continuar”, que permita ao usuário acessar o site.

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

g) Implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP, LDAP/AD.

h) Permitir integração com *tokens* ou agentes para autenticação dos usuários.

i) Prover, no mínimo, um *token* ou agente nativamente, possibilitando autenticação de duplo fator ou baseada em Kerberos.

4.6.9.22 Requisitos mínimos para Solução de Qualidade de Serviço (QoS) e Modelagem de Tráfego:

a) Realizar *Traffic Shaping* para a solução de segurança dos Acessos Dedicados.

b) Criar políticas de QoS e *Traffic Shaping* por endereço de origem e destino.

c) Criar políticas de QoS e *Traffic Shaping* por endereço de destino.

d) Realizar a criação de políticas de QoS e *Traffic Shaping* por porta.

e) Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade.

f) Disponibilizar estatísticas em tempo real para classes de QoS ou *Traffic Shaping*, em modo web ou CLI (*Command Line Interface*).

g) Realizar QoS (*traffic Shapping*) em interface agregadas ou redundantes.

4.6.9.23 Requisitos mínimos para a solução de Filtro de Dados:

a) Identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos.

b) Identificar arquivos criptografados e aplicar políticas sobre esses tipos de arquivos.

c) Identificar e prevenir a transferência de informações definidas como sensíveis pela CONTRATANTE (por exemplo, número de cartão de crédito, etc.) possibilitando a criação de novos tipos de dados via expressão regular.

4.6.9.24 Requisitos mínimos para a solução de Redes Virtuais Privadas (VPNs):

a) Criar VPN dos tipos *Site-to-Site* e *Client-To-Site*.

b) Criar IPSec VPN e SSL VPN.

c) Suportar nativamente a criação de VPN IPSec utilizando 3DES.

d) Suportar nativamente a criação de VPN IPSec utilizando AES (*Advanced Encryption Standard*) 128, 192 ou 256 bits.

e) Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1.

f) Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup Group 2, Group 5 e Group 14.

g) Suportar nativamente a criação de VPN IPSec utilizando o algoritmo *Internet Key Exchange* (IKEv1 e v2).

h) Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI.

i) Possuir interoperabilidade com, no mínimo, os seguintes fabricantes: Cisco, CheckPoint, Juniper, Palo Alto Networks, Fortinet, SonicWall.

j) Habilitar, desabilitar, reiniciar e atualizar IKE *gateways* e túneis de VPN IPSEc a partir da interface gráfica ou linhas de comando (CLI - *Command Line Interface*) da solução, facilitando o processo de resolução de problemas (*troubleshooting*).

k) Suportar, para VPN SSL, que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.

l) Atender com ou sem o uso de agente as funcionalidades de VPN SSL.

m) Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies.

n) Realizar atribuição de DNS nos clientes remotos de VPN.

o) Criar políticas de controle de aplicações, IPS, Antivírus, *Anti-spyware* e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

p) Permitir autenticação via LDAP, AD/LDAP, *Secure id*, certificado e base de usuários local.

q) Suportar leitura e verificação de CRL (*Certificate Revocation List*).

r) Aplicar políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

s) Ter a capacidade, para o agente de VPN a ser instalado nos equipamentos desktop e laptops, de ser distribuído de maneira automática via Microsoft *Active Directory* e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN.

t) Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação.

u) Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário.

v) Manter uma conexão segura com o portal durante a sessão.

w) Possuir agente de VPN SSL ou IPSEC *client-to-site* compatível com pelo menos: Linux, Windows 7 (32 e 64 bits), Windows 8/8.1 (32 e 64 bits), Windows 10 ou superior (32 e 64 bits) e Mac OS X (v10.10 ou superior).

4.7 Serviço de Wi-Fi Gerenciado

4.7.1 O Serviço de Wi-Fi Gerenciado deverá ser dimensionado e disponibilizado na infraestrutura do CONTRATANTE funcionando de forma gerenciada e integrada às soluções de segurança da operação do Link Remoto.

4.7.2 O Serviço de Wi-Fi Gerenciado deverá ser provido por uma solução integrada de software e hardware, com controladoras de rede sem fio, pontos de acesso internos (indoor) compatíveis com as Soluções de Segurança.

4.7.3 Deve ser integrado por uma controladora wireless, centralizada no Data Center, em nuvem gerenciada ou localmente na solução do Link Remoto. Em todos os casos, a gestão deve ser centralizada, realizando a gerência de todas as controladoras utilizadas.

4.7.4 Deverá prover toda a infraestrutura envolvida e realizar atividades de instalação e configurações de todos os itens necessários (pontos de acesso, antenas, injetores POE) para o pleno funcionamento do serviço, buscando sempre atender aos mais atuais padrões de qualidade para instalações físicas e lógicas para este tipo de serviço.

4.7.5 O Serviço de Wi-Fi Gerenciado deverá gerenciar todos os pontos de acesso sem fio através de controladoras ou outras tecnologias equivalentes, atendendo aos seguintes requisitos mínimos:

a) Possuir throughput mínimo de 1700 Mbps no rádio de 5 Ghz.

b) Suportar no mínimo as tecnologias 802.11 a/b/g/n/ac.

c) Possuir no mínimo 2 (dois) rádios.

d) Possuir no mínimo 4 (quatro) antenas internas.

e) Suportar as frequências de operação em 2.4 e 5 GHz.

f) Ser no mínimo MIMO (Multiple-Input and Multiple-Output) 4x4.

g) Ter potência de transmissão mínima de 18 dBm em, pelo menos, um MCS (Modulation and Coding Scheme).

h) Ter o ganho mínimo das antenas internas sendo de 5 dBi no rádio de 5Ghz.

i) Suportar, no mínimo, 50 (cinquenta) clientes simultaneamente.

j) Possuir homologação válida pela ANATEL.

k) Suportar, no mínimo, até 4 SSIDs simultâneos por rádio dos pontos de acesso sem fio.

l) Ser compatível e implementar o padrão IEEE 802.3af.

m) Garantir no mínimo o nível wave 2.

n) Os equipamentos de radiofrequência deverão ser homologados pela ANATEL (Agência Nacional de Telecomunicações).

5 Modelos a Serem Utilizados na Contratação (ART. 18, § 3º, V)

5.1 Anexo II – Modelo de Proposta Comercial.

5.2 Anexo III – Modelo de Termo de Nomeação de Preposto.

5.3 Anexo IV – Modelo de Termo de Confidencialidade.

5.4 Anexo V – Modelo de Termo de Autorização para Subcontratar

ANEXO II – MODELO DE PROPOSTA COMERCIAL

Nome Fantasia:		
Razão Social:		
CNPJ:	Inscrição Estadual:	Telefone:
Endereço:		CEP:
Cidade/UF:	E-mail:	

Lista de Preços

Item	Descrição	Unidade	Preço Unitário
1	LR Básico 10 Mbps	LR/Mês[12]	
2	LR Básico 20 Mbps	LR/Mês	
3	LR Básico 50 Mbps	LR/Mês	
4	LR Básico 100 Mbps	LR/Mês	
5	LR Básico 200 Mbps	LR/Mês	
6	LR Avançado 2 Mbps + SLR[13] + SDC[14]	LR/Mês	
7	LR Avançado 5 Mbps + SLR + SDC	LR/Mês	
8	LR Avançado 10 Mbps + SLR + SDC	LR/Mês	
9	LR Avançado 20 Mbps + SLR + SDC	LR/Mês	
10	LR Avançado 50 Mbps + SLR + SDC	LR/Mês	
11	LR Avançado 100 Mbps + SLR + SDC	LR/Mês	
12	LR Avançado 200 Mbps + SLR + SDC	LR/Mês	
13	LR Plus 5 Mbps + SLR + SDC	LR/Mês	
14	LR Plus 10 Mbps + SLR + SDC	LR/Mês	
15	LR Plus 20 Mbps + SLR + SDC	LR/Mês	
16	LR Plus 50 Mbps + SLR + SDC	LR/Mês	
17	LR Plus 100 Mbps + SLR + SDC	LR/Mês	
18	LR Plus 200 Mbps + SLR + SDC	LR/Mês	
19	Serviços de Wi-Fi Gerenciado	UJ/Mês[15]	

Cálculo do Valor Global

Item	Descrição	Valor Unitário[16]	Quantidade 1º ano	Total 1º Ano[17]	Quantidade 2º ano	Total 2º Ano[18]	Total para 2 Anos[19]
1	LR Básico 10 Mbps		10		15		
2	LR Básico 20 Mbps		8		22		
3	LR Básico 50 Mbps		15		20		
4	LR Básico 100 Mbps		1		2		
5	LR Básico 200 Mbps		0		1		
6	LR Avançado 2 Mbps + SLR + SDC		60		30		
7	LR Avançado 5 Mbps + SLR + SDC		150		105		
8	LR Avançado 10 Mbps + SLR + SDC		55		120		
9	LR Avançado 20 Mbps + SLR + SDC		26		36		
10	LR Avançado 50 Mbps + SLR + SDC		4		7		
11	LR Avançado 100 Mbps + SLR + SDC		0		2		
12	LR Avançado 200 Mbps + SLR + SDC		0		1		
13	LR Plus 5 Mbps + SLR + SDC		5		8		
14	LR Plus 10 Mbps + SLR + SDC		5		8		
15	LR Plus 20 Mbps + SLR + SDC		5		10		
16	LR Plus 50 Mbps + SLR + SDC		1		2		
17	LR Plus 100 Mbps + SLR + SDC		0		1		
18	LR Plus 200 Mbps + SLR + SDC		0		1		
19	Serviços de Wi-Fi Gerenciado		20		30		
						Valor Global do Contrato[20] ⇨	

12 LR/Mês: Custo mensal de um link remoto.
13 SLR: Segurança do Link Remoto, conforme definido no item 4.6.8.
14 SDC: Segurança de Acesso ao Data Center, conforme definido no item 4.6.9.
15 UJ/Mês: Custo mensal dos serviços de Wi/Fi Gerenciado para uma Unidade Judiciária.
16 Valor mensal unitário dos serviços especificados.
17 Valor mensal unitário x Quantidade 1º ano x 12 meses.
18 Valor mensal unitário x Quantidade 2º ano x 12 meses.
19 Total 1º Ano + Total 2º Ano.
20 Soma de todos os valores da coluna Total para 2 Anos.

Declaramos:

- Que os serviços ofertados atendem a todas as exigências técnicas e legais definidas no Termo de Referência.
- Que os preços ofertados são fixos e irreajustáveis pelo período mínimo de 12 (doze) meses e incluem todas as despesas, diretas e indiretas, não sendo admissível a cobrança de quaisquer outras não precificadas na proposta.
- Que possuímos o protocolo MPLS implementado em nosso backbone.
- Que possuímos ____ Centros de Operações de Segurança (mínimo, dois, podendo ser localizados em qualquer cidade do Brasil)

Prazo de validade da proposta: 90 dias

_____, _____de _____ de 2019.

_____
ASSINATURA DO REPRESENTANTE LEGAL DA EMPRESA

ANEXO III – MODELO DE TERMO DE NOMEAÇÃO DE PREPOSTO

ANEXO ___ AO CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI CELEBRAM _____ E A EMPRESA _____.

(Pregão Eletrônico nº _____ Processo n° _____)

Termo de Nomeação de Preposto

Contrato n°.....

Objeto: .....

Por meio deste instrumento, a (nome da empresa) nomeia e constitui seu(sua) preposto(a), o(a) Sr.(a) (nome do preposto), carteira de identidade n° ....., expedida pela ....., inscrito(a) no Cadastro de Pessoas Físicas (CPF) sob o n° ....., com endereço ....., para exercer a representação legal junto ao Tribunal de Justiça do Estado da Bahia, com poderes para receber ofícios, representar a contratada em reuniões e assinar respectivas atas obrigando a contratada nos termos dela constantes, receber solicitações e orientações para o cumprimento do contrato, notificações de descumprimento, de aplicação de penalidades, de rescisão, de convocação ou tomada de providências para ajustes e aditivos contratuais, e todas as demais que imponham, ou não, a abertura de processo administrativo ou prazo para a contratada responder ou tomar providências, e para representá-la em todos os demais atos que se relacionem à finalidade específica desta nomeação, que é a condução do contrato acima identificado.

Salvador, ... de ..... de .....

(nome da empresa)

{nome e assinatura do representante legal confirmar poderes no estatuto social ou procuração) (qualidade do representante legal sócio-gerente, diretor, procurador)

(nome e assinatura do preposto)

ANEXO IV – MODELO DE TERMO DE CONFIDENCIALIDADE

ANEXO III AO CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI CELEBRAM TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA E A EMPRESA _____.
(Pregão Eletrônico nº __/__ Processo n° _____)

TERMO DE CONFIDENCIALIDADE SOBRE A SEGURANÇA DA INFORMAÇÃO

O ESTADO DA BAHIA, pessoa jurídica de direito público, inscrito no CNPJ/MF sob o nº 13.937.032/0001-60, por intermédio do TRIBUNAL DE JUSTIÇA DA BAHIA, órgão do Poder Judiciário, inscrito no CNPJ/MF sob nº 13100722/0001-60, com sede e foro nesta cidade do Salvador, Estado da Bahia, na Quinta Avenida, nº 560, Centro Administrativo da Bahia CAB, representado por ..... adiante denominada simplesmente CONTRATANTE, e, do outro lado, ..., inscrita no CNPJ sob nº ....., doravante designada simplesmente CONTRATADA, representada por …......, inscrito no CPF/MF sob nº …......, resolvem, tendo em vista o constante do PA nº ….... com arrimo nas normas pertinentes da Lei Estadual nº 9.433/05 e, no que couber, na Lei Federal nº 8.666/93 e demais dispositivos legais aplicáveis, e tendo em vista o constante no PA nº TJ-ADM-2017/17798, e sempre que em conjunto referidas como PARTES para efeitos deste TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO, doravante denominado simplesmente TERMO, e,

CONSIDERANDO que, em razão do atendimento à exigência do Contrato Nº ..., celebrado pelas PARTES, doravante denominado CONTRATO, cujo objeto é a ....., 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 ..... NOME DA EMPRESA ..... tiver acesso em virtude da execução contratual;

CONSIDERANDO a necessidade de manter sigilo e confidencialidade, sob pena de responsabilidade civil, penal e administrativa, conforme tipificado no art.325 do Decreto Lei 2.848/1940 (Código Penal Brasileiro), sobre todo e qualquer assunto de interesse do CONTRATANTE de que a .....NOME DA EMPRESA..... tomar conhecimento em razão da execução do CONTRATO, respeitando todos os critérios estabelecidos aplicáveis às INFORMAÇÕES;

O CONTRATANTE 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 às INFORMAÇÕES do CONTRATANTE, principalmente aquelas classificadas como CONFIDENCIAIS, em razão da execução do CONTRATO celebrado entre as PARTES.

CLÁUSULA SEGUNDA DAS INFORMAÇÕES CONFIDENCIAIS

a) As estipulações e obrigações constantes do presente instrumento serão aplicadas a todas e quaisquer INFORMAÇÕES reveladas pelo CONTRATANTE;

b) A .....NOME DA EMPRESA..... se obriga a manter o mais absoluto sigilo e confidencialidade com relação a todas e quaisquer INFORMAÇÕES que venham a ser fornecidas pelo CONTRATANTE, a partir da data de assinatura deste TERMO, devendo ser tratadas como INFORMAÇÕES CONFIDENCIAIS, salvo aquelas prévia e formalmente classificadas com tratamento diferenciado pelo CONTRATANTE;

c) A .....NOME DA EMPRESA..... 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 do CONTRATANTE;

d) O CONTRATANTE, 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 .....NOME DA EMPRESA.....
e) O CONTRATANTE pode, sem aviso prévio, restringir ou bloquear o acesso a Web Sites, serviços da Internet ou download de arquivos e examinar o conteúdo das mensagens de correio eletrônico, arquivos em computadores, cache de navegadores Web, bookmarks, histórico de sites visitados, configurações dos softwares e outras informações armazenadas ou transmitidas pelos seus computadores;
f) A .....NOME DA EMPRESA..... obriga-se a preservar o sigilo das senhas das contas dos usuários, não cedê-las nem facilitar a sua descoberta, sob qualquer pretexto, bem como não utilizar contas e senhas pertencentes a outros servidores.

CLÁUSULA TERCEIRA DAS LIMITAÇÕES DA CONFIDENCIALIDADE

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:
a) 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;
b) Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
c) Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, 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

a) A .....NOME DA EMPRESA..... se compromete a utilizar as INFORMAÇÕES reveladas exclusivamente para os propósitos da execução do CONTRATO;
b) A .....NOME DA EMPRESA..... se compromete a não efetuar qualquer cópia das INFORMAÇÕES sem o consentimento prévio e expresso do CONTRATANTE;
b1) O consentimento mencionado na alínea “b”, entretanto, será dispensado para cópias, reproduções ou duplicações para uso interno das PARTES;
c) A .....NOME DA EMPRESA..... se compromete a cientificar seus diretores, empregados e/ou prepostos da existência deste TERMO e da natureza confidencial das INFORMAÇÕES do CONTRATANTE;
d) A .....NOME DA EMPRESA..... deve tomar todas as medidas necessárias à proteção das INFORMAÇÕES do CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo CONTRATANTE;
e) Cada PARTE permanecerá como única proprietária de todas e quaisquer INFORMAÇÕES eventualmente reveladas à outra parte em função da execução do CONTRATO;
f) 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;
g) Os produtos gerados na execução do CONTRATO, bem como as INFORMAÇÕES repassadas à .....NOME DA EMPRESA....., são única e exclusiva propriedade intelectual do CONTRATANTE;
h) A .....NOME DA EMPRESA..... firmará acordos por escrito com cada um de 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, entregando uma via ao CONTRATANTE;
i) A .....NOME DA EMPRESA..... 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;
j) A .....NOME DA EMPRESA..... se compromete a envidar todos os esforços para preservar a confidencialidade das informações, adotando práticas de trabalho seguras quanto

ao manuseio, armazenamento, transporte, impressão, transmissão e, quando for o caso, destruição de informações pertencentes ao CONTRATANTE;

k) A .....NOME DA EMPRESA..... se compromete a estar engajada na promoção de Segurança da Informação, incorporando as suas recomendações às atividades diárias do trabalho;

l) A .....NOME DA EMPRESA..... se compromete a notificar à Área de Segurança da Informação do CONTRATANTE em caso de divulgação ou suspeita de divulgação, acidental ou intencional, de informações pertencentes ao CONTRATANTE, bem como a descoberta de fragilidades de sistemas ou processos que possam propiciar a quebra de confidencialidade, disponibilidade ou integridade das informações.

CLÁUSULA QUINTA DO RETORNO DE INFORMAÇÕES

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.

CLÁUSULA SEXTA DA VIGÊNCIA

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, e persiste após o término da atividade, mudança de função ou de encerramento do vínculo empregatício com a empresa.

CLÁUSULA SÉTIMA DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade, 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 .....NOME DA EMPRESA....., estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e Criminal, as quais serão apuradas em regular processo administrativo ou judicial.

CLÁUSULA OITAVA DAS DISPOSIÇÕES GERAIS

a) Este TERMO constitui vínculo indissociável ao CONTRATO, que é parte independente e regulatória deste instrumento;

b) 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 em ações feitas direta ou indiretamente;

c) 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 do CONTRATANTE;

d) 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;

e) 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

As partes elegem o foro da Comarca de Salvador-BA, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, as partes firmam o presente instrumento em 2 (duas) vias de igual teor e um só efeito, juntamente com as testemunhas, abaixo identificadas.

Salvador, ___ de _____ de 2019.

_____

TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA
Des. Gesivaldo Nascimento Britto
Presidente do Tribunal de Justiça do Estado da Bahia

_____

(nome da empresa)
(nome e assinatura do representante legal confirmar poderes no estatuto social ou procuração)
(qualidade do representante legal sócio-gerente, diretor, procurador)
(nome e assinatura do preposto)

Testemunhas:

Nome: _____ CPF: _____

Nome: _____ CPF: _____

ANEXO V – MODELO DE TERMO DE AUTORIZAÇÃO PARA SUBCONTRATAR

TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA	**PODER JUDICIÁRIO** **TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA** TERMO DE AUTORIZAÇÃO DE SUBCONTRATAÇÃO

Nome da Contratada	CPF/CNPJ
Objeto	
Autorizamos que a(s) parcela(s) do(s) serviço(s) abaixo indicadas seja(m) subcontratada(s) junto à(s) empresa(s) indicada(s) pela contratada e abaixo qualificada(s), mantendo a contratada, contudo, a responsabilidade integral pelas obrigações do contrato e adicionalmente a obrigação de angariar e apresentar ao Tribunal documentos da subcontratada equivalentes aos exigidos da contratada no contrato, como condição para o pagamento.	
Parcela subcontratada	Nome e CNPJ da empresa subcontratada
Parcela subcontratada	Nome e CNPJ da empresa subcontratada
Nome do Fiscal ou Gerente do Contrato que esteja autorizando	N° do Cadastro
Data / /	Assinatura
Nome do Preposto da Contratada	
Data / /	Assinatura

1ª VIA – FORNECEDOR / 2° VIA – ÓRGÃO/ENTIDADE

ANEXO VI – CIRCUITOS COMPREENDIDOS NA DEMANDA INICIAL[21]

PODER JUDICIÁRIO

Localidade	Unidade	Endereço	CEP	Velocidade
Alagoinhas	SAJ	Avenida Dantas Bião, s/n, Shopping Laguna.	48030-030	10 Mbps
Alagoinhas	Fórum	Avenida Juracy Magalhães, Centro, Alagoinhas.	48040-970	20 Mbps
Amargosa	Fórum	Praça Tiradentes, nº 366, Centro.	45300-000	5 Mbps
Amélia Rodrigues	Fórum	Rua Raulino Bastos dos Santos, s/n.	44230-000	5 Mbps
Anagé	Fórum	Rua Fidélis Botelho, s/n, Centro.	45180-000	5 Mbps
Andaraí	Fórum	Rua Alto do Ibirapitanga, s/n.	46830-000	5 Mbps
Antas	Fórum	Rua João Nilo, n° 538.	48420-000	2 Mbps
Araci	Fórum	Rua Sete Setembro, n° 323, Centro.	48760-000	2 Mbps
Baianópolis	Fórum	Praça Municipal, s/n.	47830-000	2 Mbps
Barra	Fórum	Praça do Rosário, s/n.	47100-000	5 Mbps
Barra da Estiva	Fórum	Rua Santa Vieira de Castro, n° 106.	46650-000	2 Mbps
Barra do Choça	Fórum	Rua Dom Climério, n° 111.	45120-000	5 Mbps
Barra do Mendes	Fórum	Rua Antônio Evaristo dos Santos.	44990-000	5 Mbps
Barreiras	Juizado	Avenida Benedita Silveira, nº 201.	47800-000	10 Mbps
Barreiras	Fórum	Rua Coronel Magno, S/N, Centro.	47800-270	20 Mbps
Barreiras	SAJ	BR 020 Km 02 Shopping Center Rio das Ondas SL 04.	47807-970	5 Mbps
Belmonte	Fórum	Avenida Riomar, nº 159.	45800-000	5 Mbps
Belo Campo	Fórum	Rua Almiro Ferraz de Almeida, nº 193.	45160-000	5 Mbps
Boa Nova	Fórum	Praça da Bandeira, nº 08.	45250-000	2 Mbps
Bom Jesus da Lapa	Fórum	Rua das Escoteiras, s/n.	47600-000	10 Mbps
Brumado	Fórum	Rua Rio de Contas, s/n.	46100-000	10 Mbps
Brumado	Juizado	Rua Mourão Guimarães, 251, 1º andar.	46100-000	10 Mbps
Buerarema	Fórum	Avenida Góes Calmon, 513.	45615-000	5 Mbps
Cachoeira	Fórum	Pça. Juíza Ivone Bessa Ramos, s/n.	44300-000	10 Mbps
Caculé	Fórum	Rua Miguel Fernandes.	46300-000	5 Mbps
Caetité	Fórum	Rua Pernambuco, s/n.	46400-000	10 Mbps
Camacã	Fórum	Avenida Pioneiros, s/n.	45880-000	5 Mbps
Camacã	CEJUSC	Avenida Everaldo Figueiredo dos Anjos, 182.	45880-000	2 Mbps
Camaçari	Fórum	Rua Contorno do Centro Cultural, 216 Centro.	42800-610	20 Mbps
Camaçari	SAJ	Boulevard Shopping Camaçari, BA-535, s/n.	42800-170	5 Mbps
Camamu	Fórum	Praça Pirajá da Silva, 437.	45445-000	5 Mbps
Campo Formoso	Fórum	Praça 2 de Julho, s/n.	44790-000	5 Mbps
Canarana	Fórum	Rua Durval Cardoso Pimenta, s/n.	44890-000	2 Mbps
Canavieiras	Juizado	Praçada Bandeira, s/n.	45860-000	5 Mbps
Canavieiras	Fórum	Praça São Boaventura, Nº 40.	45860-000	5 Mbps
Candeias	Fórum	Bairro Ouro Negro, s/n.	43800-000	10 Mbps
Cândido Sales	Fórum	Rua José Porto, 51.	45157-000	5 Mbps
Cansanção	Fórum	Avenida Tancredo Neves, 584.	48840-000	5 Mbps
Capela do Alto Alegre	Fórum	Avenida Lindolfo João Carneiro, s/n.	44645-000	2 Mbps
Capim Grosso	Fórum	Rua Esmerando Santiago, s/n.	44695-000	5 Mbps
Caravelas	Fórum	Praça Teófilo Otoni, s/n.	45900-000	5 Mbps
Carinhanha	Fórum	Praça Deputado Henrique Brito, 296.	46445-000	5 Mbps
Casa Nova	Fórum	Praça Três, s/n.	47300-000	5 Mbps
Castro Alves	Fórum	Praça Liberdade, s/n.	44500-000	2 Mbps
Catu	Fórum	Rua Ministro Ernesto Simões Filho, 315.	48110-000	10 Mbps
Central	Fórum	Praça Cantidio Pires Maciel, Nº 88.	44940-000	5 Mbps
Chorrochó	Fórum	Rua Coronel João Sá, s/n.	48660-000	2 Mbps
Cícero Dantas	Fórum	Praça Municipal, s/n.	48410-000	5 Mbps

21 Entende-se por instalação inicial a substituição dos circuitos atualmente em uso. Ao longo do contrato, esses circuitos poderão sofrer desativação, upgrade, downgrade ou mudança de endereço respondendo a solicitação do CONTRATANTE, bem como poderá ser solicitada a instalação de novos circuitos em unidades ainda não contempladas.

Localidade	Unidade	Endereço	CEP	Velocidade
Cícero Dantas	Juizado	Praça Municipal, s/n.	48410-000	5 Mbps
Cipó	Fórum	Avenida Sete de Setembro, s/n.	48450-000	2 Mbps
Coaraci	Fórum	Rua Clarêncio Gomes Baracho, 36.	45640-638	5 Mbps
Cocos	Fórum	Praça da Matriz, s/n.	47680-000	2 Mbps
Conceição do Almeida	Fórum	Rua Dr. José Joaquim de Almeida, s/n.	44540-000	2 Mbps
Conceição do Coité	Juizado	Rua Clarêncio Gomes Barracho, 36.	48730-000	5 Mbps
Conceição do Coité	Fórum	Praca Porcina Rosa de Araujo s/n.	48730-000	5 Mbps
Conceição do Jacuípe	Fórum	Rua Manoel Anacleto Ferreira da Silva s/n.	44245-000	5 Mbps
Conde	Fórum	Praça Valter de Carvalho Batista, s/n.	48300-000	5 Mbps
Condeúba	Fórum	Praça Santo Antônio, s/n.	46200-000	2 Mbps
Coração de Maria	Fórum	Avenida Amélio Teixeira Amorim, 14.	44250-000	5 Mbps
Coribe	Fórum	Rua Santa Cruz, 19.	47690-000	5 Mbps
Correntina	Fórum	Rua Otávio Mangabeira, s/n.	47650-000	2 Mbps
Cotegipe	Fórum	Praça Des. Oswaldo Nunes Sento Sé, s/n.	47900-000	5 Mbps
Cruz das Almas	Fórum	Clodoaldo Gomes da Costa, 89.	44380-000	10 Mbps
Curaçá	Fórum	Praça Monsenhor José Gilberto Luna, s/n.	48930-000	2 Mbps
Dias D'Ávila	Fórum	Praça dos Três Poderes.	42850-000	10 Mbps
Encruzilhada	Fórum	Rua Arlindo Marques, s/n.	45150-000	5 Mbps
Entre Rios	Fórum	Rua Antônio Barreto, 25.	48180-000	5 Mbps
Esplanada	Fórum	Praça Monsenhor Zacarias Luz 48.	48370-000	5 Mbps
Euclides da Cunha	Juizado	Rua Tiago Ferreira de Carvalho, 248.	48500-000	5 Mbps
Euclides da Cunha	Fórum	Avenida Artulino Ribeiro, s/n.	45820-000	10 Mbps
Eunápolis	Fórum	Avenida Artulino Ribeiro, s/n.	45820-000	10 Mbps
Eunápolis	SAJ	Rua 5 de Novembro, 50, Centro.	45820-000	10 Mbps
Feira de Santana	SAJ	Rua Cel. Álvaro Simões, s/n.	44026-970	10 Mbps
Feira de Santana	Juizado	Rua Aloísio Resende, 388 Queimadinha.	44050-054	10 Mbps
Feira de Santana	Fórum	Rua Coronel Álvaro Simões s/n.	44026-970	50 Mbps
Feira de Santana	Central de Flagrantes	Rua Landulfo Alves, Sobradinho (Delegacia).	44021-352	5 Mbps
Feira de Santana	Justiça pela Paz em Casa	Rua Israelândia, 78 Quadra 13 Muchila.	44005-056	5 Mbps
Formosa do Rio Preto	Fórum	Rua Perfílio Santana, 740, Centro.	47999-000	5 Mbps
Gandu	Fórum	Rua Gervásio Couto Moreira, 31.	45450-000	10 Mbps
Gandu	Juizado	Rua Gervásio Couto Moreira, 31.	45450-000	5 Mbps
Gentio do Ouro	Fórum	Rua João Figueiredo, 02.	47450-000	5 Mbps
Governador Mangabeira	Fórum	Rua Prof. Aguinaldo Viana Pereira, 91.	44350-000	5 Mbps
Guanambi	Fórum	Avenida Presidente Castelo Branco s/n Aeroporto Velho.	46430000	5 Mbps
Guanambi	Juizado	Praça José Ferreira, 94.	46430-000	5 Mbps
Guaratinga	Fórum	Avenida Alberto Costa Lima, s/n.	45840-000	2 Mbps
Iaçu	Fórum	Avenida Doutor Geraldo Mota, s/n.	46860-000	5 Mbps
Ibicaraí	Fórum	Rua Castro Alves, s/n.	45745-000	5 Mbps
Ibirapuã	Fórum	Rua Pedro Manso Cabral, 179.	45950-000	2 Mbps
Ibirataia	Fórum	Rua Ruy Barbosa, 34.	45580-000	5 Mbps
Ibititá	Fórum	Praça Martiniano Marques Dourado, s/n.	44960-000	5 Mbps
Ibotirama	Fórum	Rua Principal, s/n, Loteamento Jardim Sta. Rosa.	47520-000	5 Mbps
Igaporã	Fórum	Rua Silêncio Fernandes, s/n.	46490-000	5 Mbps
Iguaí	Fórum	Rua Castro Alves, s/n.	42280-000	2 Mbps
Ilhéus	Fórum	Avenida Osvaldo Cruz, s/n.	45660-000	20 Mbps
Ilhéus	SAJ	Rua Estaquio Basto 308 s/04.	45660-000	5 Mbps
Inhambupe	Fórum	Praça Jatahy Fonseca, s/n.	48490-000	5 Mbps
Ipiaú	Fórum	Rua Borges de Barros, 01.	45570-000	10 Mbps
Ipiaú	Juizado	Rua Silva Jardim, N° 225, Centro.	45570-000	5 Mbps
Ipirá	Fórum	Rua Dr. Elzirio Macêdo, 260.	44600-000	5 Mbps
Iraquara	Fórum	Praça Árvores, s/n.	46980-000	2 Mbps
Irará	Fórum	Praça Tancredo Neves s/n.	44255-000	5 Mbps
Irecê	Fórum	Avenida Sol Poente, s/n.	44900-000	5 Mbps

Localidade	Unidade	Endereço	CEP	Velocidade
Itabela	Fórum	Rua Castro Alves, s/n.	45833-000	5 Mbps
Itaberaba	Fórum	Rua Doutor Osmar Ribeiro dos Santos, s/n.	46880-000	10 Mbps
Itabuna	Fórum Cível	Rua Santa Cruz, s/n, bairro Nossa Senhora das Graças.	45600-000	50 Mbps
Itabuna	SAJ	Shopping Jequitibá, Rua Aziz Marrom Góes Calmon.	45600-000	10 Mbps
Itacaré	Fórum	Rua Joaquim Vieira, s/n.	45530-000	2 Mbps
Itagibá	Fórum	Rua Chile nº 70.	45585-000	5 Mbps
Itajuípe	Fórum	Rua Francolino Gonçalves dos Santos, 85.	45630-000	5 Mbps
Itamaraju	Fórum	Praça Castelo Branco, s/n.	45830-000	10 Mbps
Itamaraju	Juizado	Praça Castelo Branco, Nº 3.	45836-000	5 Mbps
Itambé	Fórum	Praça da Bandeira, s/n.	45140-000	5 Mbps
Itanhém	Fórum	Avenida Maria Moreira Lisboa, 08.	45970-000	2 Mbps
Itaparica	Fórum	Rua Direita da Gamboa s/n.	44470-000	5 Mbps
Itapebi	Fórum	Rua Jesuíno de Almeida Costa, 202.	45855-000	10 Mbps
Itapetinga	Fórum	Rua Coronel Belisário Ferraz,137.	45700-000	10 Mbps
Itapetinga	CEJUSC	Rua Itambé 80, Centro.	45700-000	5 Mbps
Itapicuru	Fórum	Praça da Bandeira, nº 92.	48475-000	2 Mbps
Itarantim	Fórum	Praça João Alves Feitosa, s/n.	45780-000	5 Mbps
Itiruçu	CEJUSC	Rua João Brandão, s/n.	45350-000	2 Mbps
Itiúba	Fórum	Praça 15 de Novembro, s/n.	48850-000	5 Mbps
Itororó	Fórum	Rua Duque de Caxias, s/n.	45710-000	5 Mbps
Ituaçu	Fórum	Rua José Carlos Brito s/n.	46640-970	2 Mbps
Ituberá	Fórum	Rua Duque de Caxias, nº 290.	45435-000	5 Mbps
Jacaraci	Fórum	Praça Municipal, nº 72.	46310-000	2 Mbps
Jacobina	Fórum	Rua Margem Rio do Ouro, s/n.	44700-000	20 Mbps
Jaguaquara	Fórum	Avenida Ilmar Galvão, s/n.	45345-000	5 Mbps
Jaguarari	Fórum	R. Marcolino de Barros, s/n.	48960-000	2 Mbps
Jequié	Fórum	Praça Duque de Caxias, s/n.	45200-000	20 Mbps
Jequié	SAJ	Avenida Governador Otávio Mangabeira s/n, Mandacaru.	45210-000	5 Mbps
Jeremoabo	Fórum	Rua Doutor José Gonçalves de Sá, 206 Centro.	48540-000	5 Mbps
Jitaúna	Fórum	Avenida Maria Eleonora Cajaíba, nº 110.	45225-000	2 Mbps
João Dourado	Fórum	Avenida Eneas Silva Dourado, s/n.	44920-970	5 Mbps
Juazeiro	SAJ	Juá Garden Shopping: Rod. Lomanto Júnior, Km 06, s/n.	48908-000	10 Mbps
Juazeiro	Fórum	Travessa Venezia s/n Alagadiço.	48904-350	20 Mbps
Laje	Fórum	Praça Luiz Eduardo Magalhães, s/n.	45490-000	2 Mbps
Lapão	Fórum	Rua Filadelfo Cardoso Nº 777, Centro.	44905-000	5 Mbps
Lauro de Freitas	Fazenda Pública	Avenida Santos Dumont, n° 3109, Centro.	42700-000	10 Mbps
Lauro de Freitas	Fórum Criminal	Rua da Saúde, nº 90.	42700-000	10 Mbps
Lauro de Freitas	SAJ	Avenida Santos Dumont, Km 3,5, Shopping Passeio Norte, G1.	42700-000	10 Mbps
Lauro de Freitas	Fórum Cível	Rua Romoaldo de Brito, s/n, Centro.	42700-000	20 Mbps
Lençóis	Fórum	Praça João Lima, s/n.	46960-000	2 Mbps
Livramento de Nossa Senhora	Fórum	Avenida Dr. Nelson Leal, 568.	46140-000	5 Mbps
Luís Eduardo Magalhães	Fórum	Avenida Octogonal, Quadra GNV I, Loteamento Imperial.	47580-000	10 Mbps
Macarani	Fórum	Rua José de Souza Nogueira, nº 123.	45760-000	5 Mbps
Macaúbas	Fórum	Rua Dr. Manoel Vitorino, nº 356.	46500-000	5 Mbps
Mairi	Fórum	Rua Claudionora Brasil, s/n.	44630-000	5 Mbps
Maracás	Fórum	Praça Ruy Barbosa, nº 671.	45360-000	5 Mbps
Maragogipe	Fórum	Praça Ernezindo Mendes, nº 8.	44420-000	5 Mbps
Mata de São João	Fórum	Rua Eurico de Freitas, s/n.	48280-000	10 Mbps
Mata de São João	CEJUSC	Rua J. J. Seabra, nº 247, Centro.	48280-000	5 Mbps
Medeiros Neto	Fórum	Rua Plínio Mariani Guerreiro, s/n.	45960-000	2 Mbps
Miguel Calmon	Fórum	Rua Luiz Gonzaga Rios, nº 10.	44720-000	2 Mbps
Monte Santo	Fórum	Rua Dr. Manoel Novaes, nº 400.	48800-000	2 Mbps
Morro do Chapéu	Fórum	Rua Mário Chiarini, s/n.	44850-000	5 Mbps
Mucuri	Fórum	Pça Custódia Costa Oliveira, nº 194.	45930-000	5 Mbps

Localidade	Unidade	Endereço	CEP	Velocidade
Mundo Novo	Fórum	Praça Jairo Moreira de Almeida, s/n.	44800-000	5 Mbps
Muritiba	Fórum	Rua Dr. Pedreira Franco, nº 105.	44340-000	5 Mbps
Mutuípe	Fórum	Rua Santo Antônio, s/n.	45480-000	5 Mbps
Nazaré	Fórum	Rua Dr. Eurico Matta, 81.	44400-000	5 Mbps
Nova Soure	Fórum	Rua 1º de Junho, nº 423.	48460-000	2 Mbps
Nova Viçosa	Fórum	Avenida Oceânica, nº 84.	45920-000	5 Mbps
Olindina	Fórum	Praça 14 de Agosto, s/n.	48470-000	5 Mbps
Oliveira dos Brejinhos	Fórum	Praça Marechal Deodoro, s/n.	47530-000	5 Mbps
Palmas de Monte Alto	Fórum	Praça Tiradentes, n° 274.	46460-000	2 Mbps
Paramirim	Fórum	Rua Irmã Dulce, nº 31.	46190-000	5 Mbps
Paripiranga	Fórum	Praça Pedro Rabelo de Matos, s/n.	48430-000	5 Mbps
Paulo Afonso	Fórum	Rua Carlos Berenhausen Júnior, s/n.	48600-000	20 Mbps
Piatã	Fórum	Rua Coronel José Lisboa Xavier, nº 178.	46765-970	2 Mbps
Pilão Arcado	Fórum	Rua Pedro Pereira, s/n.	47240-000	5 Mbps
Pindobaçu	Fórum	R. Antônio Lareiro, Bairro Novo, s/n.	44770-000	2 Mbps
Piritiba	Fórum	Rua Regis Pacheco, s/n.	44830-000	5 Mbps
Planalto	Fórum	Avenida John Kennedy, nº 1.	45190-000	2 Mbps
Poções	Fórum	Praça da Bandeira, n° 70, Centro.	45260-000	5 Mbps
Pojuca	Fórum	Praça Antônio Carlos Magalhães, nº 1.	48120-000	10 Mbps
Porto Seguro	SAJ	Praça Antônio Carlos Magalhães, nº 266.	45810-000	5 Mbps
Porto Seguro	Fórum	Rodovia BR-367, Km27, s/n. Cambolo.	45810-000	20 Mbps
Potiraguá	Fórum	Praça Getúlio Vargas, n° 210.	45790-000	2 Mbps
Prado	Fórum	Rua Presidente Kennedy, s/n.	45980-000	2 Mbps
Presidente Dutra	Fórum	Praça Aurora, s/n.	44930-000	2 Mbps
Presidente Jânio Quadros	Fórum	Avenida Antônio Carlos Magalhães, n° 459.	46250-000	10 Mbps
Queimadas	Fórum	Avenida Nonato Marques, n° 73.	48860-000	5 Mbps
Remanso	Fórum	Rua Virgílio de Sá, n° 06, Quadra 06.	47200-000	5 Mbps
Retirolândia	Fórum	Rua Argemiro Evaristo da Costa, n° 177, 1º andar.	48750-000	5 Mbps
Riachão das Neves	Fórum	Praça Antônio Carlos Magalhães, s/n.	47970-000	2 Mbps
Riachão do Jacuípe	Fórum	Praça Pedro Paulo Mascarenhas, s/n.	44640-000	2 Mbps
Riachão do Jacuípe	Juizado	Rua Aurélio Mascarenhas, n° 150, Centro.	44640-000	2 Mbps
Riacho de Santana	Fórum	Rua Duque de Caxias, n° 225.	46470-000	5 Mbps
Ribeira do Pombal	Fórum	Avenida Evência Brito, s/n.	48400-000	2 Mbps
Rio Real	Fórum	Praça da Bandeira, n° 42.	48330-000	5 Mbps
Ruy Barbosa	Fórum	Rua Corinto Silva, n° 47.	46800-000	5 Mbps
Santa Bárbara	Fórum	Rua Isaltina Campos, s/n.	44150-000	5 Mbps
Santa Cruz de Cabrália	Fórum	BR 367, Km 80, Praia de Mutari.	45807-000	5 Mbps
Santa Inês	Fórum	Praça Araújo Pinho, s/n, Centro.	45320-000	5 Mbps
Santa Maria da Vitória	Fórum	Rua Capitão José Alfaiate, s/n.	47640-000	10 Mbps
Santa Maria da Vitória	Juizado	Rua Desembargador Mário Campos, n° 110, Centro.	47640-000	10 Mbps
Santa Rita de Cássia	Fórum	Praça Ruy Barbosa, s/n.	47150-000	5 Mbps
Santa Terezinha	Fórum	Praça Ápio Medrado, s/n.	44590-000	2 Mbps
Santaluz	Fórum	Praça João Durval Carneiro, s/n.	48880-000	5 Mbps
Santana	Fórum	Rua Monteiro Lobato, s/n.	47700-000	5 Mbps
Santo Amaro	Fórum	Avenida Presidente Vargas, n° 148.	44200-000	10 Mbps
Santo Antônio de Jesus	Fórum	Rua Antônio Carlos Magalhães, s/n, Bairro São Paulo.	44473-440	20 Mbps
Santo Antônio de Jesus	SAJ	Av Luiz Argolo s/n 1º piso Itaguari Sh. Center.	44473-440	5 Mbps
Santo Estevão	Fórum	Avenida Getúlio Vargas.	44190-000	5 Mbps
Santo Estevão	Juizado	Avenida Castro Alves, s/n, Centro.	44190-000	5 Mbps
São Desidério	Fórum	Rua do Estádio, s/n, Tangará.	47820-000	5 Mbps
São Felipe	Fórum	Rua Dom Macedo Costa, n° 311.	44550-000	5 Mbps
São Félix	Fórum	Rua Senador Temístocles, n° 13.	44360-000	10 Mbps
São Francisco do Conde	Fórum	Rua do Asfalto, n° 9, Centro.	43900-000	10 Mbps

Localidade	Unidade	Endereço	CEP	Velocidade
São Gonçalo dos Campos	Fórum	Avenida Aníbal Pedreira, n° 03.	44330-000	5 Mbps
São Sebastião do Passé	Fórum	Rua do Mercado s/n, Centro, Cinco Rios	42800-050	10 Mbps
Sapeaçu	Fórum	Praça da Bandeira, s/n.	44530-000	5 Mbps
Saúde	Fórum	Rua Antônio Ferreira Rocha, s/n.	44740-000	5 Mbps
Seabra	Fórum	Rua Pio XII, n° 100.	46970-000	5 Mbps
Senhor do Bonfim	Fórum	Avenida Roberto Santos, n° 373, Centro.	48970-000	20 Mbps
Senhor do Bonfim	Juizado	Avenida 2 de Julho, 280.	48970-000	10 Mbps
Sento Sé	Fórum	Praça Coronel João Nunes Sento Sé, s/n.	47350-000	5 Mbps
Serra Dourada	Fórum	Praça Pedro José de Aquino, s/n.	47740-000	10 Mbps
Serrinha	Fórum	Avenida Josias Alves Santiago, s/n, Cidade Nova.	48700-000	10 Mbps
Simões Filho	Juizado	Rua Valter Aragão de Souza, Km 25.	43700-000	10 Mbps
Simões Filho	Fórum	Avenida Altamirando de Araújo Ramos, s/n.	43700-000	20 Mbps
Sobradinho	Fórum	Avenida José Balbino de Souza, s/n, Vila São Joaquim.	48925-000	5 Mbps
Tanhaçu	Fórum	Rua Ituaçu, s/n.	46600-000	2 Mbps
Tanque Novo	Fórum	Praça da Matriz, s/n.	46580-000	5 Mbps
Taperoá	Fórum	Rua Francisco Marques Filho, n° 185.	45430-000	5 Mbps
Teixeira de Freitas	Fórum	Avenida Pres. Getúlio Vargas, 1885, Bairro Monte Castelo.	45990-904	20 Mbps
Teixeira de Freitas	Juizado	Avenida Pres. Getúlio Vargas, 3.253.	45995-000	10 Mbps
Teixeira de Freitas	SAC	Avenida São Paulo, 2575 (Shopping Pátio Mix) Bairro Vila Verde.	45990-678	10 Mbps
Teofilândia	Fórum	Praça Lomanto Júnior, n° 229.	48770-000	5 Mbps
Terra Nova	Fórum	Avenida Jaime Vilas Boas, n° 52.	44270-000	2 Mbps
Tremedal	Fórum	Rua Castelo Branco, n° 47.	45170-000	2 Mbps
Tremedal	Fórum	Rua Castelo Branco, n° 47.	45170-000	2 Mbps
Tucano	Fórum	Praça Osvaldo Assunção, s/n.	48790-000	2 Mbps
Uauá	Fórum	Rua da Independência, s/n.	48950-000	2 Mbps
Ubaíra	Fórum	Praça dos Três Poderes, s/n.	45310-000	5 Mbps
Ubaitaba	Fórum	Avenida Presidente Vargas, s/n.	45545-000	5 Mbps
Ubatã	Fórum	Avenida Presidente Vargas, s/n, Centro.	45550-000	10 Mbps
Una	Fórum	Rua São Pedro, n° 10, Bairro Sucupira.	45690-000	5 Mbps
Urandi	Fórum	Praça Luiz Gomes, n° 100.	46350-000	2 Mbps
Uruçuca	Fórum	Praça das Maçons, s/n, Centro.	45680-000	5 Mbps
Utinga	Fórum	Praça Wilson Peixoto Karaoglan, s/n, Centro.	46810-000	5 Mbps
Valença	Fórum	Rua Adauê Charoub, s/n, Grimaldi.	45400-000	20 Mbps
Valença	Juizado	Praça Conselheiro Baltazar, n° 28, antigo Fórum Gonçalo Porto de Souza, Centro.	45400-000	10 Mbps
Valente	Fórum	Rua Everaldino Antônio da Cunha, n° 60, Centro.	48890-000	5 Mbps
Vitória da Conquista	Fórum Cível	Avenida Luiz Fernandes de Oliveira, nº 75, Universidade.	45000-905	20 Mbps
Vitória da Conquista	Fórum Criminal	Praça Estêvão Santos, n° 41, Centro.	45000-905	20 Mbps
Vitória da Conquista	SAJ	Rua Rotary Clube 107, sala108.	45000-905	10 Mbps
Vitória da Conquista	Vara de Infância	Praça Estêvão Santos, n° 41, Centro.	45000-905	10 Mbps
Wenceslau Guimarães	Fórum	Praça Dr. Nelson David Ribeiro, n° 33, Centro.	45460-000	2 Mbps
Xique Xique	Fórum	Praça Francolino José dos Santos, s/n.	47400-000	5 Mbps

Observação: Todos os circuitos são do tipo Avançado.