



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

PREGÃO ELETRÔNICO SRP Nº 90005/2025 – DETRAN/PA

PAE nº E-2024/2528582

RESUMO

PROMOTOR

Departamento de Trânsito do Estado do Pará

CNPJ nº 04.822.060/0001-40

OBJETO

Registro de Preços para eventual e futura contratação de empresa especializada na prestação de serviços de telecomunicações e transmissão de dados, através de uma rede de comunicação digital, determinística, privativa e independente, com locação de roteadores (Solução UTM/NGFW), no-breaks, switches e firewall, cuja finalidade é a interligação corporativa das redes locais (LAN) das unidades do Departamento de Trânsito do Estado do Pará (CIRETRANS e Postos de Atendimento) e acesso IP (Internet Protocol) a rede mundial de internet centralizada na sede do DETRAN/PA, prestação de serviço de transmissão de dados, voz e imagem via satélite, através de solução portátil, móvel com locação de equipamentos e o fornecimento de toda infraestrutura necessária para a solução móvel de fiscalização, incluindo equipamentos, veículos e logística, cujas especificações se encontram detalhadas no Termo de Referência e seus anexos.

MÉTODO DE DISPUTA

Aberto

CRITÉRIO DE JULGAMENTO

Menor Preço Mensal

VIGÊNCIA

24 (vinte e quatro) meses, podendo ser prorrogado, com base no artigo 107 da Lei nº 14.133/2021

REAJUSTE

Índice: IPCA

Período: a cada 12 (doze) meses, a contar da assinatura do contrato

FORMA DE PAGAMENTO

Ordem bancária

Prazo: 30 (trinta) dias corridos, a contar do recebimento da nota fiscal ou da fatura atestada pelo fiscal do Contrato

ABERTURA DA SESSÃO

Dia: 01 de setembro de 2026.

Horas: 10:00 (dez) horas



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

EDITAL

PREGÃO ELETRÔNICO SRP Nº 90005/2025 – DETRAN/PA
Processo Administrativo nº E-2024/2528582

O PROMOTOR deste Pregão é o Departamento de Trânsito do Estado do Pará – DETRAN/PA, CNPJ nº 04.822.060/0001-40, representado pela sua Diretora Geral, e informa aos interessados que, por meio da Pregoeira nomeada pela Portaria nº 3310/2025 - DG/CGP, realizará licitação, para registro de preços, na modalidade **PREGÃO**, na forma **ELETRÔNICA**, com critério de julgamento “**MENOR PREÇO MENSAL**”, em sessão pública que será regida pela Lei Federal nº 14.133/21, Decretos Estaduais nº 2.939/2023 e nº 2.940/2023, Lei Complementar Federal nº 123/2006, demais normas aplicáveis e as condições estabelecidas neste Edital.

Na data, horário e endereço eletrônico abaixo indicado far-se-á a abertura da sessão pública de Pregão Eletrônico, por meio de Sistema Eletrônico COMPRASGOVERNAMENTAIS.

Data da abertura: 01 de setembro de 2026.

Horário: 10:00 (dez) horas (horário de Brasília)

Local: www.comprasgovernamentais.gov.br

UASG: 925447

Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a abertura do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e local estabelecidos no preâmbulo deste Edital, desde que não haja comunicação em contrário da Pregoeira.

1. DO OBJETO

1.1. O objeto desta licitação é o Registro de Preços para eventual e futura contratação de empresa especializada na prestação de serviços de telecomunicações e transmissão de dados, através de uma rede de comunicação digital, determinística, privativa e independente, com locação de roteadores (Solução UTM/NGFW), no-breaks, switches e firewall, cuja finalidade é a interligação corporativa das redes locais (LAN) das unidades do Departamento de Trânsito do Estado do Pará (CIRETRANS e Postos de Atendimento) e acesso IP (Internet Protocol) a rede mundial de internet centralizada na sede do DETRAN/PA, prestação de serviço de transmissão de dados, voz e imagem via satélite, através de solução portátil, móvel com locação de equipamentos e o fornecimento de toda infraestrutura necessária para a solução móvel de fiscalização, incluindo equipamentos, veículos e logística, cujas especificações se encontram detalhadas no Termo de Referência e seus anexos, o qual **ADERE** a este documento para todos os fins.

1.2. Os serviços a serem licitados são os seguintes itens descritos no Termo de Referência:

Item	Descrição	Und	Qtd.	Valor Unitário Estimado Mensal
1	Solução de Telecomunicação Intranet	Und	01	R\$ 2.437.122,85
2	Solução de Telecomunicação – Sub Redes – Sob Demanda	Und	01	R\$ 1.084.497,20
3	Solução de Telecomunicação UPGRADE de 100% de Link de Intranet/Internet a partir do 13º Mês – Sob Demanda	Und	01	R\$ 557.111,03
4	Solução de Telecomunicação – Link de Internet Determinístico – DETRAN/PA – Sede	Und	01	R\$ 846.759,24
5	Solução de Telecomunicação Portátil para Acesso Via Satélite	Und	01	R\$ 74.866,67



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

6	Tabela de Valores de Consumo da Solução de Telecomunicação Portátil e Veicular para Acesso Via Satélite	Und	01	R\$ 261.666,67
7	Composição de Preço para Solução de Telecomunicação Móvel de Fiscalização	Und	01	R\$ 3.188.957,40
8	Composição de Preço de Instalação e Configuração de Todos os Equipamentos nas Localidades	Und	01	R\$ 77.036,89
9	Composição de Preço para Instalação da Base de Infraestrutura para Solução de Telecomunicação Móvel de Fiscalização	Und	01	R\$ 101.051,39
10	Composição de Preço para Serviços de segurança da informação para a Rede de Telecomunicações nas CIRETRANS, POSTOS AVANÇADOS E POSTOS DE FISCALIZAÇÃO	Und	01	R\$ 273.939,36
11	Composição de Preço para Serviços de segurança da informação para a Rede de Telecomunicações para o DETRAN SEDE	Und	01	R\$ 486.904,00
12	Composição de Preço para implantação de Serviços de Gestão da Segurança da Informação para a Rede de Telecomunicações	Und	01	R\$ 1.131.215,00
R\$ 10.521.127,70				

1.3. A licitação observará o seguinte:

1.3.1. Lote único, formado por 12 (dez) itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

1.3.2. O valor máximo mensal do certame é de R\$ 10.521.127,70 (Dez milhões, quinhentos e vinte e um mil, cento e vinte e sete reais e setenta centavos).

2. DO REGISTRO DE PREÇOS

2.1. As regras referentes ao órgão gerenciador e participantes, bem como eventuais adesões são as que constam da minuta de Ata de Registro de Preços.

2. DAS CONDIÇÕES DE PARTICIPAÇÃO

2.1. Poderão participar desta licitação os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores (SICAF) e no Sistema de Compras do Governo Federal (www.gov.br/compras), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

2.1.1. Os interessados deverão atender às condições exigidas no cadastramento no SICAF até o 3º (terceiro) dia útil anterior à data prevista para recebimento das propostas.

2.2. O LICITANTE se responsabiliza pelas transações efetuadas em seu nome, assumindo como verdadeiras suas propostas e lances, excluindo a responsabilidade do provedor do sistema ou do PROMOTOR por danos decorrentes de uso indevido das credenciais de acesso.

2.3. É de responsabilidade do LICITANTE conferir a exatidão dos seus dados cadastrais nos sistemas relacionados no item 2.1 e mantê-los atualizados junto aos órgãos responsáveis pela informação.

2.4. A incorreção dos dados registrados nos sistemas relacionados no item 2.1 poderá motivar a inabilitação do licitante, por descumprimento do dever constante no item anterior.

2.5. Não poderão disputar esta licitação:

a) Aquele que não atenda às condições deste Edital e seus anexos;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- b) Autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;
 - c) Empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação for para serviços ou fornecimento de bens a ela necessários;
 - d) Pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;
 - e) Aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que atue na licitação ou fiscalização ou gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;
 - f) Empresas controladoras, controladas ou coligadas, nos termos da Lei Federal nº 6.404/76, concorrendo entre si;
 - g) Pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos proibidos pela legislação trabalhista;
 - h) Organizações da Sociedade Civil de Interesse Público (OSCIP), atuando nessa condição.
- 2.6. É vedada a participação direta ou indireta de agente público do órgão ou entidade contratante na licitação ou da execução do contrato.
- 2.7. Para o cumprimento do item anterior, deve-se observar situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria.
- 2.8. O impedimento de que trata a alínea “d” do item 2.5 será também aplicado ao LICITANTE que atue em substituição a outra pessoa, física ou jurídica, com a intenção de evitar a aplicação da sanção que impede a participação na licitação, inclusive a sua controladora, controlada ou coligada, desde que comprovada a utilização fraudulenta da personalidade jurídica do LICITANTE.
- 2.9. Desde que o órgão ou entidade julgue necessário para o atendimento da necessidade que motiva a contratação, o autor dos projetos e a empresa a que se referem as alíneas “b” e “c” do item 2.5 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.
- 2.10. As empresas integrantes do mesmo grupo econômico também são consideradas como autoras do projeto.
- 2.11. O disposto nas alíneas “b” e “c” do item 2.5 não impede a licitação ou a contratação de serviço que inclua como obrigação do contratado a elaboração do projeto executivo.
- 2.12. A proibição do item 2.6 também se aplica ao terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.
- 2.13. Não será admitida a subcontratação do objeto contratual.

3. DAS FASES DA LICITAÇÃO, APRESENTAÇÃO DAS PROPOSTAS E DOCUMENTOS DE HABILITAÇÃO

- 3.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.
- 3.2. Os LICITANTES encaminharão por meio do sistema eletrônico as suas propostas com o preço ou percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a abertura da sessão pública.
- 3.3. No cadastramento da proposta inicial, o LICITANTE declarará em campo próprio que:



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- a) Está ciente e concorda com as condições contidas neste edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na legislação, convenções coletivas de trabalho e termos de ajustamento de conduta vigentes na data de sua proposição e que preenche os requisitos de habilitação definidos no instrumento convocatório;
- b) Não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz;
- c) Não possui empregados executando trabalho degradante ou forçado;
- d) Cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.
- e) Se o LICITANTE for organizado em cooperativa, declarará também que cumpre os requisitos estabelecidos no art. 16 da Lei Federal nº 14.133/21.

3.4. As ME's, EPP's ou sociedade cooperativa deverão declarar, ainda, em campo correspondente que cumprem os requisitos estabelecidos no art. 3º da Lei Complementar Federal nº 123/06 e podem usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto no art. 4º, §§ 1º ao 3º, da Lei Federal nº 14.133/21.

3.4.1. Se houver item exclusivo para participação de ME e EPP, a marcação do campo “*não*” impedirá o prosseguimento na licitação para aquele item;

3.4.2. Nos itens em que a participação não for exclusiva para ME e EPP, a marcação do campo “*não*” apenas impedirá que o LICITANTE se beneficie do tratamento favorecido previsto na Lei Complementar nº 123/06, mesmo que ele seja ME, EPP ou sociedade cooperativa.

3.5. A realização de declarações falsas nos itens 3.3 e 3.4 sujeitará o LICITANTE às sanções previstas na Lei Federal nº 14.133/21 e neste Edital.

3.6. Os LICITANTES poderão retirar ou substituir a proposta inserida no sistema até a abertura da sessão pública.

3.7. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo LICITANTE. A classificação ocorrerá somente depois dos procedimentos de abertura da sessão pública e da fase de lances.

3.8. Os documentos que compõem a proposta dos LICITANTES convocados para apresentação de propostas serão disponibilizados para acesso público após a fase de lances.

3.9. Desde que disponibilizada a funcionalidade no sistema, o LICITANTE poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastro da proposta e obedecerá às seguintes regras:

- a) A aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e
- b) Os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

3.10. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo LICITANTE durante a fase de disputa, sendo proibido:

- a) A inserção de lance em valor superior ao já registrado pelo LICITANTE no sistema, quando adotado o critério de julgamento por *menor preço*; e
- b) A inserção de percentual de desconto inferior ao lance já registrado pelo LICITANTE no sistema, quando adotado o critério de julgamento por *maior desconto*.

3.11. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 3.9 será **sigiloso** para os demais LICITANTES e para o PROMOTOR, mas pode ser disponibilizado aos órgãos de controle externo e interno da administração.

3.12. Caberá ao LICITANTE acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela administração ou de sua desconexão.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

3.13. O LICITANTE deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

4. DO PREENCHIMENTO DA PROPOSTA

4.1. O LICITANTE deverá enviar sua proposta por meio do preenchimento dos seguintes campos no sistema eletrônico:

- a) valor global mensal do Lote, em formato numérico e extenso, composto pelo valor de todos os itens que o compõem.
- b) Para fim de julgamento da proposta comercial será considerado o valor GLOBAL MENSAL, considerando a somatória dos serviços por 1 (hum) mês.
- b.1) A apresentação do valor total mensal não isenta o licitante de apresentar, em sua proposta comercial, o valor global anual dos serviços.
- c) Marca.
- d) Fabricante.
- e) Descrição do objeto, contendo informações similares à especificação do Termo de Referência.

4.2. O LICITANTE está vinculado a todas as especificações do objeto feitas na proposta.

4.3. Os valores propostos incluem todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e outros que incidam direta ou indiretamente na execução do objeto.

4.4. Os preços ofertados na proposta inicial e na fase de lances serão de responsabilidade do LICITANTE e são inalteráveis, mesmo na hipótese de erro, omissão ou outro pretexto, salvo a hipótese do item 5.13.

4.5. Nesta licitação, a ME e a EPP poderão se beneficiar do regime de tributação pelo Simples Nacional.

4.6. A apresentação das propostas implica obrigatoriedade ao cumprimento das disposições nela contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios em quantidades e qualidades adequadas à perfeita execução contratual, promovendo sua substituição, quando requerido.

4.8. O prazo de validade da proposta não será inferior a 90 (noventa) dias, a contar da data de sua apresentação.

4.9. Os LICITANTES devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas:

- a) Caso o critério de julgamento seja o de *maior desconto*, o preço decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas.
- b) O descumprimento das regras deste item pode causar a responsabilização pelo Tribunal de Contas do Estado, e, após o devido processo legal, gerar as seguintes consequências:
 - b.1) Determinação, aos envolvidos, de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, IX, da CF/88; e/ou,
 - b.2) Condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao Tesouro, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

5.2. A proposta que identifique o LICITANTE será desclassificada.

5.3. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

5.4. A não desclassificação da proposta não impede que ela seja julgada desclassificada, por ocasião de sua aceitação definitiva.

5.5. O sistema ordenará automaticamente as propostas classificadas.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 5.6. Apenas as propostas classificadas participarão da fase de lances.
- 5.7. O sistema disponibilizará campo próprio para troca de mensagens entre a PREGOEIRA e os LICITANTES.
- 5.8. Iniciada a fase de lances, os LICITANTES deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.
- 5.9. O lance deverá ser ofertado do seguinte modo:
- 5.9.1. O licitante deverá cotar o PREÇO GLOBAL MENSAL DO LOTE, em moeda nacional, em algarismo e por extenso. No caso de divergência entre ambos, o valor por extenso será levado em consideração.
- 5.9.2. O critério de aceitabilidade dos preços unitários e global ofertados pelas licitantes observará rigorosamente os limites máximos fixados nesta contratação, conforme rege o artigo 82, §1º, da Lei nº 14.133/2021.
- 5.9.3. Não serão aceitas propostas com valores incompatíveis com os estimados para a contratação, analisando-se tanto o preço global quanto os preços unitários.
- 5.10. Os LICITANTES poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas neste Edital.
- 5.11. O LICITANTE somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema, conforme o critério de julgamento deste edital.
- 5.12. O intervalo mínimo de diferença de valores ou percentuais entre os lances ofertados pelos LICITANTES será de R\$ 1,00 (um real).
- 5.13. O LICITANTE poderá, uma única vez, excluir seu último lance ofertado, no intervalo de 15 (quinze) segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.
- 5.14. O procedimento observará modo de disputa adotado da seguinte forma:
- 5.14.1. **Modo de disputa Aberto:**
- a) No modo de disputa aberto, os LICITANTES apresentarão lances públicos e sucessivos, com prorrogações.
- b) A fase de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 (dois) minutos da sessão pública.
- c) A prorrogação automática da etapa de lances, de que trata a alínea anterior, será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.
- d) Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública se encerrará automaticamente e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.
- e) Definida a melhor proposta, se a diferença em relação à proposta classificada em 2º lugar for de pelo menos 5%, a PREGOEIRA, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.
- f) Após o reinício previsto na alínea anterior, os LICITANTES serão convocados para apresentar lances intermediários.
- 5.15. Após o término dos prazos estabelecidos no item 5.14, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.
- 5.16. Não serão aceitos 2 ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em 1º lugar.
- 5.17. Durante o transcurso da sessão pública, os LICITANTES serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do LICITANTE.
- 5.18. No caso de desconexão com a PREGOEIRA durante a etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos LICITANTES para a recepção dos lances.
- 5.19. Quando a desconexão do sistema eletrônico para a PREGOEIRA durar mais de 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente após decorridas 24 horas da comunicação deste fato pela PREGOEIRA aos LICITANTES, no sítio eletrônico utilizado para divulgação.
- 5.20. Caso o LICITANTE não apresente lances, concorrerá com o valor de sua proposta.
- 5.21. Em relação a itens não exclusivos para participação de ME's e EPP's, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

identificará em coluna própria as ME's e EPP's participantes, procedendo à comparação com os valores da 1ª colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de se aplicar o disposto nos arts. 44 e 45 da Lei Complementar Federal nº 123/2006, regulamentada pela Lei Estadual nº 8.417/16.

5.21.1. Nessas condições, as propostas de MEs e EPPs que se encontrarem na faixa de até 5% acima da melhor proposta ou melhor lance serão consideradas empatadas com a 1ª colocada.

5.21.2. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da 1ª colocada, no prazo de 5 minutos controlados pelo sistema, contados a partir comunicação automática para tanto.

5.21.3. Caso a ME ou EPP melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais LICITANTES ME e EPP que se encontrem naquele intervalo de 5% na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no item anterior.

5.21.4. No caso de equivalência dos valores apresentados pelas MEs e EPPs que se encontrem nos intervalos estabelecidos nos itens anteriores, será realizado sorteio entre elas para que se identifique aquela que 1º poderá apresentar melhor oferta.

5.22. Só poderá haver empate entre propostas iguais (não seguidas de lances) ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

5.23. Havendo empate entre propostas ou lances, o critério de desempate será:

- a) Disputa final: os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação,
- b) Avaliação do desempenho contratual prévio: deverão ser utilizados, preferencialmente, registros cadastrais, para efeito de atesto de cumprimento de obrigações contratuais previstas nesta Lei,
- c) Desenvolvimento de ações de equidade entre homens e mulheres no ambiente de trabalho: conforme regulamento,
- d) Desenvolvimento de programa de integridade: conforme orientações dos órgãos de controle.

5.24. Persistindo o empate, será assegurada preferência sucessivamente às:

- 1º. Empresas estabelecidas no território do Estado do Pará,
- 2º. Empresas brasileiras,
- 3º. Empresas que invistam em pesquisa e no desenvolvimento de tecnologia no país,
- 4º. Empresas que comprovem a prática de mitigação, nos termos da Lei Federal nº 12.187/2009.

5.25. Na hipótese da proposta do 1º colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação após o encerramento da etapa de lances da sessão pública, a PREGOEIRA poderá negociar condições mais vantajosas depois de definido o resultado do julgamento.

5.26. Se após a negociação com o 1º colocado ele for desclassificado em razão de sua proposta permanecer acima do preço máximo ou inferior ao desconto definido para a contratação pela Administração, a negociação poderá ser feita com os demais LICITANTES, de acordo com a ordem de classificação inicialmente estabelecida.

5.27. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais LICITANTES.

5.28. O resultado da negociação será divulgado a todos os LICITANTES e anexado aos autos do processo licitatório.

5.29. A PREGOEIRA solicitará ao LICITANTE mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado, após a negociação realizada acompanhada dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

5.30. É facultado à PREGOEIRA prorrogar o prazo estabelecido no item anterior, a partir de solicitação fundamentada feita no chat pelo LICITANTE, se o requerimento for feito antes do término do prazo.

5.31. Após a negociação do preço, a PREGOEIRA iniciará a fase de aceitação e julgamento da proposta.

6. DO JULGAMENTO DAS PROPOSTAS

6.1. Encerrada a negociação do preço, a PREGOEIRA verificará se o LICITANTE provisoriamente classificado em 1º lugar atende às condições de participação na licitação, conforme previsto no art. 14 da Lei Federal nº



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

14.133/21, seus regulamentos e este Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

- a) SICAF;
- b) Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/ceis>); e
- c) Cadastro Nacional de Empresas Punidas (CNEP), mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/cnep>).

6.2. A consulta aos cadastros será realizada em nome da empresa LICITANTE e de seu sócio majoritário, considerando a proibição do art. 12 da Lei Federal nº 8.429/92.

6.3. Caso a consulta mostre OCORRÊNCIAS IMPEDITIVAS INDIRETAS, a PREGOEIRA verificará se houve fraude por parte das empresas apontadas no relatório de ocorrências impeditivas indiretas, de acordo com o seguinte procedimento:

- a) A tentativa de fraude será verificada por meio da checagem de vínculos societários, linhas de fornecimento similares ou outros elementos que indiquem a tentativa de fugir da aplicação de sanção impeditiva de licitar ou de contratar;
- b) O LICITANTE será convocado para manifestação antes de uma eventual desclassificação;
- c) Após a defesa e sendo constatada a tentativa de fraudar a aplicação de sanção, o LICITANTE será julgado inabilitado.

6.4. O procedimento de habilitação será iniciado depois de constada a capacidade do LICITANTE participar.

6.5. Caso o LICITANTE provisoriamente classificado em 1º lugar tenha utilizado algum tratamento favorecido às MEs e EPPs, a PREGOEIRA verificará se ele faz jus ao benefício, em conformidade com este Edital.

6.6. Verificadas as condições de participação e de utilização do tratamento favorecido, a PREGOEIRA examinará a proposta classificada em 1º lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos.

6.7. Será desclassificada a proposta vencedora que:

- a) Contiver vícios que não possam ser sanados;
- b) Não obedecer às especificações técnicas contidas no TR;
- c) Apresentar preços inexecutáveis ou permanecerem acima do preço máximo definido para a contratação;
- d) Não tiver sua exequibilidade demonstrada, quando exigido pela administração;
- e) Não estiver de acordo com as exigências deste Edital ou seus anexos, desde que o erro não possa ser sanado.

6.8. É indício de inexecutabilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela administração, devendo a PREGOEIRA investigar a exequibilidade da proposta por meio das seguintes análises:

- a) Verificação se o custo do LICITANTE ultrapassa o valor da proposta; e
- b) Ausência de custos de oportunidade que justifiquem a oferta realizada.

6.9. Somente a verificação dos fatos referidos nas alíneas “a” e “b” do item anterior autoriza a constatação da inexecutabilidade da proposta e a sua consequente desclassificação.

6.10. Se houver indícios de inexecutabilidade da proposta ou em caso da necessidade de esclarecimentos complementares, o LICITANTE poderá ser notificado para comprovar a exequibilidade da proposta.

6.11. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS elaborada pela Administração, o LICITANTE classificado em 1º lugar será convocado para apresentar planilha elaborada por ele com os valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

6.12. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo LICITANTE no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação.

6.12.1. O ajuste de que trata este dispositivo se limita a corrigir erros ou falhas que não alterem a substância das propostas.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

6.12.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

6.12.3. Caso o TR exija a apresentação de amostra, o LICITANTE classificado em 1º lugar deverá apresentá-la conforme ali descrito, sob pena de não aceitação da proposta.

6.12.4. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença é aberta a todos os LICITANTES e interessados.

6.12.5. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

6.12.6. A proposta do LICITANTE será recusada nos seguintes casos:

a. Não entrega ou entrega atrasada da amostra, sem que tenha havido justificativa aceita pela PREGOEIRA; ou

b. Entrega no prazo, mas fora das especificações previstas no TR.

6.12.7. Se a amostra apresentada pelo 1º classificado não for aceita, a PREGOEIRA analisará a aceitabilidade da proposta ou lance ofertado pelo 2º classificado.

6.12.8. Seguir-se-á com a verificação das amostras e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no TR.

6.12.3. DA PROVA DE CONCEITO – POC

a) Caberá ao licitante provisoriamente classificado em primeiro lugar demonstrar as funcionalidades exigidas para a solução ofertada, por meio da Prova de Conceito. Caso o resultado da POC seja satisfatório, o licitante será homologado como vencedor. A Prova de Conceito está especificada em detalhes no Anexo VII do Termo de Referência.

b) No caso do LICITANTE não ser aprovado na Prova de Conceito, o Agente de Licitação convocará a colocada subsequente (observando a ordem de classificação estabelecida no final da etapa competitiva, por meio de lances) e assim sucessivamente, até a apuração de uma proposta que atenda às exigências do Edital.

c) No prazo de 10 (dez) dias úteis após a convocação pelo DETRAN/PA, a licitante convocada deverá iniciar a realização da Prova de Conceito. Os custos de disponibilização de equipamentos para a realização PoC são de responsabilidade da licitante. A PoC da solução ofertada deverá ser realizada sem custo para o DETRAN/PA. O licitante que for reprovado na Prova de Conceito ou não cumpra os prazos acima determinados, não terá direito a qualquer indenização. Será emitido um relatório sucinto, descrevendo os exames realizados e contendo a aprovação ou reprovação da Prova de Conceito.

d) O licitante interessado em acompanhar a PoC deverá, até 1 (um) dia útil antes do início da PoC, informar até dois endereços de e-mail ao Agente de Licitação, para os quais serão enviadas informações para o acompanhamento da POC. Todas as despesas decorrentes de acompanhamento da PoC são de responsabilidade de cada um dos licitantes. No momento de execução da PoC os licitantes deverão apenas assistir ao procedimento de aferição, não sendo permitido interferir, nem interagir durante toda a execução da Prova de Conceito.

f) Caso seja detectada a interferência, o representante do licitante será retirado do ambiente e não poderá mais acompanhar a PoC.

7. DA HABILITAÇÃO

7.1. Além dos documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos, também, para fins de habilitação, os documentos dispostos no item 7.20 em diante, deste edital.

7.2. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

7.3. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

7.4. Se o LICITANTE vencedor for empresa estrangeira que não funcione no País, para fins de assinatura do contrato, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

apostilados nos termos do disposto no Decreto Federal nº 8.660/16, ou consularizados pelos respectivos consulados ou embaixadas.

7.5. Os documentos exigidos para a habilitação poderão ser apresentados em original ou por cópia enviada por meio eletrônico.

7.6. Os documentos exigidos para a habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei Federal nº 14.133/21.

7.7. Será verificado se o LICITANTE apresentou declaração de que atende aos requisitos de habilitação, o declarante responderá pela veracidade das informações prestadas, na forma da lei.

7.8. Será verificado se o LICITANTE apresentou no sistema a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, sob pena de inabilitação.

7.9. O LICITANTE deverá apresentar declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na legislação, convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, sob pena de desclassificação.

7.10. Caso o TR preveja a realização de vistoria, o licitante deve atestar, sob pena de inabilitação, que conhece o local e as condições de realização do serviço, assegurado a ele o direito de realização da vistoria prévia.

7.10.1. O licitante que optar por realizar vistoria prévia terá disponibilizado pela Administração data e horário exclusivos, a ser agendado através do telefone (91) 3214.6312, de modo que seu agendamento não coincida com o agendamento de outros licitantes.

7.10.2. Caso o licitante opte por não realizar vistoria, poderá substituir a declaração exigida por declaração formal, assinada pelo responsável técnico acerca do conhecimento das condições e peculiaridades da contratação.

7.11. A habilitação será verificada por meio do SICAF nos documentos abrangidos por ele.

7.11.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir.

7.12. A verificação em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões pela PREGOEIRA constitui prova para fins de habilitação.

7.13. Os documentos exigidos para habilitação que não estejam contemplados no SICAF serão enviados por meio do sistema, em formato digital, no prazo de, no mínimo, 2 (duas) horas, prorrogável por igual período, contado da solicitação da PREGOEIRA.

7.14. A verificação no SICAF ou a exigência dos documentos nele não contidos somente será feita em relação ao LICITANTE vencedor.

7.15. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em diligência para:

- a) Complementação de informações sobre os documentos apresentados pelo LICITANTE e desde que necessária para apurar fatos existentes à época da abertura da licitação; e
- b) Atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

7.16. Na análise dos documentos de habilitação, o agente de contratação ou a comissão de contratação poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.17. Se o LICITANTE não atender às exigências para habilitação, a PREGOEIRA examinará a proposta subsequente na ordem de classificação até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no item 7.13.

7.18. Somente serão disponibilizados para acesso público os documentos de habilitação do LICITANTE cuja proposta atenda ao edital de licitação, após concluídos o procedimento de habilitação.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.19. A comprovação de regularidade fiscal e trabalhista das MEs e EPPs somente será exigida para efeito de contratação, e não como condição para participação na licitação.

7.20. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

7.20.1. Habilitação jurídica

7.20.1.1. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

7.20.1.2. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

7.20.1.3. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

7.20.1.4. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

7.20.1.5. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

7.20.1.6. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz.

7.20.1.7. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro de 1971.

7.20.1.8. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

7.20.2. Habilitação fiscal, social e trabalhista

7.20.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

7.20.2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

7.20.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

7.20.2.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

7.20.2.5. Prova de inscrição no cadastro de contribuintes Estadual/Distrital e Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

7.20.2.6. Prova de regularidade com a Fazenda Estadual/Distrital e Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

7.20.2.7. Caso o fornecedor seja considerado isento dos tributos Estadual/Distrital ou Municipal/Distrital relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.20.2.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

7.20.2.3. Qualificação Econômico-Financeira

7.20.2.3.1. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

7.20.2.3.2. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

7.20.2.3.3. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

a) índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

b) As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura; e

c) Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

d) Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

7.20.3.4. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação capital mínimo OU patrimônio líquido mínimo de 10% do valor total estimado da contratação.

7.20.3.5. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

7.20.3.6. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

7.20.4. Da Qualificação Técnica:

7.20.4.1. A proponente interessada deverá comprovar mediante apresentação de **Atestado de Capacidade Técnica** fornecido por pessoa jurídica de direito público ou privado para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação. Entende-se por compatível o percentual mínimo de 30% (trinta por cento) dos quantitativos estimados neste documento, contendo o atestado técnico as seguintes informações:

a) Que a licitante fornece ou forneceu a prestação de serviço para **REDE DE COMUNICAÇÃO DIGITAL DETERMINISTICA PRIVATIVA E INDEPENDENTE** descritos nos itens 5, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 6, 6.1, 6.1.1, 6.1.2, 6.1.3, 6.2, 6.2.1, 6.2.2, 6.2.3, 6.3, 6.4, 6.4.1, 6.4.2, 7 e 7.2 do ANEXO I do Termo de Referência,

b) Que a licitante fornece ou forneceu a prestação de serviço para **SERVIÇO DE ACESSO PORTÁTIL E MÓVEL VIA SATÉLITE** descritos nos itens 12, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8 e 12.9. do ANEXO I do Termo de Referência,

c) Que a licitante fornece ou forneceu a prestação de serviço para **SERVIÇO DE SOLUÇÃO DE TELECOMUNICAÇÃO MÓVEL DE POSTO DE FISCALIZAÇÃO** descritos nos itens 14, 14.1, 14.1.1, 14.1.3, 14.3 e 14.3.1 do ANEXO I do Termo de Referência,

d) que a licitante fornece ou forneceu a prestação de serviço para **SERVIÇO DE GERENCIAMENTO DE ATIVOS DE REDE** descritos nos itens 7.5.1.1 ao 7.5.1.4 e dos itens 7.5.3.1 a 7.5.3.9 do ANEXO I do Termo de Referência.

e) No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

e) Fica resguardada à Pregoeira da Licitação a faculdade de executar diligências, para aferir veracidade das informações constantes dos atestados apresentados.

f) O(s) atestado(s) de capacidade técnica deverá ser apresentado em papel timbrado, no qual deve ser informado, para fins de diligência: telefone, endereço, número do contato e duração, bem como os dados do responsável pela elaboração do atestado.

g) A licitante deverá apresentar Declaração de que tem disponibilidade de equipamentos, veículos, pessoal técnico especializado, essenciais para o adequado cumprimento do objeto licitado.

7.20.5. Documentação Técnico-Operacional:

7.20.5.1. Licença SCM (serviço de comunicação multimídia) expedido pela ANATEL e que se encontre na condição de válida, com autorização para prestação dos serviços dentro do território do Estado do Pará ou dentro de todo o território brasileiro, podendo a comprovação ser feita através de consulta no site da ANATEL, ou, através da apresentação do termo SCM da empresa licitante;

7.20.5.2. Apresentação da certidão negativa de débitos de receitas administradas pela ANATEL (FUST, FUNTEL, TFF e contribuição para o fomento da radio fusão pública) que esteja vigente na data da abertura desta licitação, podendo a comprovação ser feita através de consulta no site da ANATEL;

7.20.5.3. Registro válido, junto ao CREA (Conselho Regional de Engenharia e Agronomia) do Estado onde a empresa possua sua matriz;

7.20.5.4. Comprovação de que a empresa licitante possui, em seu quadro técnico, engenheiro com formação na área de telecomunicações, devendo o vínculo de trabalho ser comprovado através de contrato de prestação de serviços, carteira de trabalho ou declaração de contratação futura;

7.20.5.5. Registro do engenheiro de telecomunicações da empresa licitante junto ao CREA (Conselho Regional de Engenharia e Agronomia).

7.20.6. Qualificação Técnica:

7.20.6.1. Qualificação da empresa:

7.20.6.1.1. Atestado(s) de Capacidade Técnica, emitido(s) por pessoa jurídica de direito público ou privado, comprovando a prestação de serviços de SOC 24x7 com SIEM de código aberto por período mínimo de 6 (seis) meses ininterruptos;

7.20.6.1.2. Atestado(s) comprovando a prestação de serviços de resposta a incidentes de segurança (CSIRT);

7.20.6.1.3. Atestado(s) comprovando a prestação de serviço de gestão de riscos cibernéticos de terceiros (TPRM) contemplando, no mínimo, 50 (cinquenta) organizações monitoradas;

7.20.6.1.4. Declaração formal de que opera Centro de Operações de Segurança próprio em território brasileiro, com indicação do endereço, passível de visita técnica pela CONTRATANTE;

7.20.6.1.5 Comprovação de que as plataformas ofertadas atendem aos itens 19.3.1. (código aberto / desenvolvimento próprio) e 19.3.2. (hospedagem no Brasil) do ANEXO I do Termo de Referência;

7.20.6.1.6. A licitante deverá apresentar, no mínimo, 01 (um) Atestado de Capacidade Técnica emitido por pessoa jurídica de direito público ou privado, comprovando a execução satisfatória de serviços de monitoramento e observabilidade de ambientes de Tecnologia da Informação, contemplando ambiente com quantitativo igual ou superior a 500 (quinhentos) ativos monitorados, compatível em características, complexidade e volume com o objeto da presente contratação.

7.20.6.2. Qualificação e certificações da equipe técnica:

7.20.6.2.1. Para a execução dos serviços, a CONTRATADA deverá comprovar que a equipe alocada possui as seguintes certificações técnicas vigentes, conforme o escopo de atuação de cada profissional:

Perfil profissional	Certificações exigidas (mínimo)



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Perfil profissional	Certificações exigidas (mínimo)
Engenheiro e ou Coordenador de SOC	Pelo menos uma: CISSP, GSEC, SABSA, CEH, CISM, CRISC, CGEIT ou ISO/IEC 27001 (Auditor/Implementador).
Analista de Segurança de Perímetro (Firewall e VPNs)	ISFS (Information Security Foundation); desejável certificação do fabricante do firewall utilizado pela CONTRATANTE (ex.: Fortinet NSE).
Analista I - CSIRT	Linux LPIC-1 ou ISFS.
Analista II - CSIRT	Linux LPIC-1, ISFS ou CEH.
Analista III - CSIRT	CompTIA Security+ ou CEH.
Analista Forense Digital	Pelo menos uma: ACE, ACFEI, CCFT, CEH, CHFI, EnCE ou certificação de nível GIAC.
Analista de Governança de TI e Riscos (TPRM)	Pelo menos uma: CRISC, CISM, CGEIT, ITIL Foundation v3 (ou superior), CompTIA Security+, CEH, COBIT 5, COBIT 2019 ou ISO/IEC 27001.
Analistas de Assessment (Níveis I, II e III)	ISFS, Auditor Interno/Externo ISO 27001 ou CEH.
Head de Monitoramento e Observabilidade (NOC)	Certificação ITIL Foundation V3 ou superior; Zabbix Certified Specialist (ZCS); Zabbix Certified Professional (ZCP); Zabbix Certified Expert (ZCE).
Coordenador de Monitoramento (NOC)	Certificação Zabbix Certified Specialist (ZCS); Zabbix Certified Professional (ZCP).
Analista Sênior de Monitoramento (NOC)	Certificação ITIL Foundation V3 ou superior; Zabbix Certified Specialist (ZCS); Zabbix Certified Professional (ZCP); Zabbix Certified Expert (ZCE).
Analista de Monitoramento e Observabilidade (NOC)	Certificação Zabbix Certified Specialist (ZCS).

7.20.6.2.2. As comprovações dar-se-ão por meio de certificados válidos e vínculo formal dos profissionais com a PROPONENTE (contrato de trabalho, contrato de prestação de serviços ou declaração de contratação futura vinculada à assinatura do contrato).

8. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

8.1. O objeto da licitação será adjudicado ao licitante declarado vencedor pela autoridade competente, após a regular decisão dos recursos eventualmente apresentados.

8.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

9. DA ATA DE REGISTRO DE PREÇOS

9.1. Homologado o resultado da licitação, o licitante mais bem classificado, terá o prazo de 10 (dez) dias úteis, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

9.2. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante convocado, desde que:

- a) a solicitação seja devidamente justificada e apresentada dentro do prazo; e
- b) a justificativa apresentada seja aceita pela Administração.

9.3. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no sítio eletrônico www.compraspara.pa.gov.br e no Portal Nacional de Contratações Públicas (PNCP).

9.4. Serão formalizadas tantas Atas de Registro de Preços quantas forem necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor, descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

9.5. O preço registrado, com a indicação dos fornecedores, será divulgado no PNCP e disponibilizado durante a vigência da ata de registro de preços.

9.6. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

9.7. Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidas no edital, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

9.8. Formação do cadastro de reserva:

9.8.1. Após a homologação da licitação, será incluído na ata, na forma de anexo, o registro:

- a) dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação da licitação; e
- b) dos licitantes que mantiverem sua proposta original.

9.8.2. Será respeitada, nas contratações, a ordem de classificação dos licitantes registrados na ata.

9.8.3. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante mais bem classificado.

9.8.4. Para fins da ordem de classificação, os licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário antecederão aqueles que mantiverem sua proposta original.

9.8.5. A habilitação dos licitantes que comporão o cadastro de reserva será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

- a) Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital; ou
- b) Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas nos arts. 24 e 25 do Decreto Estadual nº 3.371/2023.

9.8.6. Na hipótese de nenhum dos licitantes aceitar cotar o objeto com preço igual ao do adjudicatário e concordar com a contratação nos termos em igual prazo e nas condições propostas pelo primeiro classificado, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

- a) Convocar os licitantes que mantiveram sua proposta original para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou
- b) Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes remanescentes, observada a ordem classificatória, quando frustrada a negociação de melhor condição.

10. DO CONTRATO



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

10.1. Após a publicação da Ata de Registro de Preços, o prazo para assinatura do contrato será de até 05 (cinco) dias úteis contados a partir da convocação do adjudicatário, podendo ser prorrogado uma vez por igual período, desde que ocorra motivo justificado e aceito pela Administração.

10.2. Farão parte integrante do contrato este TERMO DE REFERÊNCIA, Edital, Anexos e a Proposta apresentada pela LICITANTE vencedora.

10.3. Incumbirá ao CONTRATANTE providenciar a publicação resumida do instrumento do contrato e de seus eventuais termos aditivos, no Diário Oficial do Estado.

11. DA VIGÊNCIA

11.1. Inicialmente, será formalizada Ata de Registro de Preços com o LICITANTE vencedor, com prazo de vigência de 01 (um) ano, prorrogável pelo mesmo período, nos termos do art. 84 da Lei Federal nº 14.133/2021, com permissibilidade de adesão nos termos do Decreto Estadual nº 3.371/2023 e demais legislações correlatas.

11.2. Para a prestação dos serviços será formalizado um Contrato Administrativo estabelecendo em suas cláusulas todas as condições, garantias, obrigações e responsabilidades entre as partes, em conformidade com o Termo de Referência e seus anexos, além da proposta de preços da licitante vencedora.

11.3. O Contrato terá vigência de 24 (doze) meses a partir da data de sua publicação no Diário Oficial do Estado, podendo ser prorrogado por interesse das partes até o limite previsto na legislação, com base no artigo 107 da Lei federal nº 14.133/2021.

11.4. O preço ofertado na proposta da CONTRATADA deve ser fixo e irreajustável por um período de 12 (doze) meses.

12. DA GARANTIA CONTRATUAL

12.1. O CONTRATADO garantirá o cumprimento do contrato mediante a prestação de uma das modalidades de garantia previstas no art. 96, §1º, da Lei Federal nº 14.133/21, a sua escolha.

12.2. A garantia corresponderá a 1% (hum por cento) do valor atualizado do contrato.

12.3. A garantia em dinheiro deverá ser efetuada em conta bancária de titularidade do CONTRATANTE, cujos dados são:

Banco Banpará

Agência nº xxxx-x

Conta-corrente nº xxxxxx-x.

12.4. Na hipótese de suspensão do contrato por ordem ou inadimplemento do CONTRATANTE, o CONTRATADO ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pelo CONTRATANTE.

12.5. No caso de alteração do valor do Contrato, ou prorrogação de sua vigência, a garantia deverá ser atualizada ou renovada nas mesmas condições.

12.6. Se a garantia for utilizada em pagamento de qualquer obrigação, o CONTRATADO fica obrigado a recompor o que tiver sido usado no prazo máximo de 5 (cinco) dias úteis, a contar de sua notificação.

12.7. O CONTRATANTE executará a garantia na forma prevista na legislação.

12.8. A garantia prestada pelo CONTRATADO será liberada ou restituída após a execução total do contrato ou após a sua extinção por culpa exclusiva do CONTRATANTE.

12.9. Quando a garantia for em dinheiro, o valor a ser devolvido, nos termos do item 12.8, será corrigido monetariamente.

12.10. A garantia de execução do contrato não desobriga o CONTRATADO de apresentar a garantia contratual dos bens adquiridos, legal e do fabricante, a qual deve ser de 15 (quinze) dias úteis, no mínimo.

13. DOS RECURSOS

13.1. A apresentação de recurso contra o julgamento das propostas, habilitação ou inabilitação de LICITANTES, a anulação ou a revogação da licitação observará o disposto no art. 165 da Lei Federal nº 14.133/21.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

13.2. O prazo recursal é de 3 (três) dias úteis, contados da data da notificação da decisão a ser recorrida ou de lavratura da ata.

13.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do LICITANTE, deve-se observar o seguinte:

- a) O tempo para manifestação da intenção de recorrer não seja inferior a 10 (dez) minutos;
- b) A intenção de recorrer deverá ser manifestada imediatamente, sob pena de não ser possível apresentar o recurso; e
- c) O prazo para apresentação das razões do recurso será iniciado na data da notificação da decisão ou da lavratura da ata de habilitação ou inabilitação.

13.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

13.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá:

- a) Reconsiderar sua decisão no prazo de 3 (três) dias úteis; ou
- b) Encaminhar o recurso, no prazo de 3 (três) dias úteis, para a autoridade superior, que deverá decidi-lo no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

13.6. Os recursos apresentados fora do prazo não serão conhecidos.

13.7. O prazo para apresentação de contrarrazões ao recurso pelos demais LICITANTES será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista dos elementos indispensáveis à defesa de seus interesses.

13.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que a autoridade competente emita a sua decisão final.

13.9. O acolhimento do recurso invalida tão somente os atos que não possam ser aproveitados.

13.10. Os autos do processo permanecerão acessíveis aos interessados por meio do Portal ComprasPará.

14. DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

14.1. Constituem infrações administrativas do CONTRATADO a serem punidas com as seguintes sanções:

INFRAÇÃO	PENALIDADE
a. Dar causa à inexecução parcial do contrato.	Advertência* * Exceto quando se justificar a imposição de penalidade mais grave, ocasião em que poderá ser aplicada a sanção de “ <i>Impedimento de licitar e contratar</i> ”.
b. Dar causa à inexecução parcial do contrato que cause grave dano ao CONTRATANTE ou ao funcionamento dos serviços públicos ou ao interesse coletivo. c. Dar causa à inexecução total do contrato. d. Deixar de entregar a documentação exigida para o certame. e. Deixar de manter sua proposta, salvo em decorrência de fato superveniente devidamente justificado. f. Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado.	Impedimento de licitar e contratar* * Exceto quando se justificar a imposição de penalidade mais grave, ocasião em que poderá ser aplicada a sanção de “ <i>Declaração de inidoneidade para licitar e contratar</i> ”.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

g. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou execução do contrato. h. Fraudar a contratação ou praticar ato fraudulento na execução do contrato. i. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza. j. Praticar atos ilícitos com vistas a frustrar os objetivos do certame. k. Praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846/13.	Declaração de inidoneidade para licitar e contratar

14.2. O atraso superior a 15 (quinze) dias corridos autoriza a rescisão do contrato por seu descumprimento, nos termos do art. 137, I, da Lei Federal nº 14.133/21.

14.3. A aplicação das sanções previstas neste contrato não exclui a obrigação de reparação integral do dano causado ao CONTRATANTE.

14.4. As sanções podem ser cumuladas com as seguintes multas:

MULTA	
Moratória a. 0,1% (zero vírgula um por cento) sobre o valor da parcela inadimplida por dia de atraso injustificado até o limite de 15 dias corridos. b. 1% (um por cento) sobre o valor total do contrato por dia de atraso injustificado até o limite de 30 dias corridos, pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.	Compensatória 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do seu objeto.

14.5. Antes da aplicação das sanções, o CONTRATADO será notificado para apresentar defesa no prazo de 15 (quinze) dias úteis, contado de sua intimação.

14.6. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor devido ao CONTRATADO, além da perda deste valor, a diferença será descontada da garantia prestada e/ou será cobrada judicialmente.

14.7. Antes do ajuizamento da cobrança, a multa poderá ser recolhida administrativamente em até 15 (quinze) dias úteis, a contar do trânsito em julgado da decisão administrativa.

14.8. A aplicação das sanções será precedida de processo administrativo em que seja assegurado o contraditório e a ampla defesa ao CONTRATADO, observando o rito especial previsto no art. 158 da Lei Federal nº 14.133/21 para as penalidades de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar.

14.9. A aplicação das sanções deve observar:

- a) A natureza e gravidade da infração.
- b) As peculiaridades do caso.
- c) As circunstâncias agravantes e/ou atenuantes.
- d) Os danos causados ao CONTRATANTE.

14.10. A implantação ou aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

14.11. As infrações administrativas tipificadas como atos lesivos na Lei Federal nº 12.846/13 serão apuradas e julgadas em conjunto com as infrações previstas neste contrato, nos mesmos autos.

14.12. A personalidade jurídica do CONTRATADO poderá ser desconsiderada quando for utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste contrato ou para



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

provocar confusão patrimonial e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o CONTRATADO, observados o contraditório, ampla defesa e a obrigatoriedade de análise jurídica prévia.

14.13. No prazo de 15 (quinze) dias úteis, a contar da data de aplicação da sanção, o CONTRATANTE informará e manterá atualizados os dados relativos às sanções aplicadas por ela, para publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

14.14. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação, na forma do art. 163 da Lei Federal nº 14.133/21.

14.15. Caso ocorra degradação do tipo, aumento no tempo de resposta, ou aumento na taxa de erro, ou aumento na latência (entende-se por degradação como sendo toda interferência que venha causar sucessivas retransmissões de pacotes no circuito de dados), acumulativa superior a 4 (quatro) horas no período de 30 (trinta) dias, a CONTRATADA será penalizada com multa compensatória sobre o valor mensal do circuito a cada hora pelas interrupções temporárias a serem descontadas no preço da fatura do circuito, cumulativa até o máximo de 10% (dez por cento) do valor total da fatura mensal do circuito, conforme a tabela abaixo:

<i>Criticidade</i>	<i>Multa por hora</i>
<i>1</i>	<i>0,1%</i>
<i>2</i>	<i>0,25%</i>
<i>3</i>	<i>0,5%</i>
<i>4</i>	<i>0,75 %</i>
<i>5</i>	<i>1 %</i>

Tabela 2 - Aplicação de Penalidades por Degradação

14.15.1. Para aplicação do disposto neste item a CONTRATANTE terá que registrar junto a Central de Atendimento da CONTRATADA a ocorrência de degradação. Após o registro a CONTRATADA terá o período de 04 (quatro) horas para circuitos da Região Metropolitana de Belém e 12 (doze) horas para os demais circuitos para testes e recuperação dos mesmos. Terminados estes prazos as multas compensatórias serão praticadas conforme a criticidade acima definida, considerando o período total de degradação registrado conforme o item 6.3.2 do Anexo I do Termo de Referência.

14.16. Haverá desconto dos valores na fatura da CONTRATADA, nos termos deste item, conforme critérios de cálculo estabelecidos em caso de interrupções da prestação do serviço, que não sejam causadas por:

- a) Caso fortuito ou força maior (entende-se como caso fortuito como sendo qualquer ocorrência que não seja proveniente de qualquer ação humana).
- b) Operação inadequada, falha ou mau funcionamento de equipamentos não mantidos pela CONTRATADA.
- c) Falha de equipamento de propriedade ou sob responsabilidade da CONTRATADA, ocasionada pela CONTRATANTE ou seus clientes.
- d) Falha na infraestrutura da CONTRATANTE.
- e) Realização de testes, ajustes e manutenção necessários à prestação do serviço, devidamente comunicados à CONTRATANTE com antecedência mínima de 5 (cinco) dias úteis ou em caso comprovado de urgência, conforme item 6.4.5 do Anexo I do Termo de Referência.
- f) Impedimento, por qualquer motivo, do acesso de pessoal técnico da CONTRATADA às dependências da CONTRATANTE, onde estejam localizados os equipamentos da CONTRATADA ou por estes mantidos, desde que devidamente comunicados a CONTRATANTE.
- g) Falta de energia elétrica nas dependências da CONTRATANTE.

14.17. A CONTRATADA trabalhará de forma proativa informando à CONTRATANTE sobre o andamento do processo de recuperação em até 30 (trinta) minutos após o registro do problema e a cada intervalo de 2 (duas) horas, informando inclusive a estimativa de tempo para a completa solução do problema.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

14.18. Falhas em equipamentos ou serviços de propriedade ou responsabilidade da CONTRATADA que impliquem em suspensão dos serviços prestados pela CONTRATANTE, motivarão a aplicação de multas compensatórias e descontos referentes à hora parada, ressalvado as condições listadas no item 14.17.

14.19. A CONTRATADA deverá executar a recuperação do circuito com problema em prazo determinado na coluna “Tempo Máximo de Reparo” do Anexo IV deste edital. Caso a CONTRATADA não consiga cumprir o prazo determinado pela CONTRATANTE para resolução do problema, incidirão multas compensatórias de 1% (um por cento) do valor mensal do circuito, para cada hora de paralisação, cumulativa até o máximo de 10% (dez por cento) do valor total da fatura mensal do circuito. Fica a critério da CONTRATANTE o desconto sobre a fatura mensal ao qual o circuito em questão esteja inserido, ou seu respectivo pagamento em conta, no prazo de até 30 (trinta) dias consecutivos.

Item	Critérios
Penalidade sobre o tempo de interrupção no circuito (fim-a-fim). Previsto para o não cumprimento do “Tempo Máximo de Reparo”	A cada hora de interrupção, após decorrido o tempo máximo de reparo constante no anexo IV, nas 2 (duas) primeiras horas
	A cada hora de interrupção contada após as 2 (duas) primeiras horas

Tabela 3 - Aplicação de Penalidades por Tempo Máximo de Reparo

14.20. O desconto referente à Hora Parada do Circuito será aplicado ao valor do circuito parado sob responsabilidade da CONTRATADA, conforme fórmula abaixo. Fica a critério da CONTRATANTE o desconto sobre a fatura mensal ao qual o circuito em questão esteja inserido, ou seu respectivo pagamento em conta, no prazo máximo de 30 (trinta) dias consecutivos.

Valor do desconto por Hora Parada = (Valor do circuito / 720) Quant. de Horas Paradas.

Valor do desconto mensal = Quant. de Horas Paradas x Valor do desconto por Hora Parada.

14.20.1. Para efeito de cálculo, as penalidades deverão ser aplicadas baseadas em horas fracionadas.

15. DA IMPUGNAÇÃO AO EDITAL

15.1. Qualquer pessoa pode impugnar este Edital por irregularidade na aplicação da Lei Federal nº 14.133/21 ou solicitar esclarecimento sobre os seus termos.

15.2. A impugnação ou solicitação de esclarecimento pode ser feita até 3 (três) dias úteis antes da data da abertura da sessão pública.

15.3. A resposta à impugnação ou à solicitação de esclarecimento será divulgada em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

15.4. A impugnação e a solicitação de esclarecimento poderão ser realizadas por meio eletrônico, através do correio eletrônico patricia.cunha@detran.pa.gov.br.

15.5. As impugnações e as solicitações de esclarecimentos não suspendem os prazos previstos na licitação.

15.6. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

15.7. Acolhida a impugnação, será definida e publicada nova data para a realização da licitação, observados os prazos mínimos para a apresentação das propostas e lances previstos no Decreto Estadual nº 2.940/2023.

16. DAS DISPOSIÇÕES FINAIS

16.1. A ata da sessão pública será divulgada no sistema eletrônico.

16.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização da licitação na data marcada, a sessão será automaticamente transferida para o 1º dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pela PREGOEIRA.

16.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília-DF.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 16.4. A homologação do resultado desta licitação não implicará direito à contratação.
- 16.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os LICITANTES, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.
- 16.6. Os LICITANTES assumem todos os custos de preparação e apresentação de suas propostas e a Administração não poderá ser responsabilizada por esses custos, independentemente da condução ou do resultado do processo licitatório.
- 16.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento.
- 16.8. Só se iniciam e vencem os prazos em dias de expediente na Administração.
- 16.9. O desatendimento de exigências formais não essenciais não importará o afastamento do LICITANTE, desde que seja possível o aproveitamento do ato, observados o princípio da isonomia, a finalidade e a segurança da contratação.
- 16.10. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerão as deste Edital.
- 16.11. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas e no Portal ComprasPará.
- 16.12. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:
- 16.12.1. Estudo Técnico Preliminar,
 - 16.12.2. Termo de Referência,
 - 16.12.3. ANEXO I – ESPECIFICAÇÕES TÉCNICAS,
 - 16.12.4. ANEXO II – CONDIÇÕES GERAIS,
 - 16.12.5. ANEXO III – TOPOLOGIA,
 - 16.12.6. ANEXO IV – SOLUÇÃO DE TELECOMUNICAÇÃO – CARACTERÍSTICAS DO CIRCUITO,
 - 16.12.7. ANEXO V – PLANILHAS DE PREÇOS DE REFERÊNCIA,
 - 16.12.8. ANEXO VI – MODELO DE PROPOSTA,
 - 16.12.9. ANEXO VII – PROVA DE CONCEITO,
 - 16.12.10. ANEXO VIII – DECLARAÇÃO DE SUPERVENIÊNCIA,
 - 16.12.11. ANEXO IX – DECLARAÇÃO DE MENOR,
 - 16.12.12. ANEXO X – MODELO DE ATESTADO DE VISITA TÉCNICA,
 - 16.12.13. ANEXO XI – ENDEREÇOS DAS LOCALIDADES PARA INSTALAÇÃO DOS LINKS,
 - 16.12.14. ANEXO XII – DECLARAÇÃO PARA MICROEMPRESA E EMPRESA DE PEQUENO PORTE,
 - 16.12.15. ANEXO XIII – DECLARAÇÃO DE COTA DE PESSOAS COM DEFEICIÊNCIA NO QUADRO DE EMPREGADOS,
 - 16.12.16. ANEXO XIV – ATA DE REGISTRO DE PREÇOS,
 - 16.12.17. ANEXO XV – MINUTA DE CONTRATO.

Belém/Pa, 05 de agosto de 2026.

RENATA MIRELLA FREITAS GUIMARÃES DE SOUZA COELHO
Diretora Geral
DETRAN/Pa



GOVERNO DO ESTADO DO PARÁ
Departamento de Trânsito do Estado do Pará

ESTUDO TÉCNICO PRELIMINAR 2025
PAE Nº 2025/

DESCRIÇÃO DA NECESSIDADE	
Qual a necessidade a ser atendida?	A presente contratação de serviços de comunicação é fundamental para a interconexão integral e contínua de todas as unidades descentralizadas do Departamento de Trânsito do Estado do Pará (DETRAN/PA), abrangendo as Circunscrições Regionais de Trânsito (CIRETRANS), postos fixos e móveis de atendimento, a infraestrutura de fiscalização de trânsito e as ações itinerantes, com a Sede administrativa. Essa interligação estabelece uma rede de dados privativa e segura, essencial para o controle rigoroso e a gestão eficiente de todas as informações trafegadas. A exclusividade dessa rede é o único meio de garantir o acesso restrito e autorizado aos sistemas finalísticos e de apoio do DETRAN/PA, bem como à Base Nacional de Condutores e Veículos do SENATRAN. Tal medida é condição sine qua non para preservar a confidencialidade, integridade e disponibilidade dos dados de condutores e veículos, alinhada às políticas de segurança e eficiência. Necessidades Detalhadas e Abrangência Territorial A necessidade primordial reside em assegurar que quaisquer atividades e serviços prestados pelo DETRAN/PA possam ser realizados a todo tempo e em qualquer localidade dentro do vasto território geográfico do Pará, seguindo um padrão único e regras consistentes de política de segurança. ● Alcance Irrestrito: O serviço de comunicação deve garantir a conectividade independentemente da localização das unidades (CIRETRANS, Postos de Serviços, ações itinerantes e infraestrutura de fiscalização), cobrindo a extensão total do território paraense. ● Expansão da Presença Institucional: É de vital importância ampliar a cobertura e a presença do DETRAN/PA, sobretudo nas regiões de fronteira com os estados do Maranhão, Tocantins e Mato Grosso. Essa estratégia visa evitar o deslocamento de cidadãos paraenses em busca de serviços em DETRANS de outros estados, suprimindo a ausência de atendimento e oferecendo uma solução de proximidade ao cliente. Impacto Econômico e Sustentação da Receita Estadual O serviço de comunicação é indispensável para a implementação de soluções tecnológicas avançadas em um estado de grande dimensão geográfica, com impactos diretos e significativos na esfera econômica: ● Aumento da Arrecadação: A modernização e a capilaridade dos serviços possibilitarão o crescimento progressivo e sustentável na arrecadação de



GOVERNO DO ESTADO DO PARÁ

Departamento de Trânsito do Estado do Pará

	tributos, taxas e impostos. O DETRAN/PA é uma das principais fontes de receita para: ○ A SEFA (Secretaria de Estado da Fazenda), no que tange ao Imposto sobre a Propriedade de Veículos Automotores (IPVA). ○ Os Municípios, por meio de receitas provenientes de licenciamentos e multas. ○ O BANPARÁ, em razão da movimentação de serviços bancários específicos vinculados ao órgão. ● Sustentação da Receita: A continuidade e a eficiência dos serviços de comunicação são, portanto, de caráter essencial para a sustentação e estabilidade da receita estadual. Imperativo da Digitalização e Continuidade do Serviço Público Em um cenário global cada vez mais digitalizado, os serviços essenciais do DETRAN/PA – como a transferência de propriedade, a emissão do Certificado de Registro e Licenciamento de Veículo (CRLV) e da Carteira Nacional de Habilitação (CNH) – são integralmente digitais. Neste diapasão, a continuidade e a robustez dos serviços de comunicação são uma condicionante inegociável para o atendimento eficaz do anseio público, garantindo a modernização e a acessibilidade do serviço estatal de trânsito.		
DESCRIÇÃO DOS REQUISITOS DE CONTRATAÇÃO			
Qual o tipo de objeto?	☐ Bem.		
	☒ Prestação de Serviços comum.		
Qual a natureza?	☒ Continuada	☐ Com monopólio.	
		☒ Sem monopólio.	
	☐ Não continuada.		
Qual a vigência?	☐ 30 dias (pronta entrega).		
	☐ 180 dias.		
	☒ 24 meses.		
	☐ Indeterminado.		
Poderá haver prorrogação ?	☒ Sim. Considerando que se trata de um serviço essencial e a prestação deve ser contínua, sem interrupção para atendimento da necessidade tecnológica e operacional do DETRAN/PA, com ênfase no interesse público, em conformidade ao disposto na Lei Federal nº 14.133/2021.		
		Contrato nº:	007/2018.



GOVERNO DO ESTADO DO PARÁ
Departamento de Trânsito do Estado do Pará

Há transição com contrato anterior?	☒ Sim.	Prazo final:	17/05/2024.
	☐ Não.		
Padrão mínimo de qualidade	Item	Descrição detalhada	
	1	Rede de comunicação digital, privativa e independente.	
	2	A Licitante deve ter a Licença SCM (serviço de comunicação multimídia) expedido pela ANATEL.	
	3	A rede de comunicação digital deve ter garantia de desempenho, privacidade e suporte a diversos protocolos, além de permitir a utilização de endereçamento IP privativo	
	4	Infraestrutura de Rede de Comunicação Digital (backbone), utilizando circuitos privativos, ponto-a-ponto ou ponto-multiponto	
	5	Local via enlace de alta velocidade através de fibra óptica em rotas alternativas e redundantes, instaladas fisicamente em SWITCHS METRO, utilizando equipamentos de comunicação de rede e segurança capazes de suportarem fail-over e load balance	
Há critérios de sustentabilidade?	☒ Sim.	A Contratada deve utilizar materiais e equipamentos que não atentem contra o meio ambiente, devendo obedecer as normas técnicas do meio ambiente e ser aplicada uma tecnologia auto sustentável.	
	☐ Não.		
Há necessidade de treinamento?	☐ Sim.		
	☒ Não. Devido ser auto aplicável.		
LEVANTAMENTO DE MERCADO			
Onde foram pesquisadas as possíveis soluções?	☐ Consulta a fornecedores.		☒ Contratações similares.
	☐ Internet.		☐ Audiência pública.
	☒ Outro.	Especificar: COMPRAS PARÁ, não havendo ATAS DE REGISTRO DE PREÇOS do Estado do Pará vigentes para os objetos em questão. Tomaram-se por base contratações anteriores, sendo essa uma solução cabível para resolução da necessidade. Também foram pesquisadas no site oficial do Governo Federal voltado à contratações públicas	
Justificativa técnica e econômica para a escolha da melhor solução	A empresa contratada deve atentar a questão de qualidade técnica dos serviços propostos, a confiabilidade e experiência da empresa na prestação de serviço desta natureza, observância se presta o serviço em alusão ao objeto do TR, em especial, a comunicação de dados, transmissão e infraestrutura. Portanto, a escolha da empresa se sustentará pela qualidade na prestação, pois não apenas se atentar a preço, mas o conjunto da solução que ora já é aplicada. Portanto, o conjunto proposto deve ser justificado na qualidade para de fato e de direito ser a melhor solução e atendimento ao anseio do DETRAN/PA.		



GOVERNO DO ESTADO DO PARÁ
Departamento de Trânsito do Estado do Pará

Há restrição de fornecedores?	☒ Não.	
DESCRIÇÃO DA SOLUÇÃO		
O que será contratado?	A contratação pretendida visa contemplar serviços telecomunicação é de natureza continuada, serviço de extrema necessidade e vital para o funcionamento de todos os sistemas finalísticos desta autarquia. Os serviços prestados de forma contínua são aqueles que, pela sua essencialidade, visam atender à necessidade pública de forma permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público ou o funcionamento das atividades finalísticas do órgão ou entidade, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional. Ressaltamos a capacidade e disponibilidade de banda de transmissão e recebimento de dados de todos os pontos remotos (CIRETRANS e POSTOS DE SERVIÇOS) interligados com o DETRAN/PA-SEDE, constatou-se a necessidade da continuidade de banda em cada localidade, assim como, a quantidade de acesso portátil e móvel via satélite que atendam às necessidades dos serviços de fiscalização e atendimento itinerante realizadas pelo DETRAN-PA dentro do extenso território geográfico do estado do Pará, incluindo os seus 144 (cento e quarenta e quatro) municípios e da necessidade de implantação de solução	
	móvel de postos de fiscalização para atender as demandas de atendimento Itinerantes da CNCIR (Coordenadoria do Núcleo da Circunscrições de Trânsito) e de fiscalização da DTO (Diretoria Técnica operacional) para o maior controle na fiscalização e apoio dos condutores e seus veículos que trafegam nas estradas e rodovias do estado do Pará que estão sob a jurisdição do DETRAN- PA. Cabe enfatizar que a sustentação do Programa CNH Pai d'égua é oriunda de tecnologia móvel e infraestrutura. Ressalta-se que foi observada a infraestrutura da Fiscalização de Trânsito garantindo uma estrutura robusta e capaz de oferecer conforto, segurança e tecnologia. Portanto, o objeto da contratação está sob a égide do de link de comunicação, transmissão de dados, telecomunicações, interligação entre postos fixos e móveis e infraestrutura.	
Qual o prazo da garantia contratual?	☐ Não há.	
	☐ 90 dias.	
	☒ 12 meses, a Contratada , deverá no prazo de 10 (dez) dias após a assinatura do Contrato prestar a garantia de 1% (um por cento) do valor global do contrato.	
		☐ dias.
	Outro:	☐ meses.
Há necessidade de assistência técnica?	☒ Sim.	Considerando que os equipamentos são de uso contínuo poderá causar dano, com isso há necessidade de regular acompanhamento para possível troca no decorrer do contrato.



GOVERNO DO ESTADO DO PARÁ
Departamento de Trânsito do Estado do Pará

	☐ Não.			
Há necessidade de manutenção?	☒ Sim.	A manutenção deverá ser de cunho preventivo e corretivo no decorrer do contrato.		
	☐ Não.			
ESTIMATIVA DO QUANTITATIVO NECESSÁRIO				
Como se obteve o quantitativo estimado?	☒ Análise de contratações anteriores		☐ Análise de contratações similares.	
	☐ Outros			
Descrição do quantitativo?	O cálculo para chegar no quantitativo ideal obedeceu a seguinte ordem: 1. Necessidade do DETRAN consoante ao alcance administrativo, tecnológico e operacional. Considerando que a expansão de serviço e posterior a rede de serviço, logo houve o cálculo previsto a partir das demandas.			
Especificação	Item	Descrição	Und/Vel.	Qtd
	1	Solução de Telecomunicação Intranet	1	
	2	Solução de Telecomunicação – Sub Redes – Sob Demanda	1	
	3	Solução de Telecomunicação UPGRADE de 100% de Link de Intranet/Internet a partir do 13º Mês – Sob Demanda	1	
	4	Solução de Telecomunicação – Link de Internet Determinístico – DETRAN/PA – Sede	1	
	5	Solução de Telecomunicação Portátil para Acesso Via Satélite	1	
	6	Tabela de Valores de Consumo da Solução de Telecomunicação Portátil e Veicular para Acesso Via Satélite	1	
	7	Composição de Preço para Solução de Telecomunicação Móvel de Fiscalização	1	
	8	Composição de Preço de Instalação e Configuração de Todos os Equipamentos nas Localidades	1	
	9	Composição de Preço para Instalação da Base de Infraestrutura para Solução de Telecomunicação Móvel de Fiscalização	1	
	10	Composição de Preço para Serviços de segurança da informação para a Rede de Telecomunicações nas CIRETRANS, POSTOS AVANÇADOS E POSTOS DE FISCALIZAÇÃO.	1	



GOVERNO DO ESTADO DO PARÁ

Departamento de Trânsito do Estado do Pará

	11	Composição de Preço para Serviços de segurança da informação para a Rede de Telecomunicações para o DETRAN SEDE	1		
	12	Composição de Preço para implantação de Serviços de Gestão da Segurança da Informação para a Rede de Telecomunicações	1		
ESTIMATIVA DO VALOR DA CONTRATAÇÃO					
Meios usados na pesquisa	☐ Painel de preços.	☒ Contratações similares.			
	☐ Simas.	☐ Fornecedores.			
	☐ Internet.	☐ Outros			
de preço	Item	Descrição	Valor Unitário Mensal	Vel/Unid	Valor Total 24 meses
	1	Solução de Telecomunicação Intranet			
	2	Solução de Telecomunicação – Sub Redes – Sob Demanda			
	3	Solução de Telecomunicação UPGRADE de 100% de Link de Intranet/Internet a partir do 13º Mês – Sob Demanda			
	4	Solução de Telecomunicação – Link de Internet – DETRAN/PA – Sede			
	5	Solução de Telecomunicação Portátil para Acesso Via Satélite			
	6	Tabela de Valores de Consumo da Solução de Telecomunicação Portátil e Veicular para Acesso Via Satélite			
	7	Composição de Preço para Solução de Telecomunicação Móvel de Fiscalização			
	8	Composição de Preço de Instalação e Configuração de Todos os Equipamentos nas Localidades			
	9	Composição de Preço para Instalação da Base de Infraestrutura para Solução de Telecomunicação Móvel de Fiscalização.			



GOVERNO DO ESTADO DO PARÁ

Departamento de Trânsito do Estado do Pará

	10	Composição de Preço para Serviços Gerenciados de Cibersegurança para a Rede de Telecomunicações.			
				TOTAL	

JUSTIFICATIVA PARA O PARCELAMENTO DA SOLUÇÃO

A solução será dividida em itens?	☐ Sim.			
	☒ Não.	Por quê ?	☒ Objeto indivisível.	☐ Perda de escala.
			☒ Tecnicamente inviável.	☒ Economicamente inviável.
			☒ Aproveitamento da competitividade.	☐ Outro. Especificar:

CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES

Há contratações correlatas ou interdependentes ?	☐ Sim. ☒ Não.	

ALINHAMENTO DA CONTRATAÇÃO COM O PLANEJAMENTO

Há previsão no plano de contratações anual?	☒ Sim	Especificar item do PCA:
	☐ Não.	Providências: Em razão de atendimento da necessidade da continuidade do serviço público, e ainda para maior economicidade.

RESULTADOS PRETENDIDOS

Quais os benefícios pretendidos na contratação?	☒ Manutenção do Funcionamento Administrativo	☐ Redução de Custos
	☐ Redução dos Riscos do Trabalho	☒ Aproveitamento de Recursos Humanos
	☒ Serviço/Bem de Consumo	☒ Ganho de Eficiência
	☐ Outro.	☐ Realização de Política Pública

PROVIDÊNCIAS PENDENTES

Há providências pendentes para o sucesso da	☐ ☐ Sim.	



GOVERNO DO ESTADO DO PARÁ
Departamento de Trânsito do Estado do Pará

contratação?	☒ Não.	
IMPACTOS AMBIENTAS E MEDIDAS DE MITIGAÇÃO		
Há previsão de impacto ambiental na contratação?	☐ Sim.	
	☒ Não. Em razão de tecnologia com baixa emissão de poluentes.	
CONCLUSÃO		
A contratação possui viabilidade técnica, socioeconômica e ambiental?	☒ Sim. A socioeconômica: A futura contratação está fundamentada e com recurso devido à previsão orçamentária. Viabilidade Técnica: Com viabilidade devido projeto técnico com descritivo detalhado, métodos e procedimentos a serem seguidos para ensejar o projeto. Ambiental: Solução com baixo nível de poluente.	
	☐ Não.	

Belém (PA), de Novembro de 2025.

COMISSÃO DE ESTUDO DE LICITAÇÃO DE TECNOLOGIA
Portaria CGP/DG 2024/



GOVERNO DO ESTADO DO PARÁ
Departamento de Trânsito do Estado do Pará

TERMO DE REFERÊNCIA

PAE nº

1- O QUE SERÁ CONTRATADO?

1.1- OBJETO:

Contratação de empresa especializada na prestação de serviços de telecomunicações e transmissão de dados, através de uma rede de comunicação digital, privativa e independente, com locação de roteadores (Solução UTM/NGFW), no-breaks, switches e firewall, cuja finalidade é a interligação corporativa das redes locais (LAN) das unidades do Departamento de Trânsito do Estado do Pará (CIRETRANS e Postos de Atendimento) e acesso IP (Internet Protocol) a rede mundial de internet centralizada na sede do DETRAN/PA, prestação de serviço de transmissão de dados, voz e imagem via satélite, através de solução portátil, móvel com locação de equipamentos e o fornecimento de toda infraestrutura necessária para a solução móvel de fiscalização, cujas especificações se encontram detalhadas neste Termo de Referência e seus anexos.

Os serviços solicitados se discriminam melhor no quadro abaixo:

Lote	Item	Descrição	Cód. SIMAS	Und	Qtd.	Valor Unitário Estimado Mensal*	Valor Total 24 meses**
I	1	Solução de Telecomunicação Intranet	----	Und.	01	R\$ 2.437.122,85	R\$ 58.490.948,48
	2	Solução de Telecomunicação – Sub Redes – Sob Demanda	----	Und	01	R\$ 1.084.497,20	R\$ 26.027.932,80
	3	Solução de Telecomunicação UPGRADE de 100% de Link de Intranet/Internet a partir do 13º Mês – Sob Demanda	----	Und	01	R\$ 557.111,03	R\$ 13.370.664,80
	4	Solução de Telecomunicação – Link de Internet Determinístico – DETRAN/PA – Sede	----	Und	01	R\$ 846.759,24	R\$ 20.322.221,68
	5	Solução de Telecomunicação Portátil para Acesso Via Satélite	----	Und	01	R\$ 74.866,67	R\$ 1.796.800,00
	6	Tabela de Valores de Consumo da Solução de Telecomunicação Portátil e Veicular para Acesso Via Satélite	----	Und	01	R\$ 261.666,67	R\$ 6.280.000,00
	7	Composição de Preço para Solução de Telecomunicação Móvel de Fiscalização	----	Und	01	R\$ 3.188.957,40	R\$ 76.534.977,60



GOVERNO DO ESTADO DO PARÁ
Departamento de Trânsito do Estado do Pará

	8	Composição de Preço de Instalação e Configuração de Todos os Equipamentos nas Localidades	----	Und	01	R\$ 77.036,89	R\$ 1.848.885,44
	9	Composição de Preço para Instalação da Base de Infraestrutura para Solução de Telecomunicação Móvel de Fiscalização	----	Und	01	R\$ 101.051,39	R\$ 2.425.233,36
	10	Composição de Preço para Serviços de segurança da informação para a Rede de Telecomunicações nas CIRETRANS, POSTOS AVANÇADOS E POSTOS DE FISCALIZAÇÃO		Und	01	R\$ 273.939,36	R\$ 6.574.544,64
	11	Composição de Preço para Serviços de segurança da informação para a Rede de Telecomunicações para o DETRAN SEDE	----	Und	01	R\$ 486.904,00	R\$ 11.685.696,00
	12	Composição de Preço para implantação de Serviços de Gestão da Segurança da Informação para a Rede de Telecomunicações		Und	01	R\$ 1.131.215,00	R\$ 27.149.160,00
						VALOR GLOBAL ESTIMADO**	R\$ 252.507.064,80



GOVERNO DO ESTADO DO PARÁ
Departamento de Trânsito do Estado do Pará

2- JUSTIFICATIVA DA ADOÇÃO DO PREGÃO ELETRÔNICO DO TIPO MENOR PREÇO GLOBAL

2.1-A presente licitação, que trata da prestação dos serviços do objeto deste Termo de Referência e seus anexos, será realizada conforme regulamentação da Lei nº 14.133/2021, na modalidade **PREGÃO ELETRÔNICO do tipo MENOR PREÇO GLOBAL**.

2.2. Adicionalmente, pela Lei Estadual nº 6.474/2000, Lei Complementar Federal nº 123/2006, Lei Complementar Federal nº 147/2014, Lei Estadual nº 8.417/2016, Decreto Estadual nº 878/2006, Decreto Estadual nº 2.734/2022 e Decreto Estadual nº 2.939/2023.

2.3-Os itens deste certame foram agrupados em um único lote devido à sua necessidade de integração e sua interdependência, ou seja, a exigência de compatibilidade entre as partes e gestão integrada das entregas para garantir o seu funcionamento, dado que a sua implementação é bastante ampla com atividades interdependentes.

2.4-Nesta esteira, além da interdependência entre seus módulos, os serviços acessórios devem ser fornecidos por uma única empresa, pois é incoerente no caso desta contratação, que a empresa que forneça a solução e faça sua instalação seja diversa da que prestará o suporte técnico, fornecimento e serviços de manutenções.

2.5-Além disso o agrupamento dos itens em Lote Único é imprescindível, pois em se tratando de gestão contratual através de uma solução integrada torna-se inviável que os serviços como neste caso sejam fornecidos por diferentes fornecedores, dado que traria alta dificuldade de gerenciamento e compartilhamento de responsabilidades, custo de gestão e controle do DETRAN-PA;

2.6-Em se tratando do viés econômico, o parcelamento dos serviços acessórios do objeto pode impactar diretamente os custos da contratação, considerando que a execução desses serviços por uma única empresa se traduz em diluição do custo administrativo e maior economia de escala, possibilitando menor preço global. Isso também porque, o objeto possui características de dependências entre os serviços a serem prestados, sendo certo que seu parcelamento aumentaria os riscos de execução insatisfatória do serviço.

2.7-Em termos técnicos há uma relação direta entre os módulos, serviços prestados e sua vinculação com o licenciamento da solução, sendo certo que os profissionais que trabalhem de forma harmônica e integrada, que conheçam o objeto a ser contratado, para que os serviços acessórios sejam prestados com qualidade e atendendo as necessidades do DETRAN-PA. Deste modo, justifica-se o não fracionamento do objeto licitado, conforme permissivo contido no art. 40, § 2º, I, da Lei n. 14.133/2021.

2.8-Portanto, o lote único atende ao requisito legal já definido por lei, pois só poderá ocorrer parcelamento quando há viabilidade técnica para sua adoção. Nesse diapasão há interesse de natureza técnica na manutenção da unicidade da licitação devido a disponibilidade de sistemas que devem estar interligados, integrados e disponíveis integralmente., pois o fracionamento não atribui a administração pública economicidade, tampouco melhor técnica; mas sim maior custo, possibilidade real de conflito sistêmico. (texto adaptado do Parecer n. 2086/00, elaborado no Processo n.194/2000 do TCDF, da lavra do Professor Fernandes, JORGE ULISSES JACOBY).



GOVERNO DO ESTADO DO PARÁ
Departamento de Trânsito do Estado do Pará

2.9-Cabe ressaltar que a experiência demonstra que a utilização de lote único, com isso, a gestão contratual decorre de mais celeridade em pronta resposta quando há demanda e “partilhar” o lote teríamos dificuldade na entrega e poderia ainda ter fornecedores diversos, que em consequência prestação com dificuldade e por conseguinte, problemas na totalidade.

2.10. As regras e condições deste processo de contratação estão devidamente explicitadas neste Termo de Referência e nos seus anexos que são parte integrante deste processo:

- a) Anexo I – ESPECIFICAÇÕES TÉCNICAS
- b) Anexo II – CONDIÇÕES GERAIS.
- c) Anexo III - TOPOLOGIA.
- d) Anexo IV – SOLUÇÃO DE TELECOMUNICAÇÃO – CARACTERÍSTICAS DO CIRCUITO
- e) Anexo V – PLANILHAS DE PREÇOS DE REFERÊNCIA
- f) Anexo VI – MODELO DE PROPOSTA
- g) Anexo VII – PROVA DE CONCEITO
- h) ANEXO VIII – DECLARAÇÃO DE SUPERVENIÊNCIA
- i) ANEXO IX – DECLARAÇÃO DE MENOR
- j) ANEXO X – MODELO DE ATESTADO DE VISITA TÉCNICA
- k) ANEXO XI – ENDEREÇOS DAS LOCALIDADES PARA INSTALAÇÃO DOS LINKS
- l) ANEXO XII – DECLARAÇÃO PARA MICROEMPRESA E EMPRESA DE PEQUENO PORTE
- m) ANEXO XIII – DECLARAÇÃO DE COTA DE PESSOAS COM DEFICIÊNCIA NO QUADRO DE EMPREGADOS

3- DA PARTICIPAÇÃO DE EMPRESAS EM CONSÓRCIO

3.1. Da permissão de participação de consórcios.

3.2. Será permitido a participação de consórcio nos termos do art. 15 da Lei 14.133/2021, respeitando as condições previstas em Lei:

“Art. 15. Salvo vedação devidamente justificada no processo licitatório, pessoa jurídica poderá participar de licitação em consórcio, observadas as seguintes normas:”

3.3. Quando o objeto a ser licitado envolve questões de alta complexidade, via de regra, a Administração, com intuito de aumentar o número de participantes, admite a formação de consórcio. O que no contexto em análise, essa hipótese se aplica, pois, o objeto pretendido, a contratação de empresa especializada na prestação de serviços de telecomunicações e transmissão de dados, através de uma rede de comunicação digital, determinística, privativa e independente, com locação de roteadores (Solução UTM/NGFW), no-breaks, switches e firewall, cuja finalidade é a interligação corporativa das redes locais (LAN) das unidades do Departamento de Trânsito do Estado do Pará (CIRETRANS e Postos de Atendimento) e acesso IP (Internet



GOVERNO DO ESTADO DO PARÁ
Departamento de Trânsito do Estado do Pará

Protocol) a rede mundial de internet centralizada na sede do DETRAN/PA, prestação de serviço de transmissão de dados, voz e imagem via satélite, através de solução portátil, móvel com locação de equipamentos e o fornecimento de toda infraestrutura necessária para a solução móvel de fiscalização, incluindo equipamentos, encontra-se consolidada no mercado e no âmbito da Administração Pública, vez que são serviços prestados por diversas empresas atualmente.

3.4. Destaca-se que a participação de consórcios em processos licitatórios com esse objeto, visa garantir o aumento de competitividade, podendo trazer um melhor preço para à Administração Pública e uma maior sustentação dos serviços.

3.5. Neste modelo de serviço, o atendimento das demandas, deve ser estabelecido de forma estruturada e padronizada, de maneira a evitar os riscos operacionais, motivo pelos quais se optou pela permissão de participação de consórcio.

3.6. Em relação ao escopo do objeto, é possível a ampla participação de empresas atuantes no mercado, que de forma isolada ou em consórcio, consigam atender às condições e os requisitos de habilitação previstos neste documento.

3.7. O DETRAN/PA espera como resultado deste processo, contar com fornecedor único ou um consórcio para o processo de atendimento às demandas, com ampla experiência na execução de atividades operacionais e gerenciais de atendimento, suportadas por ferramentas e processos adequados e aderentes às necessidades da Diretoria de tecnologia da Informação e Diretoria Operacional, integrada a diversas áreas gestoras do Órgão, facilitando assim o processo de integração de dados e informações vitais ao desenvolvimento das atividades do DETRAN/PA.



GOVERNO DO ESTADO DO PARÁ
Departamento de Trânsito do Estado do Pará

4- DESCRIÇÃO DA SOLUÇÃO

QUAL O MOTIVO DA CONTRATAÇÃO ?

A presente contratação de serviços de comunicação **é fundamental** para a **interconexão integral e contínua** de todas as unidades descentralizadas do Departamento de Trânsito do Estado do Pará (DETRAN/PA), abrangendo as **Circunscrições Regionais de Trânsito (CIRETRANS)**, **postos fixos e móveis de atendimento**, a **infraestrutura de fiscalização de trânsito** e as **ações itinerantes**, com a **Sede administrativa**.

Essa interligação estabelece uma **rede de dados privativa e segura**, essencial para o **controle rigoroso e a gestão eficiente** de todas as informações trafegadas. A exclusividade dessa rede é o **único meio** de garantir o **acesso restrito e autorizado** aos **sistemas finalísticos e de apoio** do DETRAN/PA, bem como à **Base Nacional de Condutores e Veículos do SENATRAN**. Tal medida é **condição sine qua non** para preservar a **confidencialidade, integridade e disponibilidade** dos dados de condutores e veículos, alinhada às políticas de segurança e eficiência.

Necessidades Detalhadas e Abrangência Territorial

A necessidade primordial reside em assegurar que **quaisquer atividades e serviços** prestados pelo DETRAN/PA possam ser realizados **a todo tempo e em qualquer localidade** dentro do vasto território geográfico do Pará, seguindo um **padrão único e regras consistentes** de política de segurança.

- **Alcance Irrestrito:** O serviço de comunicação deve garantir a conectividade **independentemente da localização** das unidades (CIRETRANS, Postos de Serviços, ações itinerantes e infraestrutura de fiscalização), cobrindo a **extensão total do território paraense**.
- **Expansão da Presença Institucional:** É de vital importância ampliar a **cobertura e a presença** do DETRAN/PA, sobretudo nas **regiões de fronteira** com os estados do Maranhão, Tocantins e Mato Grosso. Essa estratégia visa **evitar o deslocamento** de cidadãos paraenses em busca de serviços em DETRANS de outros estados, suprimindo a ausência de atendimento e oferecendo uma **solução de proximidade** ao cliente.

Impacto Econômico e Sustentação da Receita Estadual

O serviço de comunicação é **indispensável** para a **implementação de soluções tecnológicas avançadas** em um estado de grande dimensão geográfica, com impactos diretos e significativos na esfera econômica:

- **Aumento da Arrecadação:** A modernização e a capilaridade dos serviços possibilitarão o **crescimento progressivo e sustentável** na arrecadação de **tributos, taxas e impostos**. O DETRAN/PA é uma das **principais fontes de receita** para:
 - A **SEFA (Secretaria de Estado da Fazenda)**, no que tange ao **Imposto sobre a Propriedade de Veículos Automotores (IPVA)**.
 - Os **Municípios**, por meio de receitas provenientes de **licenciamentos e multas**.



GOVERNO DO ESTADO DO PARÁ

Departamento de Trânsito do Estado do Pará

- O **BANPARÁ**, em razão da movimentação de **serviços bancários específicos** vinculados ao órgão.
- **Sustentação da Receita:** A continuidade e a eficiência dos serviços de comunicação são, portanto, de **caráter essencial** para a **sustentação e estabilidade da receita estadual**.

Imperativo da Digitalização e Continuidade do Serviço Público

Em um cenário global cada vez mais **digitalizado**, os serviços essenciais do DETRAN/PA – como a **transferência de propriedade**, a emissão do **Certificado de Registro e Licenciamento de Veículo (CRLV)** e da **Carteira Nacional de Habilitação (CNH)** – são integralmente digitais.

Neste diapasão, a **continuidade e a robustez** dos serviços de comunicação são uma **condicionante inegociável** para o **atendimento eficaz do anseio público**, garantindo a modernização e a acessibilidade do serviço estatal de trânsito.

5-NATUREZA DOS SERVIÇOS

☒ Prestação de Serviços Comum de natureza **continuada**.

☐ Especial.

6-PROVA DE QUALIDADE, RENDIMENTO, DURABILIDADE E SEGURANÇA DO SERVIÇOS

Haverá prova de qualidade?

☒ Sim.

JUSTIFICATIVA TÉCNICA E LEGAL PARA A EXIGÊNCIA DE PROVA DE CONCEITO (POC)

1. DA PREVISÃO LEGAL E NECESSIDADE Em conformidade com o **Art. 17, §3º da Lei nº 14.133/2021**, a exigência de Prova de Conceito (PoC) neste certame justifica-se pelo **detalhamento** do objeto licitado, que integra serviços de telecomunicações críticas em áreas remotas da Amazônia com logística especializada de transporte pesado. A mera análise documental (propostas de papel) é insuficiente para comprovar a real capacidade de entrega dos níveis de serviço (SLA) exigidos para a fiscalização de trânsito e segurança pública.

2. DA MITIGAÇÃO DE RISCOS DE INEXECUÇÃO CONTRATUAL O histórico de contratações de serviços de conectividade no Estado do Pará demonstra que soluções teóricas muitas vezes falham ao enfrentar a realidade geográfica da região (latência, instabilidade, "zonas de sombra"). A PoC visa mitigar o risco de contratação de empresa que, embora apresente atestados, não possua tecnologia capaz de operar com **latência inferior a 90ms em localidades críticas** (como São Félix do Xingu) ou **inferior a 5ms na região metropolitana**. A falha neste requisito inviabiliza o acesso aos sistemas



GOVERNO DO ESTADO DO PARÁ

Departamento de Trânsito do Estado do Pará

	RENAVAM/RENACH, paralisando as operações do DETRAN. Portanto, a PoC atua como filtro de exequibilidade técnica, protegendo a Administração Pública de contratos ineficazes. 3. DA COMPLEXIDADE LOGÍSTICA E SEGURANÇA OPERACIONAL (ITEM 1.3) A exigência de demonstração prática da capacidade de movimentação de contêineres de 12 metros com equipamento do tipo <i>Munck</i> de alta capacidade mínima (lança de 15m/10ton). Trata-se de uma manobra de alto risco e especificidade técnica. A justificativa para testar este item, exigindo equipamentos próprios, baseia-se na necessidade de pronto atendimento (disponibilidade imediata de 12 horas) para movimentação das bases móveis de fiscalização. A dependência de locação ou subcontratação no mercado spot para equipamentos tão específicos colocaria em risco a continuidade das operações de fiscalização do Estado. A PoC visa assegurar que a licitante detém o domínio operacional e o ativo necessário para realizar a manobra com segurança, evitando acidentes e paralisações. 4. DA NECESSIDADE DE TESTES EM AMBIENTE REAL (FIELD TEST) Diferente
	de softwares ou equipamentos de prateleira, a solução de conectividade via satélite "on-the-move" (veicular) e estacionária (portátil) depende de variáveis físicas incontornáveis (relevo, interferência climática, visada de satélite). A exigência de testes em locais distintos (Região Metropolitana e Interior do Estado) é proporcional à necessidade de garantir que o sistema de fiscalização funcione tanto na capital quanto nas fronteiras do estado, onde a presença do Estado é mais necessária e a infraestrutura é precária. A simulação em laboratório não reproduziria as adversidades que os agentes de trânsito enfrentam em campo. 5. DA ADERÊNCIA AOS PRINCÍPIOS DA EFICIÊNCIA E ISONOMIA A PoC será aplicada apenas ao licitante provisoriamente vencedor, não gerando custos aos demais participantes, preservando a competitividade. Os critérios estabelecidos no Anexo VII são objetivos (métricas de latência, sucesso na manobra de carga, funcionamento de links), mensuráveis e binários (Aprovado/Reprovado), eliminando a subjetividade do julgamento e garantindo a isonomia. CONCLUSÃO A realização da Prova de Conceito é, portanto, medida de prudência administrativa, essencial para garantir que a solução entregue seja aderente às especificações vitais do DETRAN/PA, assegurando a continuidade do serviço público de fiscalização de trânsito e evitando prejuízos ao erário decorrentes de rescisões contratuais por deficiência técnica superveniente.



GOVERNO DO ESTADO DO PARÁ

Departamento de Trânsito do Estado do Pará

O edital exigirá amostra?	☒ não	Justificativa:
Haverá garantia do serviços?	☒ Sim. Justificativa: A empresa deverá promover a garantia e o atendimento de serviço de qualquer eventualidade, poderá realizar a troca de equipamento, garantir a continuidade de software e/ou afins.	
Haverá assistência técnica?	☒ Sim. Justificativa: A manutenção continuada para melhoria de funcionalidades e serviço de suporte técnico.	

7-CRITÉRIOS DE SELEÇÃO

Forma de contratação	☐ Inexigibilidade de licitação, com fundamento no art. 74, Y, da Lei Federal nº 14.133/21.	
	☐ Dispensa de licitação em razão do valor*, com fundamento no art. 75, II, da Lei Federal nº 14.133/21. * Nesta hipótese, deve-se utilizar preferencialmente a dispensa eletrônica.	
	☐ Dispensa de licitação, com fundamento no art. 75, VIII, da Lei Federal nº 14.133/21.	
	☒ Pregão eletrônico	
Critério de Julgamento	☒ Menor preço.	
	☐ Maior desconto.	
O orçamento estimado é sigiloso?	☐ Sim.	
	☒ Não.	
Critério para a proposta ser aceita	A proposta deve observar os valores unitários e global máximos aceitáveis conforme planilha de composição de preços do orçamento estimado, para fins de aceitação da proposta ora praticado no mercado.	
Há itens com participação exclusiva para microempresas e empresa de pequeno porte?	☐ Sim. ☒ Não.	

8-REQUISITOS DA CONTRATADA



GOVERNO DO ESTADO DO PARÁ

Departamento de Trânsito do Estado do Pará

Será exigida habilitação técnica?	☒ Sim.	Qual?	Será exigido padrões de qualidade, experiência, certificações entre outras obrigаторiedades para aferir se a empresa possui capacidade técnica compatível com a contratação. Conforme Anexo I do presente TR
Qualificações técnicas exigidas	☒ Declaração de ciência das informações necessárias para o cumprimento da futura obrigação contratual.		A empresa deverá apresentar DECLARAÇÃO de que possui equipe técnica para a execução dos serviços a serem contratados.
	☒ Registro na entidade profissional competente		Licença SCM (serviço de comunicação multimídia) expedido pela ANATEL e que se encontre na Condição de válida, com autorização para prestação dos serviços dentro do território do estado do Pará ou dentro de todo o Território brasileiro, podendo a comprovação ser feita através de consulta no site da Anatel ou através da apresentação do termo SCM pela empresa licitante.
	☐ Indicação de pessoal técnico, instalações e aparelhamento para o cumprimento da futura obrigação contratual com a comprovação de qualificação técnica de cada membro da equipe técnica responsável pela execução dos trabalhos.		
	☒ Outro previsto em lei especial		A empresa deverá apresentar comprovação de aptidão para o fornecimento dos bens e serviços ora contratados, por meio de Atestado de Capacidade Técnica, emitido por entidade Pública ou Privada no qual comprove o fornecimento de materiais e a execução de serviços compatíveis e pertinentes em características, quantidades e prazos.
	☐ Não será exigida prova de		



GOVERNO DO ESTADO DO PARÁ

Departamento de Trânsito do Estado do Pará

	qualificação técnica em razão da baixa complexidade da contratação.	
Há critério de sustentabilidade?	☒ Sim.	Justificativa: O material de hardware não pode ser descartado, quando ocorrer a troca durante troca normal por uso, em local comum, deve ser inutilizado em lixo próprio de tecnologia e não ir a natureza ou lixo comum.
Há riscos a serem assumidos pela contratada?	☒ Sim.	Justificativa: De manter a continuidade dos serviços por tempo determinado ao contrato e mantendo a mesma prestação sem alteração da proposta original, exceto quando haja aceite entre as partes.
9-FORMA DA PRESTAÇÃO DOS SERVIÇOS		
Como o serviço será prestado?	☒ O serviço terá início imediato a partir da emissão de ordem de serviço pela administração .	
Local e hora da prestação dos serviços	Os serviços devem ser prestados nos endereços indicados pelo DETRAN, conforme dias, horários e locais. Conforme relação de CIRETRANS constante do Anexo do presente Termo de Referência.	
10-PRAZO, FORMA DE PAGAMENTO E GARANTIA DO CONTRATO		
Prazo do contrato	☐ 30 dias (pronta entrega).	
	☒ 24 (vinte e quatro) meses.	
Haverá possibilidade de prorrogação?	☒ Sim, observado os critérios e prazos máximos dispostos na Lei Federal nº 14.133/21.	
	☐ Não.	



GOVERNO DO ESTADO DO PARÁ
Departamento de Trânsito do Estado do Pará

Forma de pagamento	Meio	Ordem bancária.
	Onde?	Conta corrente da contratada no Banco do Estado do Pará.
	Qual o prazo?	Até 30 dias corridos, a contar do recebimento da nota fiscal (ou fatura) com o comprovante de regularidade fiscal da contratada.
	Prova da regularidade e fiscal	A regularidade fiscal pode ser provada: 1. Por consulta ao SICAF ou Cadastramento Unificado de Licitante. ou 2. Pela apresentação dos documentos constantes no art. 68 da Lei Federal nº 14.133/21, quando não for possível consulta aos sistemas oficiais.
Qual a garantia do contrato?	☒ 1% do valor inicial do contrato.	Justificativa: Comprovar de que o vencedor do certame assegure que possui capacidade de cumprir as condições, custos e prazos assumidos na assinatura do contrato. Ademais, em razão da relevância da prestação contínua do objeto a garantia objetiva cobrir eventuais prejuízos causados à administração, em decorrência de descumprimento de prazos e/ou inexecução contratual.
11-PREVISÃO ORÇAMENTÁRIA		
Dados orçamentários da contratação	Os dados orçamentários serão informados pela área competente, por meio do atestado de disponibilidade orçamentária, a ser posteriormente juntado aos autos.	

Belém (PA), de abril de 2025.

COMISSÃO DE ESTUDO DE LICITAÇÃO DE TECNOLOGIA

Portaria CGP/DG 2024/



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

ANEXO I DO TERMO DE REFERÊNCIA

ESPECIFICAÇÕES TÉCNICAS

1. INTRODUÇÃO

Este documento constitui peça integrante e inseparável do respectivo procedimento licitatório e tem por objetivo definir de forma expressa, as especificações, os serviços, os prazos de execução, quantidades, justificativas, os procedimentos de entrega, recebimento e pagamento do objeto, dentre outros, de forma a subsidiar os interessados na participação do certame licitatório, orientando-os na preparação e na elaboração de suas propostas, a fim de permitir a contratação do objeto deste Edital.

2. OBJETO

Contratação de empresa especializada na prestação de serviços de telecomunicações e transmissão de dados, através de uma rede de comunicação digital, privativa e independente, com locação de equipamentos, roteadores, no-breaks, switches e firewall, cuja finalidade é a interligação corporativa das redes locais (LAN) das unidades do Departamento de Trânsito do Estado do Pará (CIRETRANS e Postos de Atendimento) e acesso IP (Internet Protocol) a rede mundial de internet centralizada na sede do DETRAN/PA, prestação de serviço de transmissão de dados, voz e imagem via satélite, através de solução portátil, móvel com locação de equipamentos e o fornecimento de toda infraestrutura necessária para a solução móvel de fiscalização, cujas especificações se encontram detalhadas neste Termo de Referência e seus anexos.

3. OBJETIVO

A presente contratação de serviços de comunicação **é fundamental** para a **interconexão integral e contínua** de todas as unidades descentralizadas do Departamento de Trânsito do Estado do Pará (**DETRAN/PA**), abrangendo as **Circunscrições Regionais de Trânsito (CIRETRANS)**, **postos fixos e móveis de atendimento**, a **infraestrutura de fiscalização de trânsito** e as **ações itinerantes**, com a **Sede administrativa**.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Essa interligação estabelece uma **rede de dados privativa e segura**, essencial para o **controle rigoroso e a gestão eficiente** de todas as informações trafegadas. A exclusividade dessa rede é o **único meio** de garantir o **acesso restrito e autorizado** aos **sistemas finalísticos e de apoio** do DETRAN/PA, bem como à **Base Nacional de Condutores e Veículos do SENATRAN**. Tal medida é **condição sine qua non** para preservar a **confidencialidade, integridade e disponibilidade** dos dados de condutores e veículos, alinhada às políticas de segurança e eficiência.

Necessidades Detalhadas e Abrangência Territorial

A necessidade primordial reside em assegurar que **quaisquer atividades e serviços** prestados pelo DETRAN/PA possam ser realizados **a todo tempo e em qualquer localidade** dentro do vasto território geográfico do Pará, seguindo um **padrão único e regras consistentes** de política de segurança.

- **Alcance Irrestrito:** O serviço de comunicação deve garantir a conectividade **independentemente da localização** das unidades (CIRETRANS, Postos de Serviços, ações itinerantes e infraestrutura de fiscalização), cobrindo a **extensão total do território paraense**.
- **Expansão da Presença Institucional:** É de vital importância ampliar a **cobertura e a presença** do DETRAN/PA, sobretudo nas **regiões de fronteira** com os estados do Maranhão, Tocantins e Mato Grosso. Essa estratégia visa **evitar o deslocamento** de cidadãos paraenses em busca de serviços em DETRANS de outros estados, suprimindo a ausência de atendimento e oferecendo uma **solução de proximidade** ao cliente.

Impacto Econômico e Sustentação da Receita Estadual

O serviço de comunicação é **indispensável** para a **implementação de soluções tecnológicas avançadas** em um estado de grande dimensão geográfica, com impactos diretos e significativos na esfera econômica:

- **Aumento da Arrecadação:** A modernização e a capilaridade dos serviços possibilitarão o **crescimento progressivo e sustentável** na arrecadação de **tributos, taxas e impostos**. O DETRAN/PA é uma das **principais fontes de receita** para:
 - A **SEFA (Secretaria de Estado da Fazenda)**, no que tange ao **Imposto sobre a Propriedade de Veículos Automotores (IPVA)**.
 - Os **Municípios**, por meio de receitas provenientes de **licenciamentos e multas**.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- O **BANPARÁ**, em razão da movimentação de **serviços bancários específicos** vinculados ao órgão.
- **Sustentação da Receita:** A continuidade e a eficiência dos serviços de comunicação são, portanto, de **caráter essencial** para a **sustentação e estabilidade da receita estadual**.

Imperativo da Digitalização e Continuidade do Serviço Público

Em um cenário global cada vez mais **digitalizado**, os serviços essenciais do DETRAN/PA – como a **transferência de propriedade**, a emissão do **Certificado de Registro e Licenciamento de Veículo (CRLV)** e da **Carteira Nacional de Habilitação (CNH)** – são integralmente digitais.

Neste diapasão, a **continuidade e a robustez** dos serviços de comunicação são uma **condicionante inegociável** para o **atendimento eficaz do anseio público**, garantindo a modernização e a acessibilidade do serviço estatal de trânsito.

4. DA JUSTIFICATIVA / FUNDAMENTAÇÃO LEGAL / CONSIDERAÇÃO

4.1. Da Justificativa Técnica com base nas seguintes considerações:

- a) O serviço de telecomunicação é de natureza contínua, serviço de extrema necessidade e vital para o funcionamento de todos os sistemas finalísticos desta autarquia. Os serviços prestados de forma contínua são aqueles que, pela sua essencialidade, visam atender à necessidade pública de forma permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público ou o funcionamento das atividades finalísticas do órgão ou entidade, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional.
- b) A interligação, conforme ANEXO III -Topologia, todas as CIRETRANS, Postos de Serviços, unidades móveis de fiscalizações com a SEDE, possibilitando que os serviços prestados por esta autarquia cheguem a todos os cidadãos que são atendidos no território geográfico do estado do Pará.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- c) A partir do levantamento de demanda de capacidade e disponibilidade de banda de transmissão e recebimento de dados de todos os pontos remotos praticados atualmente nas CIRETRANS e POSTOS DE SERVIÇOS, interligados com o DETRAN/PA-SEDE, constatou-se:
- A necessidade de incremento de banda (aumento na disponibilidade de download/upload) em cada localidade.
 - A quantidade de acesso portátil e móvel via satélite que atendam às necessidades dos serviços de fiscalização e atendimento itinerante realizadas pelo DETRAN-PA dentro do extenso território geográfico do estado do Pará, incluindo os seus 144 (cento e quarenta e quatro) municípios.
 - A necessidade de incremento na quantidade e atualização tecnológica de solução móvel de postos de fiscalização utilizados atualmente para atender as demandas de atendimento Itinerantes da CNCIR (Coordenadoria do Núcleo da Circunscrições de Trânsito) e de fiscalização da DTO (Diretoria Técnica Operacional) para o maior controle na fiscalização e apoio dos condutores e seus veículos que trafegam nas estradas e rodovias do estado do Pará, que estão sob a jurisdição do DETRAN-PA.

4.2. Da Justificativa da prestação dos serviços de forma global:

A presente licitação, na modalidade Pregão, na forma Eletrônica, tem por objeto, eventual contratação de empresa especializada na prestação de serviços de telecomunicações e transmissão de dados, através de uma rede de comunicação digital, privativa e independente, com locação de roteadores (Solução UTM/NGFW), nobreaks, switches e firewall, cuja finalidade é a interligação corporativa das redes locais (LAN) das unidades do Departamento de Trânsito do Estado do Pará (CIRETRANS e Postos de Atendimento) e acesso IP (Internet Protocol) a rede mundial de internet centralizada na sede do DETRAN/PA, e prestação de serviço de transmissão de dados, voz e imagem via satélite, através de solução portátil e móvel, com locação de equipamentos e o fornecimento de toda infraestrutura



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

necessária para a solução móvel de fiscalização, cujas especificações se encontram detalhadas neste documento e seus ANEXOS, bem como todas as regras descritas neste edital.

1. Diante das expectativas foi verificada a possibilidade de realizar o fracionamento do objeto para fornecimento dos serviços em tela na sede do DETRAN-PA, porém, essa hipótese foi desconsiderada, em razão das evidências abaixo relacionadas:
 - Para o fracionamento seria necessária a abertura de diversos processos de licitação, implicando em custo administrativo, riscos de atrasos decorrentes de recursos, impugnações e outros eventos que podem levar ao retardamento da execução do objeto como um todo;
 - O aumento da complexidade de gerenciamento de diversos fornecedores na execução do projeto, o que demandaria riscos maiores para a conclusão da solução;
 - Por ser um serviço especializado em que a inter-relação harmoniosa de todos os elementos é condição fundamental para a obtenção de uma solução com a qualidade e nível de disponibilidade do ambiente que envolvem os objetos requeridos para o projeto;
 - O aumento da complexidade e dos custos individuais para gestão de todo o ambiente de operação que envolvem equipamentos, softwares, infraestrutura, logística e pessoal, demandaria o controle e acionamento de diversos fornecedores para suporte e manutenção de todos os elementos, ou seja, seria impossível definir as responsabilidades no apontamento de um sinistro, falha operacional do sistema, atraso na execução de rotinas por falta de sincronismo entre os fornecedores, a não compatibilidade de um único componente dentro da cadeia operacional necessária a prestação do serviço e etc.;

Portanto, fica evidenciado que o fracionamento do objeto, não representaria vantagens técnicas ou financeiras relevantes a esta autarquia, ao contrário, por se tratar de um serviço específico de complexa viabilidade técnica, a cisão do objeto, poderia inviabilizar a implementação do serviço de Telecomunicação, com



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

um aumento significativo de custo e dos riscos para a sua consecução.

Desta forma, entende-se que o não fracionamento do objeto é o mais adequado para essa contratação.

2. A prestação dos serviços deverá se processar através de um único fornecedor, cabendo a empresa fornecedora viabilizar tudo o que está sendo exigido neste documento e seus ANEXOS, bem como e as regras e diretrizes descritas neste edital.
3. Concluindo, para atender os requisitos da necessidade do DETRAN/PA relativo ao serviço de Solução de Telecomunicação, para a prestação do serviço, o fornecedor deverá efetuar investimento de grande monta, complexa administração operacional, grande volume de mobilizados e de pessoal especializado, bem como soluções tecnológicas específicas para o objeto, envolver atendimento em todo o estado do Pará, que possui um extenso território e complexidade geográfica entre outros e em razão dessas peculiaridades é que reiteramos a contratação unificada de fornecimento.

4.3. Da Fundamentação Legal:

- a) A contratação em tela, objeto desta especificação técnica tem amparo legal na Lei Federal nº. 14.133/2021 e suas alterações, e demais normas contidas neste documento.
- b) Estas Especificações Técnicas foram elaboradas de acordo com o Ordenamento Jurídico Nacional que regulamenta o processo de aquisições e contratações para a Administração Pública: Lei Federal nº. 14.133/2021, que constitui peça integrante, indispensável e inseparável do processo licitatório, visando viabilizar a contratação dos serviços descritos neste documento e seus anexos.
- c) Deste modo, o presente documento contém os elementos básicos e essenciais determinados pela legislação, descritos de forma a subsidiar os interessados em participarem do certame licitatório na preparação da documentação e na elaboração da proposta.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

4.4. Das Considerações:

- a) Os órgãos e entidades que integram o Poder Executivo demandam recursos humanos, financeiros e materiais indispensáveis ao cumprimento de suas finalidades institucionais. No que tange aos recursos materiais, destacam-se os bens físicos e os serviços especializados de suporte que, de forma integrada, viabilizam a continuidade das atividades administrativas.
- b) Nesse contexto, a presente licitação, a ser realizada por meio de **Pregão Eletrônico**, visa à contratação de pessoa jurídica especializada na prestação de **serviço de solução de telecomunicação** para atender às necessidades imediatas e contínuas do **DETRAN/PA**.
- c) O modelo de contratação adotado alinha-se às melhores práticas da administração pública moderna ao consolidar o fornecimento de insumos e a prestação de serviços em um fluxo único e coordenado. Tal estratégia garante que a infraestrutura de telecomunicações — insumo crítico e imprescindível às operações do órgão — não sofra descontinuidade por avarias técnicas ou falhas de integração, assegurando a eficiência operacional e o pleno atendimento ao interesse público.
- d) Será permitido a participação de consórcio nos termos do art. 15 da Lei 14.133/2021, respeitando as condições previstas em Lei.
- e) O critério de julgamento adotado será o Menor Preço Global do Lote Único. Logo, para fins de classificação das propostas, será considerado o Menor Valor Global do Lote que configuram a Planilha de Formação de Preços conforme o Termo de Referência.
- f) O DETRAN/PA espera como resultado deste processo, contar com fornecedor único ou um consórcio para o processo de atendimento às demandas, com ampla experiência na execução de atividades operacionais e gerenciais de atendimento, suportadas por ferramentas e processos adequados e aderentes às necessidades da Diretoria de tecnologia da Informação, integrada a diversas áreas gestoras do Órgão,



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

facilitando assim o processo de integração de dados e informações vitais ao desenvolvimento das atividades do DETRAN/PA.

- g) Neste modelo de serviço, o atendimento das demandas, deve ser estabelecido de forma estruturada e padronizada, de maneira a evitar os riscos operacionais, motivo pelos quais se optou pela permissão da participação de consórcio.

5. REQUISITOS BÁSICOS DA SOLUÇÃO DE TELECOMUNICAÇÕES PARA A REDE DE COMUNICAÇÃO DIGITAL, PRIVATIVA E INDEPENDENTE.

5.1. A CONTRATADA deve fornecer uma infraestrutura de Rede de Comunicação Digital (backbone), utilizando circuitos privativos, **ponto-a-ponto ou ponto-multiponto**, interligando a CONTRATANTE aos seus diversos clientes no Estado do Pará, conforme **Anexo III -Topologia**.

5.2. No site central da rede (CONTRATANTE - ponta A) a CONTRATADA deve disponibilizar acesso local via enlace de alta velocidade através de fibra óptica em rotas alternativas e redundantes, instaladas fisicamente em equipamento ROUTER / SWITCH METRO, utilizando equipamentos de comunicação de rede e segurança capazes de suportarem fail-over e load balance, garantindo assim, a continuidade da prestação do serviço em caso de interrupção em um dos segmentos do acesso, e em quantidade compatível às necessidades dos enlaces atendidos, devendo a rede operar obrigatoriamente sob a tecnologia/protocolo MPLS (Multiprotocol Label Switching).

5.3. Todos os serviços relativos à especificação, ao projeto, à configuração, à instalação, à operação e à manutenção da estrutura de Rede de Comunicação Digital até a interface que permita integração com os sites, central e remoto, serão de responsabilidade da CONTRATADA.

5.4. A Rede de Comunicação Digital deve ter garantia de desempenho, privacidade e suporte a diversos protocolos, além de permitir a utilização de endereçamento IP privativo.

5.5. A CONTRATADA deve disponibilizar toda a infraestrutura necessária (Ponta A, Ponta B e sub rede) de hardware e software para atender às necessidades no transporte de dados.

5.6. Os acessos concentradores redundantes e com rota alternativa da Ponta A (site



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

central), bem como o Acesso IP a Internet, devem obrigatoriamente ser atendidos por fibra óptica.

5.7. As SUB REDES atenderão qualquer ponto dentro do raio de até 15 quilômetros, a partir de qualquer CIRETRAN, conforme o **ANEXO VI**, Tabela 2, onde as SUB REDES deverão possuir as seguintes características técnicas e operacionais:

1. Deverão ser do tipo ponto a ponto a partir de uma CIRETRAN e o site num raio de até 15 quilômetros a partir da CIRETRAN;
2. Deverá possuir throughput 100% simétrico de download e upload, com velocidade mínima de 20Mbps.
3. Deverá ser implementado com uso de cabo de fibra ótica.
4. Deverá possuir capacidade de compartilhar em até 90% dos circuitos de intranet/internet entre a CIRETRAN com a SEDE DE DETRAN/PA, onde o critério do percentual de compartilhamento será definido, único e exclusivamente, pelo DETRAN/PA, sendo que o incremento do percentual de compartilhamento deverá ser de uma casa decimal, exemplo: 1%, 2%, etc.
5. Deverão ser instalados no site da SUB REDE, todos os equipamentos necessários,, conforme item 7.2 e ANEXO V, Planilha 5.
6. O serviço de instalação e configuração, por site, será conforme o ANEXO VI, Tabela 9.

Os links para as SUB REDES do Interior do Estado, serão implementadas sob demanda, a partir das CIRETRANS, ou seja, os links das CIRETRANS (municípios do ANEXO VI, Tabela 2) serão estendidos para as localidades (SUB REDES) indicadas pela CONTRATANTE, **até a uma distância de 15 quilômetros.**

6. CARACTERÍSTICAS TÉCNICAS PARA A REDE DE COMUNICAÇÃO DIGITAL PRIVATIVA E INDEPENDENTE

6.1. DA DISPONIBILIDADE

6.1.1. Os serviços deverão ser providos por uma infraestrutura de Rede de Comunicação



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Digital privativa, composta de todas as funcionalidades necessárias ao bom funcionamento desta Rede, além de oferecerem garantias nos requisitos de alta qualidade, de desempenho, de confiabilidade, de sigilo e de disponibilidade proporcionado pela comunicação digital fim-a-fim.

6.1.2. A CONTRATADA deve fornecer soluções escaláveis, possibilitando alterações nas bandas de transmissão e configurações.

6.1.3. A qualquer momento poderão ser efetuadas alterações na localização geográfica (endereço), velocidade ou criticidade nos sites central e remoto.

6.2. GERÊNCIA DE CIRCUITOS

6.2.1. A infraestrutura lógica, tais como: arquivos de atualização, nome de usuário e senha de comunidades SNMP (Simple Network Management Protocol), devem ser compartilhados para leitura (acesso completo), com o objetivo de se realizar o gerenciamento e análise dos circuitos nos sites central e remoto por parte da CONTRATANTE.

6.2.2 A CONTRATANTE após a assinatura do contrato deverá fornecer os valores dos alarmes de seus equipamentos CONTRATADA, para que sejam configurados no software de monitoramento e auditoria. Entendem-se como alarmes todos os valores de referência relevantes para a análise dos objetos gerenciados.

6.2.3 A CONTRATADA deverá disponibilizar à CONTRATANTE software de monitoramento e auditoria de link que permita consultas, emissão e visualização de relatórios na própria internet, por intermédio de navegador web, com informações referentes aos estados dos equipamentos (up/down), falhas na rede, tráfego no circuito, disponibilidade no período, alarmes e eventos, tendências e desvios de comportamentos, todos referentes à rede da CONTRATADA, com atraso máximo de 10 minutos para a atualização. Esses dados deverão ficar disponíveis para acesso por um período mínimo de 12 (doze) meses tanto para consulta online, como download e ou impressão dos mesmos pela CONTRATANTE.

6.2.3.1 O software de monitoramento e auditoria deverá suportar Multilocal com o uso de sondas remotas (remote probes), podendo monitorar redes locais inteiras em filiais ou datacenters diferentes e centralizar todos os alertas e dados na matriz.

6.2.3.2 Deverá permitir criar Dashboards "painéis" personalizáveis de diagramas visuais e



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

mapas em tempo real com a opção de arrastar e soltar, facilitando a exibição do status da infraestrutura em telas grandes para diferentes equipes.

6.2.3.3 Deverá possuir sistema de sensores dedicados com configurações complexas com "scripts" ou linhas de comando.

6.2.3.4 Deverá permitir configurar sensores de PING, utilização de CPU, tráfego web, temperatura, através de interface visual intuitiva e amigável

6.2.3.5 Deverá possuir painéis (dashboards) e mapas gráficos em tempo real fáceis de montar através do sistema drag-and-drop (arrastar e soltar).

6.2.3.6 O software de monitoramento e auditoria, deverá possuir uma "automação Inteligente" com recursos automatizados que facilitem a detecção de anomalias na rede sem exigir interação constante dos administradores. O sistema deverá conseguir "aprender" o que é o tráfego normal da sua rede e emite alertas quando ocorrem leituras incomuns, assim facilitando um monitoramento pro ativo evitando escalonamento de problemas.

6.2.3.7 Deverá possuir a capacidade de enviar notificações imediatas e customizadas (via e-mail, SMS, , Slack, Microsoft Teams, etc.) sempre que um serviço sai do ar ou apresenta lentidão ou comportamento incomum e quando normalizar o serviço avisar o status.

6.2.3.7 Deverá possuir a capacidade de monitorar até de 10.000 sensores e trabalhar em modo cluster, um servidor mestre e o outro em modo fail-over;

6.3.1 A CONTRATANTE exercerá a FISCALIZAÇÃO e GERENCIAMENTO da execução do objeto contratual, através de preposto(s) especialmente designado(s), composta de Gestor de Contrato e Fiscais, sem prejuízo, redução ou exclusão da responsabilidade da CONTRATADA, inclusive perante terceiros da CONTRATADA.

6.3.2 Reserva-se à CONTRATANTE o direito de intervir nos serviços, desde que em comum acordo com a CONTRATADA, nos casos críticos em que se confirme a dificuldade para promover o atendimento de urgência.

6.3.3 Caberá a CONTRATADA o fornecimento de 4 (quatro) estações de trabalho dedicadas para a equipe técnica da DTI de monitoramento, sem cobrança de qualquer valor monetário, devendo os custos dos mesmos estarem computados na prestação dos serviços descritos neste documento e seus anexos com o objetivo de poder acompanhar em tempo real todas as disponibilidades e parâmetros dos links de intranet, internet e ativos fornecidos pela CONTRATADA, para efeito de acompanhamento e auditoria dos serviços contratados.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

6.3.3.1 Cada posição de trabalho deverá ser composta por:

- a) 1 – Computador do tipo desktop, com processador de 13ª Geração Intel® Core™ i5-13500T (14 Núcleos, 24MB, 1.60 GHz to 4.60 GHz, 35W), sistema operacional Windows 11 Pro, 16 GB DDR4 (1x16GB) 3200MT/s, armazenamento SSD de 512GB PCIe NVMe M.2 (Classe 25), Mouse, teclado, com 2 monitores de 27 polegadas com taxa de resolução de 4K 3840 x 2160 a 60 Hz.
- b) 1 – No break de 1200 VA
- c) 1- Mesa de escritório retangular na cor cinza, com espessura do tampo em 15mm, medindo 1.50mt x 65cm x 75cm com pés em metal pintados na cor preto, branco ou cinza.
- d) 1 – Cadeira de escritório ergonômica preta com estofado de mesh, Medidas do assento: 52 cm de largura, 48 cm de altura mínima desde o chão, 58 cm de altura máxima desde o chão e 52 cm de profundidade, Peso máximo suportado: 120kg.
- e) 3 – Monitor de parede do tipo tv de led de 55 polegadas

6.4. QUALIDADE E DISPONIBILIDADE DO SERVIÇO PARA A REDE DE COMUNICAÇÃO DIGITAL PRIVATIVA E INDEPENDENTE.

6.4.1. Latência: O tempo de resposta, medido através de pacotes ICMP de 32 bytes deverá ser inferior a 400 ms (quatrocentos milissegundos) para 90% dos pacotes no caso de enlaces que usem comunicação via satélite, e inferior a 90 ms (noventa milissegundos) para 90% dos pacotes no caso de enlaces terrestres para as localidades fora da região metropolitana de Belém e de 5ms (cinco milissegundos) para as localidades que compõem a região metropolitana de Belém com os municípios de Ananindeua, Benevides e Marituba, (serão considerados apenas as cidades onde as sedes dos municípios de Ananindeua, Benevides e Marituba estão situadas) onde a medição será realizada entre um sítio remoto e o sítio central da rede, com a rede sem tráfego. A quantidade mínima testes ICMP realizadas, para efeito do cálculo dos 90% dos pacotes, será de 1000 testes.

6.4.2. Disponibilidade da Rede de Comunicação Digital: Entende-se por índice de disponibilidade mensal de cada unidade da Rede de Comunicação Digital, incluindo também qualquer sub rede, o índice que mede o percentual de tempo que uma unidade específica da Rede (ponto de acesso integrante do serviço) esteve operacional para transmissão e recepção (condições normais de funcionamento e operação), no período de 01 (um) mês.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

6.4.3. No cálculo da disponibilidade, serão consideradas todas as interrupções, exceto as programadas ou aquelas que estiverem fora da responsabilidade da CONTRATADA. Entendem-se como não sendo responsabilidade da CONTRATADA os eventos relacionados à ocorrência de caso fortuito (entende-se como caso fortuito como sendo qualquer ocorrência que não seja proveniente de qualquer ação humana, tais como: descargas atmosféricas, tremores de terra, maremotos, enchentes, etc.) ou que venham a ser causados pela própria CONTRATANTE.

6.4.4. Considera-se paralisação programada da CONTRATADA a interrupção para manutenção preventiva ou para substituição dos equipamentos e meios utilizados no provimento do serviço, desde que devidamente informado com antecedência mínima de 5 (cinco) dias úteis, preferencialmente fora dos horários de expediente da CONTRATANTE, não podendo ultrapassar os seguintes limites por circuito:

- a) Tempo máximo da interrupção: Até 120 (cento e vinte) minutos por circuito. Caso esse prazo venha a ser ultrapassado, o mesmo deve ser previamente comunicado à CONTRATANTE.
- b) Frequência máxima a 1 (uma) ocorrência em cada 30 (trinta) dias, não acumulativo.
- c) Quando for necessária ação da CONTRATADA nas dependências da CONTRATANTE, deverá ser solicitado prévio acesso à CONTRATANTE.

6.4.4.1. Quando o prazo mínimo de 5 (cinco) dias úteis de comunicação não for atendido, ou não houver a informação registrada, a interrupção incidirá no cômputo do cálculo de indisponibilidade do serviço.

6.4.5. Considera-se paralisação de urgência pela CONTRATADA a interrupção para manutenção preventiva ou para substituição dos equipamentos e meios utilizados no provimento do serviço que comprovadamente comprometam o seu funcionamento. Devendo, entretanto, ser comunicado à CONTRATANTE até 2 (duas) horas antes do início do atendimento através de relatório, para ciência do corpo técnico do DETRAN-PA. Caso contrário, a interrupção incidirá no cômputo do cálculo de indisponibilidade do serviço a ser aplicado pela CONTRATANTE.

6.4.6. O serviço será considerado indisponível a partir do início de uma interrupção, registrada pela CONTRATANTE na Central de Assistência Técnica (Call Center) da CONTRATADA, até o total restabelecimento do circuito principal às condições normais de



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

operação e a respectiva informação e certificação pela CONTRATANTE. Quando não forem cumpridos os parâmetros acordados na tomada de propostas, tais como: banda passante, tempo de resposta e taxa de erro, a CONTRATADA será penalizada conforme item 9.1.

6.4.7. A disponibilidade do serviço será calculada para cada circuito de acesso à Rede de Comunicação Digital, no decurso do mês considerado:

- a) Quando a indisponibilidade do serviço estabelecido não for atendida, será atribuída à CONTRATADA uma penalidade conforme explicitado no item 9.1.
- b) Na ocorrência de inoperância do serviço em qualquer unidade da Rede de Comunicação Digital, este serviço deve ser restabelecido com a máxima urgência, não devendo em hipótese alguma, ultrapassar os limites de criticidade determinados para cada unidade desta Rede definidos no Anexo IV – Planilha de Circuitos.

6.4.8. A Taxa de Erro de Bits (BER - Basic Error Rate) no acesso local deve ser igual ou inferior a 1×10^{-6} , e no backbone da rede deve ser igual ou inferior a 1×10^{-8} .

6.4.9. A Taxa de Perda de Pacotes será determinada testando-se a Rede de Comunicação Digital desde a porta WAN (Wide Area Network) do equipamento baseado na CONTRATANTE (ponta A), até a porta WAN respectiva do equipamento de uma unidade remota da rede (ponta B). De cada 100 (cem) pacotes, a perda máxima permitida é de 2% (dois por cento).

6.4.10. A disponibilidade apontada deve ser atendida para cada criticidade identificada na tabela abaixo:

Tabela 1 - Tabela de Criticidade

Criticidade	Crítérios
5	99,9 % (máx. 43min parados por mês)
4	99,7 % (máx. 02h09min parados por mês)
3	99,3 % (máx. 05h04min parados por mês)
2	98,6 % (máx. 10h05min parados por mês)
1	97,2% (max. 20h13min parados por mês)

6.5. DA CONTINGÊNCIA PARA A REDE DE COMUNICAÇÃO DIGITAL PRIVATIVA E



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

INDEPENDENTE.

6.5.1. A CONTRATADA deverá fornecer circuitos independentes sob a forma de contingência aos circuitos primários instalados nas CIRETRANS e postos de serviços descritos no **ANEXO IV** na **(PLANILHA DE CARACTERÍSTICAS DOS CIRCUITOS)** que possuam a indicação de **(SIM)** para um circuito com obrigatoriedade de contingência com a sua respectiva velocidade de contingência.

6.5.2. Será considerado um circuito de contingência, um circuito que não utilize o mesmo meio físico dedicado para o transporte de dados do circuito principal, que atenda uma determinada CIRETRAN, solução móvel de fiscalização ou posto de serviço, neste caso, o circuito de contingência para esta CIRETRAN, solução móvel de fiscalização ou posto de serviço deverá obrigatoriamente operar de forma totalmente independente e autônoma do circuito primário, sem que haja qualquer tipo de meio físico compartilhado e equipamento entre si, desde sua origem, na CIRETRAN, solução móvel de fiscalização ou posto de serviço até a sede do DETRAN/PA.

6.5.3. Os circuitos de contingência para as CIRETRANS, solução móvel de fiscalização ou posto de serviço que podem ser tanto terrestres como satelitais.

6.5.4. Os circuitos de contingência deverão ser disponibilizados para o DETRAN/PA sem que haja cobrança específica para este circuito, devendo o custo do mesmo fazer parte do custo de locação do link principal, conforme descrito no ANEXO V - Planilhas de Preços, onde o DETRAN/PA poderá fazer uso do mesmo sempre que haja a falha (perda) do circuito principal, motivado por qualquer situação de força maior ou por falha nos equipamentos da CONTRATADA e que dão suporte ao circuito principal da rede de comunicação digital privativa e independente fornecida para o DETRAN/PA, exceto para as cidades de Altamira, Belém, Castanhal, Marabá e Santarém, onde, estas cidades devem ser atendidas com dupla abordagem de circuitos independentes e terrestres com as mesmas características técnicas e de velocidade.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

6.5.4.1. A CONTRATADA deverá fornecer todos os equipamentos e infraestrutura necessária para permitir que ambos os circuitos dedicados para as localidades de Altamira, Belém, Castanhal, Marabá e Santarém, descritos no item 6.4.4 possam operar de forma simultânea em balanceamento de carga, onde na falha de um circuito o outro possa assumir de forma automática e em tempo real, desta forma o DETRAN/PA pagará para a contratada um valor fixo mensal para estas localidades contidas no ANEXO V – Planilha de Preços.

6.5.5. Os circuitos de contingências têm como único objetivo permitir que as CIRETRANS, soluções móveis de fiscalizações ou postos de serviços possam ter acesso a base nacional de dados do DENATRAN (hospedado no SERPRO-SP) para consulta nas bases de dados dos sistemas RENACH e RENAVAM. A velocidade do circuito de contingência não deverá ser inferior a 10 mbps, possuir IP fixo, deverá operar com VPN e possuir garantia de operação independentemente das condições climáticas (chuva ou céu nublado).

6.5.6. A CONTRATADA deverá instalar todos os equipamentos necessários para a implantação do circuito de contingência dedicado para cada CIRETRAN ou solução móvel de fiscalização.

6.5.7. O DETRAN/PA poderá fazer uso da contingência sem custo financeiro sempre que o circuito principal ficar inoperante, conforme o item 6.4.4. Porém, caso o DETRAN/PA decida usar o circuito de contingência estando o circuito principal operando em condições normais fica a CONTRATADA autorizada a cobrar pelo uso do circuito de contingência nos mesmos moldes do modelo de cobrança e os valores monetários para o serviço de acesso portátil e veicular via satélite, conforme descrito no **item 12, subitem 12.7** e da **Planilha 6 do Anexo V – Planilhas de Preços de Referência**, devendo a CONTRATADA informar para o DETRAN/PA sobre o uso da contingência para uma determinada CIRETRAN, solução móvel de fiscalização ou posto de serviço sempre que o circuito principal esteja operando em condições normais durante o tempo que o circuito de contingência foi utilizado, cabendo a contratada enviar o relatório demonstrando as condições de operação do circuito principal para o DETRAN/PA para que o mesmo possa confrontar estas informações junto ao seu sistema de monitoramento da rede de comunicação digital privativa e independente a fim de validar o relatório para que a contratada faça jus a cobrança pelo uso do circuito de contingência.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7. EQUIPAMENTOS E SOFTWARES DE GERENCIAMENTO PARA A REDE DE COMUNICAÇÃO DIGITAL PRIVATIVA E INDEPENDENTE

7.4. USO GERAL.

7.4.1. À CONTRATADA caberá fornecer, instalar e configurar todos os equipamentos de rede de comunicação necessários à prestação dos serviços, conforme o item 7.2 e a **Planilha 5 do Anexo V**, inclusive sistema ininterrupto de energia elétrica (no-break), este último, exceto quando explicitamente dispensados pela CONTRATANTE.

7.4.2. A CONTRATADA deve prover a quantidade de equipamentos de Solução de Segurança e Conectividade, **conforme item 7.2 e a Planilha 5 do Anexo V**, que possua funcionalidades de segurança, como firewall, IPS, Web Filtering, App Control, e Conectividade como Roteamento, suportar MPLS (Multiprotocol Label Switching), com e/ou sem capacidade para prover rede sem-fio, portas WAN e interfaces internas, necessários ao site central (ponta A) e às unidades remotas (ponta B), a fim de otimizar os recursos de telecomunicações e aplicar controle essencial para o bom funcionamento de toda a estrutura da rede.

7.4.3. Toda configuração e administração remota/presencial dos equipamentos de rede de comunicação responsáveis pela recepção dos links na localidade, serão feitas pela CONTRATADA, cabendo-lhe ainda as ações locais, quando necessárias, sob orientação da CONTRATANTE.

7.4.4. Toda gerência/administração remota/presencial dos equipamentos de segurança do tipo NGFW, Solução WI-FI e Switches CORE, a serem instalados nas localidades, serão feitas pela CONTRATANTE, cabendo-lhe ainda as ações locais, quando necessária, cabendo à CONTRATADA o suporte e manutenção dos equipamentos.

7.4.5. A CONTRATADA deve prover de modo proativo atualizações de sistema operacional, software de gerência, firmwares e outros essenciais ao bom e seguro funcionamento dos equipamentos fornecidos, no caso dos equipamentos sob



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

administração da CONTRATANTE, tais atualizações deverão ser demandas à CONTRATADA para provimento.

7.4.5.1. Quando da execução dos serviços listados no item 7.1.4, deverá ser fornecido pela CONTRATADA infraestrutura suficiente para que sejam mantidos em funcionamento os circuitos essenciais no período das atualizações no intuito de diminuir o impacto da indisponibilidade do serviço, entende-se por circuitos essenciais os circuitos de criticidade 4 e 5, conforme **Anexo IV– Planilha de Características dos Circuitos**.

7.4.6. Os equipamentos a serem fornecidos devem ter capacidade para operar suas interfaces especificadas à plena carga, durante 100% do tempo de operação, devendo a CONTRATADA manter todos os equipamentos devidamente atualizados e licenciados durante todo o período do contrato.

7.4.7. A LICITANTE deverá informar em sua proposta comercial o nome do fabricante, marca e modelo de todos os equipamentos e softwares especificados no item 7.2. Os equipamentos dos Tipos 1, 2, e 3 em razão de padronização em sua função deverão ser do mesmo fabricante, assim como, devem ser novos (sem uso anterior) e não estarem descontinuados pelo fabricante na data da licitação e deverão ser gerenciados pela CONTRATADA.

7.4.8. Os equipamentos dos Tipos 4, 5, 6, 7, 11 e 12 em razão de padronização em sua função deverão ser do mesmo fabricante, assim como, devem ser novos (sem uso anterior) e não estarem descontinuados pelo fabricante na data da licitação, e deverão ser gerenciados pela CONTRATANTE.

7.1.9 Os equipamentos dos Tipos 8 e 9 em razão de padronização em sua função deverão ser do mesmo fabricante, assim como, devem ser novos (sem uso anterior) e não estarem descontinuados pelo fabricante na data da licitação, deverão ser gerenciados pela CONTRATANTE.

7.1.10 A solução que abrange os equipamentos 8 e 9 deverá ser executada em



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

conformidade à LGPD (Lei Geral de Proteção de Dados).

7.1.11 Todos os equipamentos devem ser instalados pela CONTRATADA.

7.1.12 Será de Responsabilidade da CONTRATADA o fornecimento de todos os acessórios necessários ao funcionamento dos equipamentos, como cabos UTP, Patches Cords, bandejas, Racks, Cordões Ópticos, Cabos AOC, Gbics etc...

7.1.13. Os equipamentos e softwares de rede de comunicação e segurança, bem como no-breaks devem ter as seguintes **características mínimas** detalhadas no item 7.2.

7.5. TIPOS DE EQUIPAMENTOS PARA A REDE DE COMUNICAÇÃO DIGITAL PRIVATIVA E INDEPENDENTE.

7.5.1. Tipo 1 - Solução de Conectividade ROTEADOR / SWITCH - (Ponta "A" – DETRAN/SEDE)

7.2.1.1 Características Gerais

7.2.1.1.1 Switch ethernet compatível com as seguintes características:

- Roteamento IP (Camada 3);
- Giga Ethernet (802.3z);
- 10 Giga Ethernet (802.3ae);
- 100G Base-X (802.3bm) / 40G Base-X (802.3ba);

7.2.1.1.2 Possuir no mínimo 8 portas 10GE óticas (SFP+), 16 portas 25GE (SFP28) e 6 portas 100G (QSFP28).

7.2.1.1.3 O equipamento deve apresentar altura máxima de 1U em gabinete metálico, montável em rack de 19". Este vir acompanhado dos devidos acessórios para fixação em rack 19".

7.2.1.1.4 Suportar operação normal em temperaturas de 0 a 45°C.

7.2.1.1.5 Umidade Relativa 10% até 90% sem condensação.

7.2.1.1.6 O equipamento deverá ser projetado para operar em altitudes de até 3.000 metros, sem comprometimento da performance ou qualquer



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

funcionalidade.

7.2.1.1.7 O equipamento deverá ser de primeira qualidade, novo, sem uso, de fabricação recente (fabricado no máximo a 6 meses antes da data de entrega) e com acabamento apropriado.

7.2.1.2 Fonte de Alimentação

7.2.1.2.1 Possuir fonte de alimentação redundante hot-swap AC (100/240 Vac 50/60Hz).

7.2.1.2.2 Deve permitir a combinação de fontes AC e DC no mesmo chassi.

7.2.1.2.3 As fontes de alimentação devem ser internas ao chassis do equipamento.

7.2.1.2.4 A fonte de alimentação instalada deve alimentar e suportar a configuração solicitada.

7.2.1.2.5 O equipamento não deverá ter consumo superior a 380W

7.2.1.3 Desempenho

7.2.1.3.1 Deve possuir arquitetura wire-speed interna.

7.2.1.3.2 Comutação agregada maior ou igual a 2.160 Gbps.

7.2.1.3.3 Encaminhamento de pacotes de no mínimo 1.000 Mpps.

7.2.1.4 Camada de Comutação L2

7.2.1.4.1 Permitir a configuração de até 4k VLANs com até 4k VLAN IDs (não considerar mecanismos multiplicadores como por exemplo Q-in-Q).

7.2.1.4.2 Implementar no mínimo 288.000 endereços MAC.

7.2.1.4.3 Implementar 802.1Q Virtual Bridged LAN (VLAN).

7.2.1.4.4 Implementar 802.1ad Double Tagging (Q-in-Q).

7.2.1.4.5 Implementar 802.1D MAC Bridges.

7.2.1.4.6 Implementar jumbo frames (9k Bytes).

7.2.1.4.7 Implementar 802.1p Traffic Class Expediting.

7.2.1.4.8 Implementar 802.3ad (LACP).



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.1.4.9 Implementar 802.1D - STP.

7.2.1.4.10 Implementar 802.1w Rapid STP.

7.2.1.4.11 Implementar 802.1s Multiple STP (MSTP).

7.2.1.4.12 Implementar protocolo EAPS, otimizado para anéis baseado em

7.2.1.4.13 L2, conforme descrito na RFC3619.

7.2.1.4.14 Implementar protocolo ERPS, otimizado para anéis baseado em L2.

7.2.1.4.15 Implementar listas de acesso ACL em L2 em hardware.

7.2.1.4.16 Implementar o tunelamento de protocolo L2 para serviços LAN-to-LAN.

7.2.1.4.17 Implementar configuração de "Aging" L2 global.

7.2.1.4.18 Implementar QinQ seletivo.

7.2.1.5 Multicast

7.2.1.5.1 Implementar Multicast.

7.2.1.5.2 Implementar no mínimo 8000 grupos Multicast.

7.2.1.5.3 Implementar IGMP snooping com proxy report.

7.2.1.5.4 Implementar RFC 2236 IGMP v2.

7.2.1.5.5 Implementar RFC 3376 IGMP v3.

7.2.1.6 Funcionalidades L3

7.2.1.6.1 Implementar roteamento estático IPv4 e IPv6

7.2.1.6.2 Implementar roteamento entre VLANs

7.2.1.6.3 Suportar 256 VLANs com IP configurado

7.2.1.6.4 Suportar no mínimo 168.000 rotas IPv4 e 42.000 rotas IPv6

7.2.1.6.5 Implementar BGP, com opção de autenticação MD5

7.2.1.6.6 Implementar BGP IP Prefix Lists e Route Map

7.2.1.6.7 Suportar pelo menos 256 neighbors BGP

7.2.1.6.8 Implementar OSPF Prefix Lists Filter

7.2.1.6.9 Implementar OSPFv2, com opção de autenticação MD5

7.2.1.6.10 Suportar pelo menos 32 áreas e 32 adjacências OSPFv2



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.1.6.11 Permitir redistribuição de rotas entre protocolos de roteamento
- 7.2.1.6.12 Suportar pelo menos 2.000 hosts IPv4 ou 1.000 hosts IPv6
- 7.2.1.6.13 Implementar 32 grupos de VRRP
- 7.2.1.6.14 Implementar VRF-Lite (Virtual Routing Forwarding)
- 7.2.1.6.15 Deve suportar no mínimo 222 VRFs
- 7.2.1.6.16 Implementar BFD para OSPF IPv4
- 7.2.1.6.17 Possibilitar a distribuição de rotas entre os protocolos
- 7.2.1.6.18 Suportar IETF - RFC3101 - The OSPF Not-So-Stubby Area (NSSA) Option
- 7.2.1.6.19 Implementar IETF - RFC5250 - The OSPF Opaque LSA Option
- 7.2.1.6.20 Implementar IETF - RFC5340 - OSPF for IPv6 - OSPFv3
- 7.2.1.6.21 Implementar IETF - RFC1997 - BGP Communities Attribute
- 7.2.1.6.22 Implementar IETF - RFC2545 - Use of BGP-4 Multiprotocol
- 7.2.1.6.23 Extensions for IPv6 InterDomain Routing
- 7.2.1.6.24 Suportar IETF - RFC2918 - Route Refresh Capability for BGP-4
- 7.2.1.6.25 Implementar IETF - RFC4271 - A Border Gateway Protocol 4 (BGP-4)
- 7.2.1.6.26 Suportar IETF - RFC4456 - BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
- 7.2.1.6.27 Suportar IETF - RFC4893 - BGP Support for Four-octet AS Number Space

7.2.1.7 MPLS - Multiprotocol Label Switching

- 7.2.1.7.1 A funcionalidade MPLS deve estar disponível para todas as interfaces do equipamento.
- 7.2.1.7.2 Todas as licenças devem ser fornecidas em conjunto com equipamento.
- 7.2.1.7.3 Deve permitir operação como LER (Label Edge Router) ou LSR (Label Switch Router).
- 7.2.1.7.4 Implementar L2VPN - IETF - RFC4762 - VPLS Virtual Private LAN Service using LDP.
- 7.2.1.7.5 Implementar L2VPN - IETF - RFC4447 and RFC4448 - VPWS



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Virtual Pseudo Wire Service using LDP.

7.2.1.7.6 Implementar VPLS TLS (Transparent LAN Service).

7.2.1.7.7 Suportar VPLS MAC Limit Tunning.

7.2.1.7.8 Suportar IETF - RFC6391 - Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network.

7.2.1.7.9 Suportar IETF - RFC5036 - LDP Specification.

7.2.1.7.10 Suportar MD5 authentications for LDP sessions.

7.2.1.7.11 Implementar RFC4364 - BGP/MPLS IP Virtual Private Networks (VPNs).

7.2.1.7.12 Implementar o protocolo LDP (Label Distribution Protocol).

7.2.1.7.13 Suportar pelo menos 1.024 circuitos VPWS ou VPLS.

7.2.1.7.14 Suportar a criação de pelo menos 1.024 PWs.

7.2.1.7.15 Implementar RFC 2205 - Resource ReSerVation Protocol (RSVP).

7.2.1.8 OAM - Operations, Administration and Management

7.2.1.8.1 Implementar IEEE - 802.1ag - Connectivity Fault Management (CFM) - Continuity Check Protocol

7.2.1.8.2 Implementar IEEE - 802.1ag - Connectivity Fault Management (CFM) - Linktrace Protocol

7.2.1.8.3 Implementar IEEE - 802.1ag - Connectivity Fault Management (CFM) - Loopback Protocol

7.2.1.8.4 Implementar IETF - RFC5357 - A Two-Way Active Measurement Protocol - TWAMP Session-Reflector and Server (Responder)

7.2.1.8.5 Implementar IETF - RFC5357 - A Two-Way Active Measurement Protocol - TWAMP Session-Sender and Control-Client (Controller)

7.2.1.8.6 Implementar ITU-T - Y.1731 - Fault Management - Ethernet alarm indication signal (ETH-AIS)

7.2.1.8.7 Implementar ITU-T - Y.1731 - Fault Management - Ethernet continuity check (ETH-CC)

7.2.1.8.8 Implementar ITU-T - Y.1731 - Performance Monitoring - Frame delay measurement (ETH-DM)



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.1.9 Deve implementar as seguintes normas e padrões do IETF -

Internet Engineering Task Force:

7.2.1.9.1 RFC 783 The TFTP Protocol (Revision 2)

7.2.1.9.2 RFC 791 Internet Protocol (IP)

7.2.1.9.3 RFC 792 Internet Control Message Protocol (ICMP) (Ping IPv4)

7.2.1.9.4 RFC 793 Transmission Control Protocol (TCP)

7.2.1.9.5 RFC 826 An Ethernet Address Resolution Protocol (ARP)

7.2.1.9.6 RFC 854 TELNET Protocol Specification

7.2.1.9.7 RFC 894 A Standard for the Transmission of IP Datagrams over Ethernet Networks

7.2.1.9.8 RFC 1157 A Simple Network Management Protocol (SNMPv1)

7.2.1.9.9 RFC 1213 Management Information Base for Network Management of TCP/IP-based internets: MIB-II (Obsoletes RFC 1158)

7.2.1.9.10 RFC 1215 A Convention for Defining Traps for use with the SNMP - TRAPS MIB

7.2.1.9.11 RFC 1441 Introduction to version 2 of the Internet-standard Network Management Framework (SNMPv2)

7.2.1.9.12 RFC 1700 Assigned Numbers

7.2.1.9.13 RFC 1901 to RFC1908 SNMPv2c

7.2.1.9.14 RFC 2030 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI

7.2.1.9.15 RFC 2236 Internet Group Management Protocol, Version 2 - IGMPv2

7.2.1.9.16 RFC 2328 OSPF Version 2 (obsoletes RFC2178, RFC1583, RFC1247 e RFC1131)



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.1.9.17 RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option
- 7.2.1.9.18 RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- 7.2.1.9.19 RFC 2464 Transmission of IPv6 packets over Ethernet networks
- 7.2.1.9.20 RFC 2474 Definition of the Differentiated Services Field (DSField) in the IPv4 Headers (DSCP Remarking for IPv4)
- 7.2.1.9.21 RFC 2597 Assured Forwarding PHB Group
- 7.2.1.9.22 RFC 2865 Remote Authentication Dial In User Service (RADIUS) (obsoletes RFC 2138)
- 7.2.1.9.23 RFC 2866 RADIUS Accounting (obsoletes RFC2139)
- 7.2.1.9.24 RFC 3021 Using 31-Bit Prefixes on IPv4 Point-to-Point Links
- 7.2.1.9.25 RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)
- 7.2.1.9.26 RFC 3376 Internet Group Management Protocol, Version 3 - IGMPv3
- 7.2.1.9.27 RFC 3410 to RFC3418 SNMPv3 agent
- 7.2.1.9.28 RFC 3587 IPv6 Global Unicast Address Format
- 7.2.1.9.29 RFC 3619 EAPS
- 7.2.1.9.30 RFC 4291 IP Version 6 Addressing Architecture
- 7.2.1.9.31 RFC 4632 Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
- 7.2.1.9.32 RFC 4742 Using the NETCONF Configuration Protocol over Secure Shell (SSH)
- 7.2.1.9.33 RFC 4861 Neighbor Discovery for IP version 6 (IPv6)
- 7.2.1.9.34 RFC 4862 IPv6 Stateless Address Autoconfiguration
- 7.2.1.9.35 RFC 5277 NETCONF Event Notifications
- 7.2.1.9.36 RFC 5396 Textual Representation of Autonomous System (AS) Numbers
- 7.2.1.9.37 RFC 5717 Partial Lock Remote Procedure Call (RPC) for NETCONF



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.1.9.38 RFC 6020 YANG - A Data Modeling Language for the Network Configuration Protocol (NET-CONF)

7.2.1.9.39 RFC 6021 Common YANG Data Types

7.2.1.9.40 RFC 6022 YANG Module for NETCONF Monitoring

7.2.1.9.41 RFC 6241 Network Configuration Protocol (NETCONF) (Obsoletes RFC 4741)

7.2.1.9.42 RFC 6242 Using the NETCONF Configuration Protocol over Secure Shell (SSH)

7.2.1.9.43 RFC 6243 With-defaults capability for NETCONF

7.2.1.9.44 RFC 6470 NETCONF Base Notifications

7.2.1.9.45 RFC 6536 NETCONF Access Control Model

7.2.1.9.46 RFC 6991 Common YANG Data Types (Obsoletes RFC 6021)

7.2.1.10 QoS - Quality Of Service

7.2.1.10.1 Deve suportar remarcação de P-bit (PCP).

7.2.1.10.2 Deve permitir classificação de pacotes baseada em DSCP, origem/destino IP, origem/destino MAC, VLAN, porta.

7.2.1.10.3 Deve permitir mapeamento DSCP para COS.

7.2.1.10.4 Deve implementar escalonamento de filas por WFQ (Weighted Fair Queuing) e SP (Strict Priority).

7.2.1.10.5 Deve suportar até 8 filas de prioridade por porta.

7.2.1.11 Gerenciamento

7.2.1.11.1 Deve suportar commit e rollback de operações.

7.2.1.11.2 Implementar gerenciamento in-band e out-of-band.

7.2.1.11.3 Implementar estatísticas por porta Ethernet.

7.2.1.11.4 Deve suportar firmware rollback.

7.2.1.11.5 Deve permitir upgrade de firmware via TFTP.

7.2.1.11.6 Deve suportar RADIUS Accounting.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.1.11.7 Deve suportar o protocolo SNMPv1, SNMPv2, SNMPv2c, SNMPv3.
- 7.2.1.11.8 Suportar configuração através da interface de linha de comando (CLI) via SSHv2, Telnet e console RS-232 ou USB.
- 7.2.1.11.9 Digital diagnostics de módulos óticos segundo a SFF 8472.
- 7.2.1.11.10 Possuir LED indicador de estado do sistema e alarmes.
- 7.2.1.11.11 Informações de inventário.
- 7.2.1.11.12 Deve suportar o armazenamento de até 2 firmwares e de até 8 configurações na memória Flash do equipamento.
- 7.2.1.11.13 Monitoramento de uso de CPU e memória, com status disponível por SNMP.
- 7.2.1.11.14 Suportar o protocolo SNTP (Simple Network Time Protocol)
- 7.2.1.11.15 IPv4/IPv6 conforme RFC 2030.
- 7.2.1.11.16 Suportar Syslog local e remoto.
- 7.2.1.11.17 Implementar IEEE - 802.1AB - LLDP (Link Layer Discovery Protocol).
- 7.2.1.11.18 Implementar Loopback Detection.

7.2.1.12 Características Gerais de Interface

- 7.2.1.12.1 Suportar Link Aggregation estático e dinâmico (LACP).
- 7.2.1.12.2 Implementar no mínimo 8 grupos de interfaces agregadas por sistema.
- 7.2.1.12.3 Implementar agregação de enlaces Ethernet 1GE.
- 7.2.1.12.4 Implementar agregação de enlaces Ethernet 10GE.
- 7.2.1.12.5 Implementar agregação de pelo menos 8 interfaces em cada grupo.

7.2.1.13 Filtros de Segurança

- 7.2.1.13.1 Deve suportar ACL Actions remark/deny.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.1.13.2 Deve suportar ACL Match L2 e L3.

7.2.1.13.3 Suporte a pelo menos 1000 regras de ACLs.

7.2.1.13.4 Implementar mecanismos de proteção contra ataques Broadcast, Multicast ou DLF.

7.2.1.13.5 Deve permitir a proteção de CPU contra ataques Denial of Service (DoS).

7.2.1.13.6 Deve suportar mecanismos de proteção contra IP spoofing.

7.2.1.13.7 Deve suportar autenticação de usuários através de RADIUS ou TACACS+.

7.2.1.14 ANATEL - Agência Nacional de Telecomunicações

7.2.1.14.1 Deve possuir certificação ANATEL conforme Resolução 242 (30 de Novembro 2000).

7.2.1.14.2 Deve possuir certificação ANATEL conforme Resolução 323 (7 de Novembro de 2002).

7.2.1.14.3 Deve possuir certificação ANATEL conforme Resolução 442 (21 de julho 2006).

7.2.1.15 ETSI - European Telecommunications Standards Institute

7.2.1.15.1 EN 300 019-1-1, Class 1.2 Environmental Conditions for storage.

7.2.1.15.2 EN 300 019-1-2, Class 2.3 Environmental Conditions for Transport.

7.2.1.15.3 EN 300 386 V1.6.1 (2012-09) Electromagnetic compatibility and Radio spectrum Matters (ERM).

7.2.1.15.4 EN 55022 Information technology equipment. Radio disturbance characteristics - Class A.

7.2.1.16 IEC - International Electrotechnical Commission

7.2.1.16.1 IEC 60825-1 Laser Safety Class.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.1.16.2 IEC 61000-4-11 Voltage dips, short interruptions and voltage variations immunity tests.

7.2.1.16.3 IEC 61000-4-6 Immunity to conducted disturbances, induced by radio-frequency fields.

7.2.1.16.4 EN 61000-4-2 Electrostatic Discharge Immunity Test.

7.2.1.16.5 EN 61000-4-4 Electrical fast Transient/burst Immunity Test.

7.2.1.16.6 EN 61000-4-5 Surge Immunity Test.

7.2.1.17 SUPORTE

7.2.1.17.1 Deve prover suporte do fabricante e atualização de firmware, durante a vigência do contrato.

7.5.2. Tipo 2 - Solução de Conectividade ROTEADOR / SWITCH - (Ponta “B” – CIRETRAN A)

7.2.2.1 CARACTERÍSTICAS GERAIS

7.2.2.1.1 Switch ethernet compatível com as seguintes características:

- a) Roteamento IP (Camada 3)
- b) Fast e Giga Ethernet (802.3u, 802.3ab e 802.3z)
- c) Giga Ethernet (802.3ab, 802.3z)
- d) 10 Giga Ethernet (802.3ae)
- e) Stacking

7.2.2.1.2 Possuir no mínimo 48 portas 1GE 10/100/1000Base-T, 4 portas 10GE (XFP ou SFP+).

7.2.2.1.3 O equipamento deve apresentar altura de 1U, montável em rack de 19” devendo este vir acompanhado dos devidos acessórios para tal.

7.2.2.1.4 Suportar operação normal em temperaturas de 0 a 50°C e umidade Relativa 10% até 90% sem condensação.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.2.1.5 O equipamento deverá possuir ventilação forçada e adequada à operacionalização do equipamento.

7.2.2.1.6 O equipamento deverá ser de primeira qualidade, novo, sem uso, de fabricação recente (fabricado no máximo a 6 meses antes da data de entrega) e com acabamento apropriado.

7.2.2.2 FONTE DE ALIMENTAÇÃO

7.2.2.2.1 Possuir fonte de alimentação AC de 110/220 V, com chaveamento automático

7.2.2.2.2 A fonte de alimentação instalada deve possuir potência suficiente para comportar utilização de PoE (802.3af) em todas as portas ou PoE+ (802.3at) em metade das portas do switch.

7.2.2.3 DESEMPENHO

7.2.2.3.1 O equipamento possui hardware específico com tecnologia ASICs (Application-Specific Integrated Circuits) para tratar pacotes, filtros, policies e etc.

7.2.2.3.2 Possuir arquitetura non-blocking, wire-speed interna.

7.2.2.3.3 Implementar capacidade de comutação agregada maior ou igual a 136 Gbps, entrando e saindo simultaneamente.

7.2.2.3.4 Capacidade de encaminhamento de pacotes de no mínimo 100Mpps, com pacotes de, no máximo 64 bytes.

7.2.2.4 CAMADA DE COMUTAÇÃO L2

7.2.2.4.1 Implementar no mínimo 4.094 VLANs ativas (não considerar mecanismos multiplicadores como por exemplo Q-in-Q).

7.2.2.4.2 Implementar no mínimo 32.000 endereços MAC.

7.2.2.4.3 Implementar 802.1Q Virtual Bridged LANs.

7.2.2.4.4 Implementar 802.1Q-in-Q (VLAN stacking).



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.2.4.5 Implementar 802.1ad (Provider Bridges).
- 7.2.2.4.6 Implementar jumbo frames (9000 Bytes).
- 7.2.2.4.7 Implementar 802.1p tagging.
- 7.2.2.4.8 Implementar 802.3x flow control.
- 7.2.2.4.9 Implementar 802.3ad (LACP).
- 7.2.2.4.10 Implementar 802.1D MAC Bridges.
- 7.2.2.4.11 Implementar 802.1w Rapid STP e 802.1s Multiple Spanning Trees.
- 7.2.2.4.12 Implementar listas de acesso layer 2 em HW.
- 7.2.2.4.13 Implementar 802.1ab Link Layer Discovery Protocol (LLDP).
- 7.2.2.4.14 Implementar dual-mode VLANs, isto é, VLANs cujas portas podem trabalhar simultaneamente no modo “tagged” e “untagged”.
- 7.2.2.4.15 Implementar o tunelamento de protocolo L2 - STP e derivados.
- 7.2.2.4.16 Implementar controle do recebimento/filtragem de BPDU (BPDU Guard e Filtering).
- 7.2.2.4.17 Implementar entradas estáticas na tabela ARP.
- 7.2.2.4.18 Implementar Port-Based VLAN, com possibilidade de overlap de portas.
- 7.2.2.4.19 Deverá Implementar recurso de VLANs baseada em: Protocol-Based e MAC-Based.
- 7.2.2.4.20 Deverá reescrever, incluir ou retirar VLAN IDs do Frame Ethernet.
- 7.2.2.4.21 Implementar “Aging” de L2 (MAC)
- 7.2.2.4.22 Implementar definição de “Aging” por inatividade ou por tempo absoluto.
- 7.2.2.4.23 Implementar definição de VLAN em VLAN, seguindo IEEE802.1ad ou IEEE802.1 QinQ.
- 7.2.2.4.24 Implementar IEEE 802.1 QinQ seletivo.
- 7.2.2.4.25 Implementar tradução de VLANs (S-VLAN e C-VLAN).

7.2.2.5 MULTICAST



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.2.5.1 Implementar Multicast IPv4 / IPv6.

7.2.2.5.2 Implementar no mínimo 1000 grupos Multicast L2.

7.2.2.5.3 Implementar no mínimo 4000 grupos Multicast L3 (IPv4).

7.2.2.5.4 Implementar no mínimo 2000 grupos Multicast L3 (IPv6).

7.2.2.5.5 Implementar RFC 1112 IGMP, RFC 2236 IGMPv2 e RFC 3376 IGMPv3.

7.2.2.6 FUNCIONALIDADES L3

7.2.2.6.1 Implementar a configuração de rotas estáticas.

7.2.2.6.2 Implementar redistribuição de rotas entre diferentes protocolos.

7.2.2.6.3 Implementar geração de logs dos protocolos.

7.2.2.6.4 Implementar e suportar os seguintes protocolos:

7.2.2.6.5 RFC 1723 ou RFC 2453 (RIPv2);

7.2.2.6.6 RFC 2328 (OSPFv2);

7.2.2.6.7 RFC 1587 ou RFC 3101 (OSPF NSSA);

7.2.2.6.8 RFC 2370 OSPF Opaque LSA Option.

7.2.2.6.9 RFC 3137 OSPF Stub Router Advertisement.

7.2.2.6.10 RFC 3623 Graceful OSPF Restart;

7.2.2.6.11 RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2.

7.2.2.6.12 RFC 3021 - Using 31 - Bit Prefixes.

7.2.2.6.13 RFC 4601 PIM-SM e RFC 4607 PIM-SSM;

7.2.2.6.14 RFC 2338 ou RFC 3768 – VRRP para IPv4 (Virtual Router Redundancy Protocol) ou funcionalidade similar.

7.2.2.6.15 RFC 4271 BGPv4.

7.2.2.6.16 RFC 1997 Communities and Attributes.

7.2.2.6.17 RFC 2385 TCP MD5 Signature Option.

7.2.2.6.18 RFC 2796 BGP Route Reflector.

7.2.2.6.19 RFC 5492 Capability Advertisement with BGP-4.

7.2.2.6.20 RFC 4360 BGP Extended Communities Attribute.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.2.6.21 RFC 2918 Route Refresh Capability.
- 7.2.2.6.22 RFC 4893 BGP Support for Four-octet AS Number Space.
- 7.2.2.6.23 RFC 5065 Autonomous System Confederations for BGP.
- 7.2.2.6.24 RFC 4760 MP-BGP – Multiprotocol Extensions for BGP-4.
- 7.2.2.6.25 RFC 4724 Graceful Restart Mechanism for BGP.
- 7.2.2.6.26 Implementar NSR para OSPFv2.
- 7.2.2.6.27 pelo menos 8 áreas OSPFv2;
- 7.2.2.6.28 pelo menos 15 adjacências OSPFv2;
- 7.2.2.6.29 Implementar autenticação via “simple-password” e/ou “MD5”;
- 7.2.2.6.30 Implementar NSR (Non-stop Routing) para BGP.
- 7.2.2.6.31 Quando operar como um equipamento L3, a capacidade mínima de rotas IPV4: 12k.
- 7.2.2.6.32 Quando operar como um equipamento L3, a capacidade mínima de rotas IPV6: 6k.
- 7.2.2.6.33 Implementa o switching de nível 3 (três) em Wire Speed.

7.2.2.7 IPv6

- 7.2.2.7.1 Implementar RFC 2710 Multicast Listener Discovery (MLD) for IPv6.
- 7.2.2.7.2 Implementar RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6.
- 7.2.2.7.3 Implementar telnet e ssh sobre IPv6 para gerência do equipamento.
- 7.2.2.7.4 Implementar RFC 2460 IPv6 Specification.
- 7.2.2.7.5 Implementar RFC 2461 IPv6 Neighbor Discovery.
- 7.2.2.7.6 Implementar RFC 2462 IPv6 Stateless Address Auto-Configuration.
- 7.2.2.7.7 Implementar RFC 4443 ICMPv6.
- 7.2.2.7.8 Implementar RFC 4291 IPv6 Addressing Architecture.
- 7.2.2.7.9 Implementar RFC 3587 IPv6 Global Unicast Address Format.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.2.7.10 Implementar RFC 2464 Transmission of IPv6 over Ethernet Networks.
- 7.2.2.7.11 Implementar RFC 4213 Transition Mechanisms for IPv6 Hosts and Routers - Dual IP Layer.
- 7.2.2.7.12 Implementar RFC 2740 OSPF for IPv6 (OSPFv3).
- 7.2.2.7.13 Implementar PIM SM para IPv6 - RFC 4601.
- 7.2.2.7.14 Implementar PIM SSM para IPv6 - RFC 3569.
- 7.2.2.7.15 Implementar Multicast IPv6.

7.2.2.8 OAM

- 7.2.2.8.1 Implementar Ethernet Link OAM IEEE 802.3ah.
- 7.2.2.8.2 Implementar Ethernet CFM IEEE 802.1ag.
- 7.2.2.8.3 Implementar Ethernet Y.1731.
- 7.2.2.8.4 Implementar Ethernet LMI.

7.2.2.9 MEF

- 7.2.2.9.1 Conformidade com o padrão MEF 9 - Abstract Test Suite for Ethernet Services at the UNI.
- 7.2.2.9.2 Conformidade com o padrão MEF 14 - Abstract Test Suite for Traffic Management Phase 1.
- 7.2.2.9.3 Conformidade com o padrão MEF 2.0.

7.2.2.10 CARACTERÍSTICAS GERAIS DAS INTERFACES

- 7.2.2.10.1 Suportar interface 1GE IEEE 802.3z para fibra óptica.
- 7.2.2.10.2 Suportar transceiver para fibra multimodo - 1000BASE-SX.
- 7.2.2.10.3 Suportar transceiver para fibra monomodo - 1000BASE-LX, EX e ZX
- 7.2.2.10.4 Suportar portas UTP, 1000 BASE-T - padrão IEEE 802.3ab.
- 7.2.2.10.5 Suportar transceiver para fibra monomodo - 1000BASEBX10 e 1000BASE-BX10-U para aplicações bidirecionais em fibra única.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.2.10.6 Implementar contadores de frames recebidos e descartados para interfaces 1GE.
- 7.2.2.10.7 Implementar agregação de enlaces Ethernet 1GE.
- 7.2.2.10.8 Implementar agregação de pelo menos 8 interfaces.
- 7.2.2.10.9 Implementar Auto-MDIX (automatic medium-dependent interface crossover) para as portas elétricas.
- 7.2.2.10.10 Implementar no mínimo 128 grupos de interfaces agregadas por sistema.
- 7.2.2.10.11 Implementar o Link Flap Detection. Utilizado para detectar interfaces que continuamente sinalizam “Up” e “Down” devido a algum problema.
- 7.2.2.10.12 Suportar interface 10GbE IEEE 802.3ae LAN PHY.
- 7.2.2.10.13 Suportar transceiver para fibra multimodo - 10GBASE-SR.
- 7.2.2.10.14 Suportar transceiver para fibra multimodo - 10GBASE-LR, ER e ZR.
- 7.2.2.10.15 Implementar contadores de frames recebidos e descartados para interfaces 10GE.
- 7.2.2.10.16 Implementar agregação de enlaces Ethernet 10GE.

7.2.2.11 QoS

- 7.2.2.11.1 Implementar QoS do nível L2 até L4.
- 7.2.2.11.2 Implementar priorização de tráfego (QoS) por tipo de protocolo e por serviços
- 7.2.3.11.3 TCP/IP.
- 7.2.2.11.4 Implementar RFC 2474 - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.
- 7.2.2.11.5 Implementar DiffServ - RFC 2475 - An Architecture for Differentiated Services.
- 7.2.2.11.6 Implementar RFC 2474 DiffServ Precedence, including 8 queues/port.
- 7.2.2.11.7 Implementar RFC 2598 DiffServ Expedited Forwarding (EF).



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.2.11.8 Implementar RFC 2597 DiffServ Assured Forwarding (AF).
- 7.2.2.11.9 Implementar RFC 2475 DiffServ Core and Edge Router Functions.
- 7.2.2.11.10 Implementar pelo menos 8 filas de QoS (em hardware) por porta.
- 7.2.2.11.11 Deverá implementar o Rate Shapping Bidirecional (Ingress e Egress) com granularidade a partir de 64K bit/s por porta.
- 7.2.2.11.12 Implementar Egress Shaping.
- 7.2.2.11.13 Implementar Ingress Policing.
- 7.2.2.11.14 Implementar mecanismos para avaliação dos pacotes que excederem a especificação de banda, configurando ações tais como: transmissão sem modificação, transmissão com remarcação e descarte.
- 7.2.2.11.15 Implementar RFC 2697 A Single Rate Three Color Marker.
- 7.2.2.11.16 Implementar configuração de 2 rate 3 color policer ou shaper - RFC2698 - A Two Rate Three Color Marker.
- 7.2.2.11.17 Implementar mecanismo de priorização baseado em classes.
- 7.2.2.11.18 Implementar mecanismos de QoS Strict Priority, WFQ(Weighted Fair Queuing) e WRR (Weighted Round Robin).
- 7.2.2.11.19 Implementar WRED - Weighted Random Early Detection.
- 7.2.2.11.20 Implementar funcionalidades de controle e limitação de tráfego com garantia de banda por classe de serviço.
- 7.2.2.11.21 Implementar classificação e marcação de pacotes baseada em endereço de origem.
- 7.2.2.11.22 Implementar classificação e marcação de pacotes baseada em porta de origem.
- 7.2.2.11.23 Implementar classificação e marcação de pacotes baseada em endereço de destino.
- 7.2.2.11.24 Implementar classificação e marcação de pacotes baseada em porta de destino.
- 7.2.2.11.25 Implementar classificação e marcação de pacotes baseada em marcação DSCP.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.2.11.26 Implementar classificação e marcação de pacotes baseada em marcação IP Precedence.

7.2.2.11.27 Implementar classificação e marcação de pacotes baseada em CoS ("Class of Service" – nível 2).

7.2.2.11.28 Implementar funcionalidade que permita o mapeamento do tráfego via lista de controle.

7.2.2.11.29 Implementar aplicação de políticas de QoS em todas as portas físicas do equipamento.

7.2.2.11.30 A aplicação de features de QoS e Rate shaping não deve causar impactos significativos no sistema, a ponto de degradar os serviços.

7.2.2.11.31 Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP).

7.2.2.12 GERENCIAMENTO

7.2.2.12.1 Os Switches deverão possuir pelo menos uma porta serial RS-232 para acesso ao equipamento, via console com conector DB-9 ou RJ45.

7.2.2.12.2 A Memória Flash instalada deve ser suficiente para comportar no mínimo duas imagens do Sistema Operacional simultaneamente, permitindo que seja feito um upgrade de Software e a imagem anterior seja mantida.

7.2.2.12.3 Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events.

7.2.2.12.4 Deverá armazenar simultaneamente mais de uma configuração do equipamento em memórias tipo Flash ou disco rígido.

7.2.2.12.5 Deverá realizar o upload e download da configuração.

7.2.2.12.6 Implementar SNMPv2c e SNMPv3.

7.2.2.12.7 Implementar pelo menos os seguintes níveis de segurança para SNMPv3: Com autenticação e sem privacidade, com autenticação e com privacidade.

7.2.2.12.8 Implementar SSH v2 server.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.2.12.9 Implementar cópia de arquivos de configuração e imagens de firmware usando no mínimo um dos seguintes protocolos: TFTP/FTP/SFTP/SCP.
- 7.2.2.12.10 Implementar gerência fora de banda por interface dedicada.
- 7.2.2.12.11 Deverá possuir interface Console padrão RS232 (EIA/TIA 561 – conector RJ45), ou disponibilizar adaptador, na quantidade de portas console, que atenda esse padrão.
- 7.2.2.12.12 Caso o equipamento possua funcionalidade de acesso por Telnet ou via HTTP, o equipamento deverá permitir que estas sejam desabilitadas, através de configuração, sem prejuízo às demais funcionalidades do mesmo.
- 7.2.2.12.13 Implementar criação de listas de acesso baseadas em endereços IP para limitar o acesso ao elemento de rede via Telnet ou SSH, possibilitando a definição dos endereços IP de origem das respectivas sessões:
- 7.2.2.12.14 Implementar comandos de depuração.
- 7.2.2.12.15 Implementar recursos de segurança conforme IEEE 802.1X.
- 7.2.2.12.16 Implementar RFC 854 Telnet client and server.
- 7.2.2.12.17 Implementar RFC 2131 BOOTP/DHCP relay.
- 7.2.2.12.18 Implementar RFC 1157 SNMPv1.
- 7.2.2.12.19 Implementar RFC 1212, RFC 1215 MIB-II, Ethernet-Like MIB & TRAPs.
- 7.2.2.12.20 Implementar RFC 1573 Evolution of Interfaces Group of MIB II.
- 7.2.2.12.21 Implementar RFC 1650 Ethernet-Like MIB (update of RFC 1213 for SNMPv2).
- 7.2.2.12.22 Implementar RFC 1901 – 1908 SNMP Version 2c, SMIv2 and Revised MIB-II.
- 7.2.2.12.23 Implementar RFC 2570 – 2575 SNMPv3, user based security, encryption and authentication.
- 7.2.2.12.24 Implementar RFC 2576 Coexistence between SNMP Version 1, Version 2- and Version3.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.2.12.25 Implementar RFC 2665 Ethernet-Like-MIB.
- 7.2.2.12.26 Implementar RFC 2674 802.1p / 802.1Q MIBs.
- 7.2.2.12.27 Implementar RFC 2233 Interface MIB.
- 7.2.2.12.28 Implementar restrição de encaminhamento de frames somente para MACs específicos, aprendidos dinamicamente (port security).
- 7.2.2.12.29 Implementar restrição de encaminhamento de frames somente para MACs específicos, definidos estáticamente (port security).
- 7.2.2.12.30 Implementar DHCP Helper Address (definição de endereço de servidor DHCP).
- 7.2.2.12.31 Implementar DHCP Relay, com inserção de informações (option 82).
- 7.2.2.12.32 Implementar desativação de MAC Learning por interface.
- 7.2.2.12.33 Implementar espelhamento de tráfego para portas locais.
- 7.2.2.12.34 Implementar espelhamento de tráfego para portas remotas (em outros equipamentos).
- 7.2.2.12.35 Implementar no mínimo 4 sessões simultâneas de espelhamento de tráfego
- 7.2.2.12.36 Implementar mecanismo de isolamento de comunicação entre interfaces da mesma VLAN/Bridge Domain.
- 7.2.2.12.37 Implementar monitoração do uso de CPU do processador via SNMP.
- 7.2.2.12.38 Implementar monitoração do uso de memória do processador via SNMP.
- 7.2.2.12.39 Implementar monitoração do uso de CPU do processador via comando de operação.
- 7.2.2.12.40 Implementar monitoração do uso de memória do processador via comando de operação.
- 7.2.2.12.41 Implementar menos 2000 listas de controle de tráfego (ACLs) para Ipv4.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.2.12.42 Implementar listas de controle complexas sem perda de desempenho.

7.2.2.12.43 Implementar contadores para as listas de acesso.

7.2.2.12.44 Implementar listas de acesso para o tráfego entrante e sainte.

7.2.2.13 SEGURANÇA

7.2.2.13.1 Implementar Syslog Local e Remoto, com capacidade de armazenamento de no mínimo 300 mensagens locais.

7.2.2.13.2 Implementar múltiplos servidores Syslog remotos.

7.2.2.13.3 Implementar RFC 1492 TACACS+.

7.2.2.13.4 Implementar RFC 2138 RADIUS Authentication.

7.2.2.13.5 Implementar RFC 2139 RADIUS Accounting.

7.2.2.13.6 Implementar autenticação dos administradores de rede usando RADIUS e TACACS+.

7.2.2.13.7 Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.

7.2.2.13.8 Implementar mecanismo para controlar quais comandos usuários ou grupos de usuários podem emitir.

7.2.2.13.9 Implementar autenticação mútua entre o servidor AAA e o cliente AAA.

7.2.2.13.10 Implementar recursos de segurança conforme IEEE 802.1X.

7.2.2.13.11 Suportar a autenticação de múltiplos usuários via 802.1x, sendo 1024 usuários por equipamento e 256 usuários por porta.

7.2.2.13.12 Implementar RFC 1305 Network Time Protocol (Version 3) ou RFC 2030 –Simple Network TimeProtocol (version 4).

7.2.2.13.13 Implementar o policiamento ou controle de acesso ao plano de controle.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.2.13.14 Todos os requisitos, exceção àqueles de capacidade (prefixo IP e MAC), devem ser atendidos de forma concomitante, ou seja, a conformidade de um requisito não pode afetar a disponibilidade dos demais.

7.2.2.13.15 Implementar limites máximos de MAC por interface.

7.2.2.13.16 Implementar limites máximos de MAC por VLAN/bridge domain.

7.2.2.13.17 Deverá Implementar os mecanismos de proteção aos protocolos L2 contra ataques de rede com limitação de banda para tráfegos de broadcast (storm), multicast e destination lookup failure(DLF). Quando um Mac de destino não se encontra na tabela FDB ocorre o DLF e então o pacote é descartado.

7.2.2.13.18 Implementar taxa máxima de Broadcast, Multicast e Unicast-desconhecido controlada por porta (storm control).

7.2.2.14 EMPILHAMENTO

7.2.2.14.1 O switch fornecido deverá ser empilhável. O empilhamento deve ser feito através de cabo dedicado e não deve consumir interfaces de rede.

7.2.2.14.2 O empilhamento deve ser feito em anel para garantir que, na eventual falha de um link, a pilha continue a funcionar.

7.2.2.14.3 Em caso de falha do switch controlador da pilha, um controlador “backup” deve ser selecionado de forma automática, sem que seja necessária intervenção manual.

7.2.2.14.4 Deve implementar espelhamento de tráfego entre portas residentes em switches diferentes da pilha.

7.2.2.14.5 Deve ser possível agregar links utilizando diferentes portas em diferentes switches em uma mesma pilha.

7.2.2.14.6 A pilha de switches deve ser gerenciada como uma entidade única e através de um único endereço IP.

7.2.2.14.7 Deve ser possível empilhar pelo menos 08 (oito) destes switches.

7.2.2.14.8 Velocidade mínima de empilhamento de 13 Gbps full duplex por porta (min 2 portas).



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.2.14.9 Deve possuir o cabo para empilhamento.

7.2.2.15 MPLS - Multiprotocol Label Switching

7.2.2.15.1 A funcionalidade MPLS deve estar disponível para todas as interfaces do equipamento.

7.2.2.15.2 Todas as licenças devem ser fornecidas em conjunto com equipamento.

7.2.2.15.3 Deve permitir operação como LER (Label Edge Router) ou LSR (Label Switch Router).

7.2.2.15.4 Implementar L2VPN - IETF - RFC4762 - VPLS Virtual Private LAN Service using LDP.

7.2.2.15.5 Implementar L2VPN - IETF - RFC4447 and RFC4448 - VPWS Virtual Pseudo Wire Service using LDP.

7.2.2.15.6 Implementar VPLS TLS (Transparent LAN Service).

7.2.2.15.7 Suportar VPLS MAC Limit Tunning.

7.2.2.15.8 Suportar IETF - RFC6391 - Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network.

7.2.2.15.9 Suportar IETF - RFC5036 - LDP Specification.

7.2.2.15.10 Suportar MD5 authentications for LDP sessions.

7.2.2.15.11 Implementar RFC4364 - BGP/MPLS IP Virtual Private Networks (VPNs).

7.2.2.15.12 Implementar o protocolo LDP (Label Distribution Protocol).

7.2.2.15.13 Suportar pelo menos 1.024 circuitos VPWS ou VPLS.

7.2.2.15.14 Suportar a criação de pelo menos 1.024 PWs.

7.2.2.15.15 Implementar RFC 2205 - Resource ReSerVation Protocol (RSVP).



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.5.3. Tipo 3 - Solução de Conectividade ROTEADOR / SWITCH - (Ponta “B” – CIRETRANS B e POSTOS/SUB REDE).

7.2.3.1 CARACTERÍSTICAS GERAIS

7.2.3.1.1 Switch ethernet compatível com as seguintes características:

- f) Roteamento IP (Camada 3)
- g) Fast e Giga Ethernet (802.3u, 802.3ab e 802.3z)
- h) Giga Ethernet (802.3ab, 802.3z)
- i) 10 Giga Ethernet (802.3ae)
- j) Stacking
- d) PoE e PoE+ (802.3af e 802.3at)

7.2.3.1.2 Possuir no mínimo 20 portas 1GE 10/100/1000Base-T, 4 portas combo 1GE elétrica/SFP e 2 portas 10GE (XFP ou SFP+).

7.2.3.1.3 O equipamento deve apresentar altura de 1U, montável em rack de 19” devendo este vir acompanhado dos devidos acessórios para tal.

7.2.3.1.4 Suportar operação normal em temperaturas de 0 a 50°C e umidade Relativa 10% até 90% sem condensação.

7.2.3.1.5 O equipamento deverá possuir ventilação forçada e adequada à operacionalização do equipamento.

7.2.3.1.6 O equipamento deverá ser de primeira qualidade, novo, sem uso, de fabricação recente (fabricado no máximo a 6 meses antes da data de entrega) e com acabamento apropriado.

7.2.3.2 FONTE DE ALIMENTAÇÃO

7.2.3.2.1 Possuir fonte de alimentação AC de 110/220 V, com chaveamento automático

7.2.3.2.2 A fonte de alimentação instalada deve possuir potência suficiente para comportar utilização de PoE (802.3af) em todas as portas ou PoE+ (802.3at) em metade das portas do switch.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.3.3 DESEMPENHO

7.2.3.3.1 O equipamento possui hardware específico com tecnologia ASICs (Application-Specific Integrated Circuits) para tratar pacotes, filtros, policies e etc.

7.2.3.3.2 Possuir arquitetura non-blocking, wire-speed interna.

7.2.3.3.3 Implementar capacidade de comutação agregada maior ou igual a 136 Gbps, entrando e saindo simultaneamente.

7.2.3.3.4 Capacidade de encaminhamento de pacotes de no mínimo 100Mpps, com pacotes de, no máximo 64 bytes.

7.2.3.4 CAMADA DE COMUTAÇÃO L2

7.2.3.4.1 Implementar no mínimo 4.094 VLANs ativas (não considerar mecanismos multiplicadores como por exemplo Q-in-Q).

7.2.3.4.2 Implementar no mínimo 32.000 endereços MAC.

7.2.3.4.3 Implementar 802.1Q Virtual Bridged LANs.

7.2.3.4.4 Implementar 802.1Q-in-Q (VLAN stacking).

7.2.3.4.5 Implementar 802.1ad (Provider Bridges).

7.2.3.4.6 Implementar jumbo frames (9000 Bytes).

7.2.3.4.7 Implementar 802.1p tagging.

7.2.3.4.8 Implementar 802.3x flow control.

7.2.3.4.9 Implementar 802.3ad (LACP).

7.2.3.4.10 Implementar 802.1D MAC Bridges.

7.2.3.4.11 Implementar 802.1w Rapid STP e 802.1s Multiple Spanning Trees.

7.2.3.4.12 Implementar listas de acesso layer 2 em HW.

7.2.3.4.13 Implementar 802.1ab Link Layer Discovery Protocol (LLDP).

7.2.3.4.14 Implementar dual-mode VLANs, isto é, VLANs cujas portas podem trabalhar simultaneamente no modo “tagged” e “untagged”.

7.2.3.4.15 Implementar o tunelamento de protocolo L2 - STP e derivados.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.3.4.16 Implementar controle do recebimento/filtragem de BPDU (BPDU Guard e Filtering).
- 7.2.3.4.17 Implementar entradas estáticas na tabela ARP.
- 7.2.3.4.18 Implementar Port-Based VLAN, com possibilidade de overlap de portas.
- 7.2.3.4.19 Deverá Implementar recurso de VLANs baseada em: Protocol-Based e MAC-Based.
- 7.2.3.4.20 Deverá reescrever, incluir ou retirar VLAN IDs do Frame Ethernet.
- 7.2.3.4.21 Implementar "Aging" de L2 (MAC)
- 7.2.3.4.22 Implementar definição de "Aging" por inatividade ou por tempo absoluto.
- 7.2.3.4.23 Implementar definição de VLAN em VLAN, seguindo IEEE802.1ad ou IEEE802.1 QinQ.
- 7.2.3.4.24 Implementar IEEE 802.1 QinQ seletivo.
- 7.2.3.4.25 Implementar tradução de VLANs (S-VLAN e C-VLAN).

7.2.3.5 MULTICAST

- 7.2.3.5.1 Implementar Multicast IPv4 / IPv6.
- 7.2.3.5.2 Implementar no mínimo 1000 grupos Multicast L2.
- 7.2.3.5.3 Implementar no mínimo 4000 grupos Multicast L3 (IPv4).
- 7.2.3.5.4 Implementar no mínimo 2000 grupos Multicast L3 (IPv6).
- 7.2.3.5.5 Implementar RFC 1112 IGMP, RFC 2236 IGMPv2 e RFC 3376 IGMPv3.

7.2.3.6 FUNCIONALIDADES L3

- 7.2.3.6.1 Implementar a configuração de rotas estáticas.
- 7.2.3.6.2 Implementar redistribuição de rotas entre diferentes protocolos.
- 7.2.3.6.3 Implementar geração de logs dos protocolos.
- 7.2.3.6.4 Implementar e suportar os seguintes protocolos:



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.3.6.5 RFC 1723 ou RFC 2453 (RIPv2);
- 7.2.3.6.6 RFC 2328 (OSPFv2);
- 7.2.3.6.7 RFC 1587 ou RFC 3101 (OSPF NSSA);
- 7.2.3.6.8 RFC 2370 OSPF Opaque LSA Option.
- 7.2.3.6.9 RFC 3137 OSPF Stub Router Advertisement.
- 7.2.3.6.10 RFC 3623 Graceful OSPF Restart;
- 7.2.3.6.11 RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2.
- 7.2.3.6.12 RFC 3021 - Using 31 - Bit Prefixes.
- 7.2.3.6.13 RFC 4601 PIM-SM e RFC 4607 PIM-SSM;
- 7.2.3.6.14 RFC 2338 ou RFC 3768 – VRRP para IPv4 (Virtual Router Redundancy Protocol) ou funcionalidade similar.
- 7.2.3.6.15 RFC 4271 BGPv4.
- 7.2.3.6.16 RFC 1997 Communities and Attributes.
- 7.2.3.6.17 RFC 2385 TCP MD5 Signature Option.
- 7.2.3.6.18 RFC 2796 BGP Route Reflector.
- 7.2.3.6.19 RFC 5492 Capability Advertisement with BGP-4.
- 7.2.3.6.20 RFC 4360 BGP Extended Communities Attribute.
- 7.2.3.6.21 RFC 2918 Route Refresh Capability.
- 7.2.3.6.22 RFC 4893 BGP Support for Four-octet AS Number Space.
- 7.2.3.6.23 RFC 5065 Autonomous System Confederations for BGP.
- 7.2.3.6.24 RFC 4760 MP-BGP – Multiprotocol Extensions for BGP-4.
- 7.2.3.6.25 RFC 4724 Graceful Restart Mechanism for BGP.
- 7.2.3.6.26 Implementar NSR para OSPFv2.
- 7.2.3.6.27 pelo menos 8 áreas OSPFv2;
- 7.2.3.6.28 pelo menos 15 adjacências OSPFv2;
- 7.2.3.6.29 Implementar autenticação via "simple-password" e/ou "MD5";
- 7.2.3.6.30 Implementar NSR (Non-stop Routing) para BGP.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.3.6.31 Quando operar como um equipamento L3, a capacidade mínima de rotas IPV4: 12k.

7.2.3.6.32 Quando operar como um equipamento L3, a capacidade mínima de rotas IPV6: 6k.

7.2.3.6.33 Implementa o switching de nível 3 (três) em Wire Speed.

7.2.3.7 IPv6

7.2.3.7.1 Implementar RFC 2710 Multicast Listener Discovery (MLD) for IPv6.

7.2.3.7.2 Implementar RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6.

7.2.3.7.3 Implementar telnet e ssh sobre IPv6 para gerência do equipamento.

7.2.3.7.4 Implementar RFC 2460 IPv6 Specification.

7.2.3.7.5 Implementar RFC 2461 IPv6 Neighbor Discovery.

7.2.3.7.6 Implementar RFC 2462 IPv6 Stateless Address Auto-Configuration.

7.2.3.7.7 Implementar RFC 4443 ICMPv6.

7.2.3.7.8 Implementar RFC 4291 IPv6 Addressing Architecture.

7.2.3.7.9 Implementar RFC 3587 IPv6 Global Unicast Address Format.

7.2.3.7.10 Implementar RFC 2464 Transmission of IPv6 over Ethernet Networks.

7.2.3.7.11 Implementar RFC 4213 Transition Mechanisms for IPv6 Hosts and Routers - Dual IP Layer.

7.2.3.7.12 Implementar RFC 2740 OSPF for IPv6 (OSPFv3).

7.2.3.7.13 Implementar PIM SM para IPv6 - RFC 4601.

7.2.3.7.14 Implementar PIM SSM para IPv6 - RFC 3569.

7.2.3.7.15 Implementar Multicast IPv6.

7.2.3.8 OAM

7.2.3.8.1 Implementar Ethernet Link OAM IEEE 802.3ah.

7.2.3.8.2 Implementar Ethernet CFM IEEE 802.1ag.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.3.8.3 Implementar Ethernet Y.1731.

7.2.3.8.4 Implementar Ethernet LMI.

7.2.3.9 MEF

7.2.3.9.1 Conformidade com o padrão MEF 9 - Abstract Test Suite for Ethernet Services at the UNI.

7.2.3.9.2 Conformidade com o padrão MEF 14 - Abstract Test Suite for Traffic Management Phase 1.

7.2.3.9.3 Conformidade com o padrão MEF 2.0.

7.2.3.10 CARACTERÍSTICAS GERAIS DAS INTERFACES

7.2.3.10.1 Suportar interface 1GE IEEE 802.3z para fibra óptica.

7.2.3.10.2 Suportar transceiver para fibra multimodo - 1000BASE-SX.

7.2.3.10.3 Suportar transceiver para fibra monomodo - 1000BASE-LX, EX e ZX

7.2.3.10.4 Suportar portas UTP, 1000 BASE-T - padrão IEEE 802.3ab.

7.2.3.10.5 Suportar transceiver para fibra monomodo - 1000BASEBX10 e 1000BASE-BX10-U para aplicações bidirecionais em fibra única.

7.2.3.10.6 Implementar contadores de frames recebidos e descartados para interfaces 1GE.

7.2.3.10.7 Implementar agregação de enlaces Ethernet 1GE.

7.2.3.10.8 Implementar agregação de pelo menos 8 interfaces.

7.2.3.10.9 Implementar Auto-MDIX (automatic medium-dependent interface crossover) para as portas elétricas.

7.2.3.10.10 Implementar no mínimo 128 grupos de interfaces agregadas por sistema.

7.2.3.10.11 Implementar o Link Flap Detection. Utilizado para detectar interfaces que continuamente sinalizam “Up” e “Down” devido a algum problema.

7.2.3.10.12 Suportar interface 10GbE IEEE 802.3ae LAN PHY.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.3.10.13 Suportar transceiver para fibra multimodo - 10GBASE-SR.

7.2.3.10.14 Suportar transceiver para fibra multimodo - 10GBASE-LR, ER e ZR.

7.2.3.10.15 Implementar contadores de frames recebidos e descartados para interfaces 10GE.

7.2.3.10.16 Implementar agregação de enlaces Ethernet 10GE.

7.2.3.11 QoS

7.2.3.11.1 Implementar QoS do nível L2 até L4.

7.2.3.11.2 Implementar priorização de tráfego (QoS) por tipo de protocolo e por serviços 7.2.3.11.3 TCP/IP.

7.2.3.11.4 Implementar RFC 2474 - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.

7.2.3.11.5 Implementar DiffServ - RFC 2475 - An Architecture for Differentiated Services.

7.2.3.11.6 Implementar RFC 2474 DiffServ Precedence, including 8 queues/port.

7.2.3.11.7 Implementar RFC 2598 DiffServ Expedited Forwarding (EF).

7.2.3.11.8 Implementar RFC 2597 DiffServ Assured Forwarding (AF).

7.2.3.11.9 Implementar RFC 2475 DiffServ Core and Edge Router Functions.

7.2.3.11.10 Implementar pelo menos 8 filas de QoS (em hardware) por porta.

7.2.3.11.11 Deverá implementar o Rate Shapping Bidirecional (Ingress e Egress) com granularidade a partir de 64K bit/s por porta.

7.2.3.11.12 Implementar Egress Shaping.

7.2.3.11.13 Implementar Ingress Policing.

7.2.3.11.14 Implementar mecanismos para avaliação dos pacotes que excederem a especificação de banda, configurando ações tais como: transmissão sem modificação, transmissão com remarcação e descarte.

7.2.3.11.15 Implementar RFC 2697 A Single Rate Three Color Marker.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.3.11.16 Implementar configuração de 2 rate 3 color policer ou shaper - RFC2698 - A Two Rate Three Color Marker.
- 7.2.3.11.17 Implementar mecanismo de priorização baseado em classes.
- 7.2.3.11.18 Implementar mecanismos de QoS Strict Priority, WFQ(Weighted Fair Queuing) e WRR (Weighted Round Robin).
- 7.2.3.11.19 Implementar WRED - Weighted Random Early Detection.
- 7.2.3.11.20 Implementar funcionalidades de controle e limitação de tráfego com garantia de banda por classe de serviço.
- 7.2.3.11.21 Implementar classificação e marcação de pacotes baseada em endereço de origem.
- 7.2.3.11.22 Implementar classificação e marcação de pacotes baseada em porta de origem.
- 7.2.3.11.23 Implementar classificação e marcação de pacotes baseada em endereço de destino.
- 7.2.3.11.24 Implementar classificação e marcação de pacotes baseada em porta de destino.
- 7.2.3.11.25 Implementar classificação e marcação de pacotes baseada em marcação DSCP.
- 7.2.3.11.26 Implementar classificação e marcação de pacotes baseada em marcação IP Precedence.
- 7.2.3.11.27 Implementar classificação e marcação de pacotes baseada em CoS ("Class of Service" – nível 2).
- 7.2.3.11.28 Implementar funcionalidade que permita o mapeamento do tráfego via lista de controle.
- 7.2.3.11.29 Implementar aplicação de políticas de QoS em todas as portas físicas do equipamento.
- 7.2.3.11.30 A aplicação de features de QoS e Rate shaping não deve causar impactos significativos no sistema, a ponto de degradar os serviços.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.3.11.31 Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP).

7.2.3.12 GERENCIAMENTO

7.2.3.12.1 Os Switches deverão possuir pelo menos uma porta serial RS-232 para acesso ao equipamento, via console com conector DB-9 ou RJ45.

7.2.3.12.2 A Memória Flash instalada deve ser suficiente para comportar no mínimo duas imagens do Sistema Operacional simultaneamente, permitindo que seja feito um upgrade de Software e a imagem anterior seja mantida.

7.2.3.12.3 Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events.

7.2.3.12.4 Deverá armazenar simultaneamente mais de uma configuração do equipamento em memórias tipo Flash ou disco rígido.

7.2.3.12.5 Deverá realizar o upload e download da configuração.

7.2.3.12.6 Implementar SNMPv2c e SNMPv3.

7.2.3.12.7 Implementar pelo menos os seguintes níveis de segurança para SNMPv3: Com autenticação e sem privacidade, com autenticação e com privacidade.

7.2.3.12.8 Implementar SSH v2 server.

7.2.3.12.9 Implementar cópia de arquivos de configuração e imagens de firmware usando no mínimo um dos seguintes protocolos: TFTP/FTP/SFTP/SCP.

7.2.3.12.10 Implementar gerência fora de banda por interface dedicada.

7.2.3.12.11 Deverá possuir interface Console padrão RS232 (EIA/TIA 561 – conector RJ45), ou disponibilizar adaptador, na quantidade de portas console, que atenda esse padrão.

7.2.3.12.12 Caso o equipamento possua funcionalidade de acesso por Telnet ou via HTTP, o equipamento deverá permitir que estas sejam desabilitadas, através de configuração, sem prejuízo às demais funcionalidades do mesmo.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.3.12.13 Implementar criação de listas de acesso baseadas em endereços IP para limitar o acesso ao elemento de rede via Telnet ou SSH, possibilitando a definição dos endereços IP de origem das respectivas sessões:
- 7.2.3.12.14 Implementar comandos de depuração.
- 7.2.3.12.15 Implementar recursos de segurança conforme IEEE 802.1X.
- 7.2.3.12.16 Implementar RFC 854 Telnet client and server.
- 7.2.3.12.17 Implementar RFC 2131 BOOTP/DHCP relay.
- 7.2.3.12.18 Implementar RFC 1157 SNMPv1.
- 7.2.3.12.19 Implementar RFC 1212, RFC 1215 MIB-II, Ethernet-Like MIB & TRAPs.
- 7.2.3.12.20 Implementar RFC 1573 Evolution of Interfaces Group of MIB II.
- 7.2.3.12.21 Implementar RFC 1650 Ethernet-Like MIB (update of RFC 1213 for SNMPv2).
- 7.2.3.12.22 Implementar RFC 1901 – 1908 SNMP Version 2c, SMIv2 and Revised MIB-II.
- 7.2.3.12.23 Implementar RFC 2570 – 2575 SNMPv3, user based security, encryption and authentication.
- 7.2.3.12.24 Implementar RFC 2576 Coexistence between SNMP Version 1, Version 2- and Version3.
- 7.2.3.12.25 Implementar RFC 2665 Ethernet-Like-MIB.
- 7.2.3.12.26 Implementar RFC 2674 802.1p / 802.1Q MIBs.
- 7.2.3.12.27 Implementar RFC 2233 Interface MIB.
- 7.2.3.12.28 Implementar restrição de encaminhamento de frames somente para MACs específicos, aprendidos dinamicamente (port security).
- 7.2.3.12.29 Implementar restrição de encaminhamento de frames somente para MACs específicos, definidos estáticamente (port security).
- 7.2.3.12.30 Implementar DHCP Helper Address (definição de endereço de servidor DHCP).



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.3.12.31 Implementar DHCP Relay, com inserção de informações (option 82).

7.2.3.12.32 Implementar desativação de MAC Learning por interface.

7.2.3.12.33 Implementar espelhamento de tráfego para portas locais.

1.12.34 Implementar espelhamento de tráfego para portas remotas (em outros equipamentos).

7.2.3.12.34 Implementar no mínimo 4 sessões simultâneas de espelhamento de tráfego

7.2.3.12.35 Implementar mecanismo de isolamento de comunicação entre interfaces da mesma VLAN/Bridge Domain.

7.2.3.12.36 Implementar monitoração do uso de CPU do processador via SNMP.

7.2.3.12.37 Implementar monitoração do uso de memória do processador via SNMP.

7.2.3.12.38 Implementar monitoração do uso de CPU do processador via comando de operação.

7.2.3.12.39 Implementar monitoração do uso de memória do processador via comando de operação.

7.2.3.12.40 Implementar menos 2000 listas de controle de tráfego (ACLs) para Ipv4.

7.2.3.12.41 Implementar listas de controle complexas sem perda de desempenho.

7.2.3.12.42 Implementar contadores para as listas de acesso.

7.2.3.12.43 Implementar listas de acesso para o tráfego entrante e saindo.

7.2.3.13 SEGURANÇA

7.2.3.13.1 Implementar Syslog Local e Remoto, com capacidade de armazenamento de no mínimo 300 mensagens locais.

7.2.3.13.2 Implementar múltiplos servidores Syslog remotos.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.3.13.3 Implementar RFC 1492 TACACS+.
- 7.2.3.13.4 Implementar RFC 2138 RADIUS Authentication.
- 7.2.3.13.5 Implementar RFC 2139 RADIUS Accounting.
- 7.2.3.13.6 Implementar autenticação dos administradores de rede usando RADIUS e TACACS+.
- 7.2.3.13.7 Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.
- 7.2.3.13.8 Implementar mecanismo para controlar quais comandos usuários ou grupos de usuários podem emitir.
- 7.2.3.13.9 Implementar autenticação mútua entre o servidor AAA e o cliente AAA.
- 7.2.3.13.10 Implementar recursos de segurança conforme IEEE 802.1X.
- 7.2.3.13.11 Suportar a autenticação de múltiplos usuários via 802.1x, sendo 1024 usuários por equipamento e 256 usuários por porta.
- 7.2.3.13.12 Implementar RFC 1305 Network Time Protocol (Version 3) ou RFC 2030 –Simple Network TimeProtocol (version 4).
- 7.2.3.13.13 Implementar o policiamento ou controle de acesso ao plano de controle.
- 7.2.3.13.14 Todos os requisitos, exceção àqueles de capacidade (prefixo IP e MAC), devem ser atendidos de forma concomitante, ou seja, a conformidade de um requisito não pode afetar a disponibilidade dos demais.
- 7.2.3.13.15 Implementar limites máximos de MAC por interface.
- 7.2.3.13.16 Implementar limites máximos de MAC por VLAN/bridge domain.
- 7.2.3.13.17 Deverá Implementar os mecanismos de proteção aos protocolos L2 contra ataques de rede com limitação de banda para tráfegos de broadcast (storm), multicast e destination lookup failure(DLF). Quando um Mac de destino não se encontra na tabela FDB ocorre o DLF e então o pacote é descartado.
- 7.2.3.13.18 Implementar taxa máxima de Broadcast, Multicast e Unicast-desconhecido controlada por porta (storm control).



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.3.14 EMPILHAMENTO

7.2.3.14.1 O switch fornecido deverá ser empilhável. O empilhamento deve ser feito através de cabo dedicado e não deve consumir interfaces de rede.

7.2.3.14.2 O empilhamento deve ser feito em anel para garantir que, na eventual falha de um link, a pilha continue a funcionar.

7.2.3.14.3 Em caso de falha do switch controlador da pilha, um controlador “backup” deve ser selecionado de forma automática, sem que seja necessária intervenção manual.

7.2.3.14.4 Deve implementar espelhamento de tráfego entre portas residentes em switches diferentes da pilha.

7.2.3.14.5 Deve ser possível agregar links utilizando diferentes portas em diferentes switches em uma mesma pilha.

7.2.3.14.6 A pilha de switches deve ser gerenciada como uma entidade única e através de um único endereço IP.

7.2.3.14.7 Deve ser possível empilhar pelo menos 08 (oito) destes switches.

7.2.3.14.8 Velocidade mínima de empilhamento de 13 Gbps full duplex por porta (mínimo 2 portas).

7.2.3.14.9 Deve possuir o cabo para empilhamento.

7.2.3.15 MPLS - Multiprotocol Label Switching

7.2.3.15.1 A funcionalidade MPLS deve estar disponível para todas as interfaces do equipamento.

7.2.3.15.2 Todas as licenças devem ser fornecidas em conjunto com equipamento.

7.2.3.15.3 Deve permitir operação como LER (Label Edge Router) ou LSR (Label Switch Router).



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.3.15.4 Implementar L2VPN - IETF - RFC4762 - VPLS Virtual Private LAN Service using LDP.
- 7.2.3.15.5 Implementar L2VPN - IETF - RFC4447 and RFC4448 - VPWS Virtual Pseudo Wire Service using LDP.
- 7.2.3.15.6 Implementar VPLS TLS (Transparent LAN Service).
- 7.2.3.15.7 Suportar VPLS MAC Limit Tuning.
- 7.2.3.15.8 Suportar IETF - RFC6391 - Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network.
- 7.2.3.15.9 Suportar IETF - RFC5036 - LDP Specification.
- 7.2.3.15.10 Suportar MD5 authentications for LDP sessions.
- 7.2.3.15.11 Implementar RFC4364 - BGP/MPLS IP Virtual Private Networks (VPNs).
- 7.2.3.15.12 Implementar o protocolo LDP (Label Distribution Protocol).
- 7.2.3.15.13 Suportar pelo menos 1.024 circuitos VPWS ou VPLS.
- 7.2.3.15.14 Suportar a criação de pelo menos 1.024 PWs.
- 7.2.3.15.15 Implementar RFC 2205 - Resource ReSerVation Protocol (RSVP).

7.5.4. Tipo 4 - Solução NGFW - (Ponta “A” – DETRAN/SEDE)

7.2.4.1 Solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares “Zero Day”, Filtro de URL, bem como controle de transmissão de dados e acesso a internet compondo uma plataforma de segurança integrada e robusta;

7.2.4.2 Por plataforma de segurança entende-se hardware e software integrados do tipo appliance;

7.2.4.3 Especificações Mínimas

7.2.4.3.1 A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento:

7.2.4.3.2 Throughput de 17 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.3.3 Throughput de 8.5 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

7.2.4.3.4 Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como o atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos às sanções previstas em lei;

7.2.4.3.5 Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend);

7.2.4.3.6 Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até a camada 4.

7.2.4.3.7 Trusted Platform Module (TPM) 2.0

7.2.4.3.8 Suporte a, no mínimo, 3.800.000 de conexões simultâneas;

7.2.4.3.9 Suporte a, no mínimo, 110.000 novas conexões HTTP por segundo;

7.2.4.3.10 Fonte 120/240 AC

7.2.4.3.11 Redundância total de PSU hot-swappable

7.2.4.3.12 Disco Solid State Drive (SSD) redundante de, no mínimo, 480 GB.

7.2.4.3.13 No mínimo, 04 (quatro) interfaces de rede 1 Gbps em portas cobre;

7.2.4.3.14 No mínimo, 08 (oito) interfaces de rede 1 Gbps SFP / rede 10 Gbps SFP+

7.2.4.3.15 No mínimo, 04 (quatro) interfaces de rede 25 Gbps SFP28;

7.2.4.3.16 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.3.17 1 (uma) interface do tipo console ou similar;

7.2.4.3.18 Estar licenciada para ou suportar sem o uso de licença, 10.000 (dez mil) clientes de VPN SSL simultâneos;

7.2.4.3.19 Estar licenciada para ou suportar sem o uso de licença, 3.000 (três mil) túneis de VPN IPSEC simultâneos;

7.2.4.3.20 Deve suportar, no mínimo, 10 sistemas virtuais lógicos (Contextos) no firewall Físico;

7.2.4.3.21 Deve suportar DSPs e NPUs (Processadores de Segurança)

7.2.4.3.21 Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;

7.2.4.3.22 Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

7.2.4.3.23 Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;

7.2.4.3.24 A console de gerência e monitoração podem residir no mesmo appliance de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função;

7.2.4.3.25 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.

7.2.4.4 CARACTERÍSTICAS GERAIS

7.2.4.4.1 A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

7.2.4.4.2 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.4.3 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;

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

7.2.4.4.5 O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

7.2.4.4.6 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

7.2.4.4.7 O software deverá ser fornecido em sua versão mais atualizada, e manter atualizado e devidamente licenciado até o término do contrato.

7.2.4.4.8 Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

7.2.4.4.9 Suporte a 4094 VLAN Tags 802.1q;

7.2.4.4.10 Agregação de links 802.3ad e LACP;

7.2.4.4.11 Policy based routing ou policy based forwarding;

7.2.4.4.12 Roteamento multicast (PIM-SM);

7.2.4.4.13 DHCP Relay;

7.2.4.4.14 DHCP Server;

7.2.4.4.15 Jumbo Frames;

7.2.4.4.16 Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;

7.2.4.4.17 Suportar sub-interfaces ethernet logicas;

7.2.4.4.18 Suporte a, no mínimo, 15 (quinze) roteadores virtuais na mesma instância de firewall;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.4.19 O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;

7.2.4.4.20 Deve suportar os seguintes tipos de NAT:

7.2.4.4.21 Nat dinâmico (Many-to-1);

7.2.4.4.22 Nat dinâmico (Many-to-Many);

7.2.4.4.23 Nat estático (1-to-1);

7.2.4.4.24 NAT estático (Many-to-Many);

7.2.4.4.25 Nat estático bidirecional 1-to-1;

7.2.4.4.26 Tradução de porta (PAT);

7.2.4.4.27 NAT de Origem;

7.2.4.4.28 NAT de Destino;

7.2.4.4.29 Suportar NAT de Origem e NAT de Destino simultaneamente;

7.2.4.4.30 Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;

7.2.4.4.31 Deve implementar o protocolo ECMP;

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

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

7.2.4.4.34 Deve implementar balanceamento de link através do método round-robin;

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



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.4.36 Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;

7.2.4.4.37 Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;

7.2.4.4.38 Deve implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;

7.2.4.4.39 Enviar log para sistemas de monitoração externos, simultaneamente;

7.2.4.4.40 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

7.2.4.4.41 Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

7.2.4.4.42 Proteção contra anti-spoofing;

7.2.4.4.43 Deve permitir bloquear sessões TCP que usem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;

7.2.4.4.44 Dever permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;

7.2.4.4.45 Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;

7.2.4.4.46 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

7.2.4.4.47 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

7.2.4.4.48 Suportar a OSPF graceful restart;

7.2.4.4.49 Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.4.50 Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPsec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPsec, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação;

7.2.4.4.51 Os dispositivos de proteção devem 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);

7.2.4.4.52 Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

7.2.4.4.53 Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

7.2.4.4.54 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;

7.2.4.4.55 Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

7.2.4.4.56 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

- a) Em modo transparente;
- b) Em layer 3;

7.2.4.4.57 A configuração em alta disponibilidade deve sincronizar:

- a) Sessões;
- b) Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
- c) Certificados de-criptografados;
- d) Associações de Segurança das VPNs;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

e) Tabelas FIB;

f) O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

7.2.4.4.58 As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

7.2.4.5 CONTROLE POR POLÍTICA DE FIREWALL

7.2.4.5.1 ZTNA embutido (Zero Trust Network Access)

7.2.4.5.2 Inline CASB (Cloud Access Security Broker)

7.2.4.5.3 FWaaS / SASE-ready

7.2.4.5.4 Inspeção SSL/TLS suportando TLS 1.3 por hardware

7.2.4.5.5 IPS com ML (Machine Learning) em tempo real

7.2.4.5.6 Antivírus com Deep Learning

7.2.4.5.7 Anti-botnet

7.2.4.5.8 DNS Security incrustado

7.2.4.5.9 Deverá suportar controles por zona de segurança.

7.2.4.5.10 Controles de políticas por porta e protocolo.

7.2.4.5.11 Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

7.2.4.5.12 Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

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



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.5.14 Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;

7.2.4.5.15 Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;

7.2.4.5.16 Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

7.2.4.5.17 Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).

7.2.4.5.18 Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

7.2.4.5.19 Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

7.2.7.5.20 Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);

7.2.4.5.21 Controle de inspeção e de-criptografia de SSH por política;

7.2.4.5.22 A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

7.2.4.5.23 A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);

7.2.4.5.24 É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise.

7.2.4.5.25 Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)

7.2.4.5.26 QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.

7.2.4.5.27 Suporte a objetos e regras IPV6.

7.2.4.5.28 Suporte a objetos e regras multicast.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.5.29 Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;

7.2.4.5.30 Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

7.2.4.6 CONTROLE DE APLICAÇÕES

7.2.4.6.1 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

7.2.4.6.2 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

7.2.4.6.3 Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

7.2.4.6.4 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;

7.2.4.6.5 Deve inspecionar o payload do pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;
Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

7.2.4.6.6 Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.6.7 GUI moderna com dashboard em tempo real em HTML5

7.2.4.6.8 Cloud Management

7.2.4.6.9 Fabric View – mapa automático da rede

7.2.4.6.10 Análises de risco de configuração (Security Rating)

7.2.4.6.11 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

7.2.4.6.12 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivos dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

7.2.4.6.13 Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

7.2.4.6.14 Identificar o uso de táticas evasivas via comunicações criptografadas;

7.2.4.6.15 Atualizar a base de assinaturas de aplicações automaticamente;

7.2.4.6.16 Automação nativa

7.2.4.6.17 Automation Stitches

7.2.4.6.18 Threat Intelligence local + global

7.2.4.6.19 Reconhecer aplicações em IPv6;

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



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.6.21 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

7.2.4.6.22 Deve ser possível 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;

7.2.4.6.23 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

7.2.4.6.24 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

7.2.4.6.25 Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

7.2.4.6.26 A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:

- a) HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.

7.2.4.6.27 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

7.2.4.6.28 Deve alertar o usuário quando uma aplicação for bloqueada;

7.2.4.6.29 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

7.2.4.6.30 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;

7.2.4.6.31 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.6.32 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;

7.2.4.6.33 Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;

7.2.4.6.34 Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

7.2.4.6.35 Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc).

7.2.4.6.36 Nível de risco da aplicação.

7.2.4.6.37 IoT Detection

7.2.4.6.38 Perfilamento dinâmico

7.2.4.6.39 Application Metadata & Behavior Analysis

7.2.4.6.40 Categoria e sub-categoria de aplicações.

7.2.4.6.41 Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

7.2.4.7 PREVENÇÃO DE AMEAÇAS

7.2.4.7.1 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante.

7.2.4.7.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

7.2.4.7.3 As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.7.4 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

7.2.4.7.5 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Antipyyware e Antivírus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

7.2.4.7.6 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

7.2.4.7.7 Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

7.2.4.7.8 Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware , possibilitando a criação de diferentes

7.2.4.7.9 Políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

7.2.4.7.10 Deve permitir o bloqueio de vulnerabilidades.

7.2.4.7.11 Deve permitir o bloqueio de exploits conhecidos.

7.2.4.7.12 Deve incluir proteção contra ataques de negação de serviços.

7.2.4.7.13 Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE;

7.2.4.7.14 Deverá possuir os seguintes mecanismos de inspeção de IPS:

7.2.4.7.15 Análise de padrões de estado de conexões;

7.2.4.7.16 Análise de decodificação de protocolo;

7.2.4.7.17 Análise para detecção de anomalias de protocolo;

7.2.4.7.18 Análise heurística;

7.2.4.7.19 IP Defragmentation;

7.2.4.7.20 Remontagem de pacotes de TCP;

7.2.4.7.21 Bloqueio de pacotes malformados.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.7.22 Ser imune e ter a capacidade de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;

7.2.4.7.23 Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

7.2.4.7.24 Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

7.2.4.7.25 Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

7.2.4.7.26 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

7.2.4.7.27 Possuir assinaturas para bloqueio de ataques de buffer overflow;

7.2.4.7.28 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

7.2.4.7.29 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

7.2.4.7.30 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

7.2.4.7.31 É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;

7.2.4.7.32 Suportar bloqueio de arquivos por tipo;

7.2.4.7.33 Identificar e bloquear comunicação com botnets;

7.2.4.7.34 Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

7.2.4.7.35 Deve suportar referência cruzada com CVE;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.7.36 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

7.2.4.7.37 O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

7.2.4.7.38 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antispyware;

7.2.4.7.39 Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;

7.2.4.7.40 Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

7.2.4.7.41 Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

7.2.4.7.42 Os eventos devem identificar o país de onde partiu a ameaça;

7.2.4.7.43 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

7.2.4.7.44 Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos.

7.2.4.7.45 Rastreamento de vírus em pdf.

7.2.4.7.46 Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)

7.2.4.7.47 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada regra de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

7.2.4.8 ANÁLISE DE MALWARES MODERNOS

7.2.4.8.1 Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;

7.2.4.8.2 O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

7.2.4.8.3 Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

7.2.4.8.4 Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;

7.2.4.8.5 Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;

7.2.4.8.6 Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits);

7.2.4.8.8 Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;

7.2.4.8.9 A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;

7.2.4.8.10 A análise de links em sand-box deve deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

7.2.4.8.11 Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.8.12 O sistema de análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);

7.2.4.8.13 O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;

7.2.4.8.14 Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

7.2.4.8.15 Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

7.2.4.8.16 Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

7.2.4.8.17 Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.

7.2.4.8.18 Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;

7.2.4.8.19 Caso seja necessário licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

7.2.4.8.20 Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

7.2.4.8.21 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs MacOS (mach-O, DMG e PKG) no ambiente de sandbox;

7.2.4.8.22 Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.8.23 Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

7.2.4.8.24 Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;

7.2.4.9 FILTRO DE URL

7.2.4.9.1 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

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

7.2.4.9.3 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança

7.2.4.9.4 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.

7.2.4.9.5 Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

7.2.4.9.6 Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

7.2.4.9.7 Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;

7.2.4.9.8 Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

7.2.4.9.9 Possui pelo menos 60 categorias de URLs;

7.2.4.9.10 A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;

7.2.4.9.11 Suporta a criação categorias de URLs customizadas;

7.2.4.9.12 Suporta a exclusão de URLs do bloqueio, por categoria;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.9.13 Permite a customização de página de bloqueio;

7.2.4.9.14 Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;

7.2.4.9.5 Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credencias em sites classificados como phishing pelo filtro de URL da solução;

7.2.4.9.6 Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);

7.2.4.9.7 Suporta a inclusão nos logs do produto de informações das atividades dos usuários;

7.2.4.9.8 Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

7.2.4.10 IDENTIFICAÇÃO DE USUÁRIOS

7.2.4.10.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;

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

7.2.4.10.3 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

7.2.4.10.4 Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.10.5 Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

7.2.4.10.6 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;

7.2.4.10.7 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

7.2.4.10.8 Suporte a autenticação Kerberos;

7.2.4.10.9 Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;

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

7.2.4.10.11 Deve identificar usuários através de leitura do campo x-forwarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

7.2.4.10.12 Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-forwarded-for;

7.2.4.10.13 O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos à organização;

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

7.2.4.10.15 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.11 QOS

7.2.4.11.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

7.2.4.11.2 Suportar a criação de políticas de QoS por:

7.2.4.11.3 Endereço de origem

7.2.4.11.4 Endereço de destino

7.2.4.11.5 Por usuário e grupo do LDAP/AD.

7.2.4.11.6 Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

7.2.4.11.7 Por porta;

7.2.4.11.8 O QoS deve possibilitar a definição de classes por:

7.2.4.11.9 Banda Garantida

7.2.4.11.10 Banda Máxima

7.2.4.11.11 Fila de Prioridade.

7.2.4.11.12 Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

7.2.4.11.13 Suportar marcação de pacotes Diffserv, inclusive por aplicação;

7.2.4.11.14 Deve implementar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inbound e outbound);

7.2.4.11.15 Disponibilizar estatísticas RealTime para classes de QoS.

7.2.4.11.16 Deve suportar QOS (traffic-shapping), em interface agregadas;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

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

7.2.4.12 FILTRO DE DADOS

7.2.4.12.1 Permite a criação de filtros para arquivos e dados pré-definidos;

7.2.4.12.2 Os arquivos devem ser identificados por extensão e assinaturas;

7.2.4.12.3 Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);

7.2.4.12.4 Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

7.2.4.12.5 Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

7.2.4.12.6 Permitir listar o número de aplicações suportadas para controle de dados;

7.2.4.12.7 Permitir listar o número de tipos de arquivos suportados para controle de dados;

7.2.4.13 GEO-LOCALIZAÇÃO

7.2.7.13.1 Suportar a criação de políticas por Geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados.

7.2.4.13.2 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

7.2.4.13.3 Deve permitir visualizar nos logs e criar políticas para liberar e bloquear tráfego de países por: tipo de arquivo, aplicação e categoria de URL;

7.2.4.13.4 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

7.2.4.14 VPN

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



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.14.2 Suportar IPSec VPN;

7.2.4.14.3 Suportar SSL VPN;

7.2.4.14.4 A VPN IPSEc deve suportar:

7.2.4.14.5 DES e 3DES;

7.2.4.14.6 Autenticação MD5 e SHA-1;

7.2.4.14.7 Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;

7.2.4.14.8 Algoritmo Internet Key Exchange (IKEv1 e v2);

7.2.4.14.9 AES 128, 192 e 256 (Advanced Encryption Standard)

7.2.4.14.10 Autenticação via certificado IKE PKI.

7.2.4.14.11 Deve possuir interoperabilidade com os seguintes fabricantes:

a) Cisco;

b) Checkpoint;

c) Juniper;

d) Palo Alto Networks;

e) Fortinet;

f) Sonic Wall;

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

7.2.4.14.13 A VPN SSL deve suportar:

7.2.4.14.14 SD-WAN avançado com medição ativa

7.2.4.14.15 Automação por IA



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.14.16 Segmentação baseada em identidade (Identity-based segmentation)

7.2.4.14.17 Suporte a IPv6 avançado (NAT64/DNS64/Teredo/6RD)

7.2.4.14.18 Dynamic Multicast NAT

7.2.4.14.19 Fabric Connector

7.2.4.14.20 O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

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

7.2.4.14.22 Atribuição de endereço IP nos clientes remotos de VPN SSL;

7.2.4.14.23 Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;

7.2.4.14.24 SSL-VPN com autenticação reforçada (SAML, Azure AD, MFA, FIDO2)

7.2.4.14.25 Suporte a IPsec com aceleração ASIC

7.2.4.14.26 Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;

7.2.4.14.27 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

7.2.4.14.28 Atribuição de DNS nos clientes remotos de VPN;

7.2.4.14.29 Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);

7.2.4.14.30 A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;

Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.14.31 Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;

7.2.4.14.32 Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;

7.2.4.14.33 Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;

7.2.4.14.34 Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

7.2.4.14.35 A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;

7.2.4.14.36 Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

7.2.4.14.37 Deve permitir a distribuição de certificado para o usuário remoto através do portal de VPN de forma automatizada;

7.2.4.14.38 Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;

7.2.4.14.39 Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;

7.2.4.14.40 Suporta leitura e verificação de CRL (certificate revocation list);

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

7.2.4.14.42 O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;

7.2.4.14.43 O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.14.44 Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

7.2.4.14.45 Antes do usuário autenticar na estação;

7.2.4.14.46 Após autenticação do usuário na estação;

7.2.4.14.47 Sob demanda do usuário;

7.2.4.14.48 Deverá manter uma conexão segura com o portal durante a sessão.

7.2.4.14.49 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OSx e Chrome OS;

7.2.4.14.50 O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;

7.2.4.14.51 Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;

7.2.4.14.52 Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;

7.2.4.15 CONSOLE DE GERÊNCIA E MONITORAÇÃO

7.2.4.15.1 Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

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

7.2.4.15.3 Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;

7.2.4.15.4 Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;

7.2.4.15.5 O gerenciamento deve permitir/possuir:

a) Criação e administração de políticas de firewall e controle de aplicação;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- b) Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- c) Criação e administração de políticas de Filtro de URL;
- d) Monitoração de logs;
- e) Ferramentas de investigação de logs;
- f) Debugging;
- g) Captura de pacotes.
- h) Acesso concorrente de administradores;

7.2.4.15.6 Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;

7.2.4.15.7 Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.

7.2.4.15.8 Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;

7.2.4.15.9 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

7.2.4.15.10 Deve permitir usar palavras chaves e cores para facilitar a identificação de regras;

7.2.4.15.11 Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;

7.2.4.15.12 Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.15.13 Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

7.2.4.15.14 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

7.2.4.15.15 Autenticação integrada ao Microsoft Active Directory e servidor Radius;

7.2.4.15.16 Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

7.2.4.15.17 Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

7.2.4.15.18 Criação de regras que fiquem ativas em horário definido;

7.2.4.15.19 Criação de regras com data de expiração;

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

7.2.4.15.21 Suportar Rollback de Sistema Operacional para a última versão local;

7.2.4.15.22 Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

7.2.4.15.23 Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;

7.2.4.15.24 Validação de regras antes da aplicação;

7.2.4.15.25 Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.

7.2.4.15.26 É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.15.27 Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

7.2.4.15.28 É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

7.2.4.15.29 Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.

7.2.4.15.30 Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)

7.2.4.15.31 Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

7.2.4.15.32 Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

7.2.4.15.33 Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;

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

7.2.4.15.35 Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day" detectados em sand-box e tráfego bloqueado;

7.2.4.15.36 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

7.2.4.15.37 Deve permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela.

7.2.4.15.38 Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.15.39 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;

7.2.4.15.40 Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

7.2.4.15.41 Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;

7.2.4.15.42 Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;

7.2.4.15.43 Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;

7.2.4.15.44 Deve ser possível exportar os logs em CSV;

7.2.4.15.45 Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.
Rotação do log;

7.2.4.15.46 Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

7.2.4.15.47 Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;

7.2.4.15.48 Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

7.2.4.15.49 Situação do dispositivo e do cluster;

7.2.4.15.50 Principais aplicações;

7.2.4.15.51 Principais aplicações por risco;

7.2.4.15.52 Administradores autenticados na gerência da plataforma de segurança;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.4.15.53 Número de sessões simultâneas;

7.2.4.15.54 Status das interfaces; 7.2.4.15.55

Uso de CPU;

7.2.4.15.56 Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

7.2.4.15.57 Resumo gráfico de aplicações utilizadas;

7.2.4.15.58 Principais aplicações por utilização de largura de banda de entrada e saída;

7.2.4.15.59 Principais aplicações por taxa de transferência de bytes;

7.2.4.15.60 Principais hosts por número de ameaças identificadas;

7.2.4.15.61 Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;

7.2.4.15.62 Deve permitir a criação de relatórios personalizados;

7.2.7.15.63 Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

7.2.4.15.64 Gerar alertas automáticos via:

- a) Email;
- b) SNMP;
- c) Syslog;

7.2.4.15.65 A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.5.5. Tipo 5 - Solução NGFW - (Ponta “B” – CIRETRAN A)

7.2.5.1 ESPECIFICAÇÃO TÉCNICA

7.2.5.1.1. HARDWARE E PERFORMANCE

7.2.5.1.1. Appliance NGFW físico dedicado;

7.2.5.1.2. Throughput de Firewall de, no mínimo, 38 Gbps;

7.2.5.1.3. Throughput de IPS de, no mínimo, 5 Gbps;

7.2.5.1.4. Throughput de NGFW (Firewall + IPS + Application Control) de, no mínimo, 3 Gbps;

7.2.5.1.5. Throughput de Threat Prevention (Firewall + IPS + App Control + Malware) de, no mínimo, 2.8 Gbps;

7.2.5.1.6. Throughput de VPN IPSec de, no mínimo, 30 Gbps;

7.2.5.1.7. Suportar, no mínimo, 2.000 túneis de VPN IPSEC Site-to-Site simultâneos;

7.2.5.1.8. Suportar, no mínimo, 3.000.000 (três milhões) de conexões simultâneas;

7.2.5.1.9. Suporte a, no mínimo, 250.000 novas conexões por segundo;

7.2.5.1.10. Suportar no mínimo 3 Gbps de throughput de Inspeção SSL;

7.2.5.1.11. Possuir no mínimo 16 (dezesesseis) interfaces 1 GE RJ45 integradas ao chassi;

7.2.5.1.12. Possuir no mínimo 4 (quatro) interfaces 10 GE SFP+ integradas ao chassi;

7.2.5.1.13. Possuir porta de gerência dedicada (RJ45) e porta USB para recuperação de sistema;

7.2.5.1.14. Possuir fonte de alimentação interna dupla e redundante;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.5.1.15. O equipamento deve ser montável em rack padrão 19”, acompanhando os kits de fixação (orelhas/trilhos);

7.2.5.1.16. (Opcional - *Apenas se for o modelo 121G*) Possuir armazenamento interno SSD de no mínimo 480GB. *[Nota: O modelo 120G padrão não tem disco interno para logs, se quiser o 120G padrão, remova este item ou aceite logs em nuvem/gerência externa];*

7.2.5.2 FUNCIONALIDADES GERAIS E SISTEMA OPERACIONAL

7.2.5.2.1 A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), SD-WAN seguro e gerenciamento unificado;

7.2.5.2.2 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

7.2.5.2.3 O software deverá ser fornecido em sua versão mais atualizada e estável;

7.2.5.2.4 Suporte a Alta Disponibilidade (HA) nos modos Ativo-Passivo e Ativo-Ativo, com monitoramento de falha de link e sessão;

7.2.5.2.5 Interface de gerenciamento gráfica (Web GUI) intuitiva em português e Interface de Linha de Comando (CLI) completa;

7.2.5.2.6 Suporte a SNMPv2c, SNMPv3 e envio de logs via Syslog (TLS);

7.2.5.2.7 Suporte a Netflow ou sFlow;

7.2.5.2.8 Firewall Stateful com inspeção profunda de pacotes (DPI);

7.2.5.3 REDE E CONECTIVIDADE

7.2.5.3.1 Suporte total a IPv4 e IPv6 (Dual Stack);

7.2.5.3.2 Suporte a tunelamento IPv6 (6in4, 6to4, 4in6);

7.2.5.3.3 Suporte a roteamento Estático e Dinâmico (RIP, OSPFv2/v3, BGP4/BGP4+);

7.2.5.3.4 Suporte a Multicast (PIM-SM, PIM-DM, IGMP);

7.2.5.3.5 Suporte a 802.1Q (VLANs) e Link Aggregation (802.3ad / LACP);



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.5.3.6 Funcionalidade de Servidor DHCP, Cliente DHCP, DHCP Relay e DHCPv6 Prefix Delegation;

7.2.5.3.7 Suporte a Jumbo Frames nas interfaces;

7.2.5.3.8 Traffic Shaping (QoS) granular por política, aplicação, usuário ou interface (garantia de banda, limite máximo e priorização);

7.2.5.4 SD-WAN (SOFTWARE DEFINED WAN)

7.2.5.4.1 Funcionalidade de SD-WAN nativa integrada ao sistema operacional, sem necessidade de hardware ou licença adicional específica;

7.2.5.4.2 Balanceamento de links WAN baseado em algoritmos como: Source IP, Source-Destination IP, Spillover, Usage (Bandwidth) e medição de qualidade (SLA);

7.2.5.4.3 Monitoramento de saúde dos links (Health Check) em tempo real medindo Latência, Jitter e Packet Loss;

7.2.5.4.4 Capacidade de direcionar aplicações específicas (ex: Office365, Voz, Zoom) por links específicos baseados no SLA medido;

7.2.5.4.5 Suporte a FEC (Forward Error Correction) para otimização de tráfego em links instáveis;

7.2.5.5 PREVENÇÃO DE AMEAÇAS E SEGURANÇA

7.2.5.5.1 Controle de Aplicações: Capacidade de identificar e controlar mais de 3.000 aplicações, independente da porta ou protocolo (Camada 7), incluindo tráfego criptografado (SSL/TLS);

7.2.5.5.2 IPS (Intrusion Prevention System): Proteção baseada em assinatura e anomalia, com atualização automática de vacinas, permitindo bloqueio de exploits conhecidos e ataques de DoS/DDoS;

7.2.5.5.3 Antivírus/Anti-Malware: Inspeção de fluxo em tempo real contra vírus, spyware, ransomware e malwares, com suporte a inspeção SSL;

7.2.5.5.4 Filtro Web (Web Filtering): Classificação de URLs em categorias (mínimo 70 categorias), permitindo bloqueio por categoria, URL específica, coringa (*) e reputação;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.5.5.5 Sandboxing: Suporte a envio de arquivos suspeitos para análise em Sandbox (em nuvem ou on-premise) para detecção de Zero-Day (pode exigir licença específica);

7.2.5.5.6 Inspeção SSL/TLS: Capacidade de decryptar tráfego HTTPS (TLS 1.3) para inspeção de ameaças com alto desempenho, utilizando aceleração por hardware (ASIC);

7.2.5.6 VPN E ACESSO REMOTO

7.2.5.6.1 Suporte nativo a VPN IPSEC (Site-to-Site) e VPN SSL (Remote Access);

7.2.5.6.2 Cliente de VPN gratuito para instalação em estações de trabalho (Windows, MacOS, Linux, Android, iOS);

7.2.5.6.3 Suporte a autenticação de dois fatores (MFA/2FA) integrado (via Token físico, App ou E-mail);

7.2.5.6.4 Portal Web para VPN SSL (Clientless) para acesso a serviços internos via navegador;

7.2.5.6.5 Integração com AD/LDAP, Radius e Azure AD para autenticação de usuários de VPN;

7.2.5.7 IDENTIDADE E INTEGRAÇÃO

7.2.5.7.1 Identificação de usuários integrada ao Active Directory (AD) de forma transparente (FSSO) sem necessidade de instalar agentes em todas as estações;

7.2.5.7.2 Suporte a criação de regras baseadas em usuários e grupos do AD, e não apenas IPs;

7.2.5.7.3 Recurso de Captive Portal para autenticação de convidados;

7.2.5.7.4 (Opcional - ZTNA) Suporte a Zero Trust Network Access (ZTNA) integrado ao firewall.

7.2.5.7.5 O equipamento deve possuir arquitetura baseada em Processadores de Segurança Dedicados (ASIC) de 5ª Geração (SP5 ou equivalente)

7.2.5.7.6 O hardware deve possuir aceleração nativa via ASIC para inspeção de tráfego criptografado (SSL/TLS 1.3), garantindo baixa latência sem sobrecarregar a CPU de gerenciamento.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.5.7.7 O chipset de aceleração deve suportar VXLAN hardware acceleration, permitindo o processamento de túneis VXLAN com performance próxima a *wire-speed*.

7.2.5.7.8 O equipamento deve suportar a identificação e aceleração de 'Elephant Flows' via hardware, garantindo que conexões de longa duração e alto volume não impactem a performance de novas conexões.

7.5.6. Tipo 6 - Solução NGFW - (Ponta “B” – CIRETRAN B, POSTOS/SUB REDE)

7.2.5.1 ESPECIFICAÇÃO TÉCNICA

7.2.6.1.1. HARDWARE E PERFORMANCE

7.2.5.6.1.1. Appliance NGFW físico dedicado;

7.2.6.1.2. Throughput de Firewall de, no mínimo, 38 Gbps;

7.2.6.1.3. Throughput de IPS de, no mínimo, 5 Gbps;

7.2.6.1.4. Throughput de NGFW (Firewall + IPS + Application Control) de, no mínimo, 3 Gbps;

7.2.6.1.5. Throughput de Threat Prevention (Firewall + IPS + App Control + Malware) de, no mínimo, 2.8 Gbps;

7.2.6.1.6. Throughput de VPN IPsec de, no mínimo, 30 Gbps;

7.2.6.1.7. Suportar, no mínimo, 2.000 túneis de VPN IPSEC Site-to-Site simultâneos;

7.2.6.1.8. Suportar, no mínimo, 3.000.000 (três milhões) de conexões simultâneas;

7.2.6.1.9. Suporte a, no mínimo, 250.000 novas conexões por segundo;

7.2.6.1.10. Suportar no mínimo 3 Gbps de throughput de Inspeção SSL;

7.2.6.1.11. Possuir no mínimo 16 (dezesesseis) interfaces 1 GE RJ45 integradas ao chassi;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.6.1.12. Possuir no mínimo 4 (quatro) interfaces 10 GE SFP+ integradas ao chassi;

7.2.6.1.13. Possuir porta de gerência dedicada (RJ45) e porta USB para recuperação de sistema;

7.2.6.1.14. Possuir fonte de alimentação interna dupla e redundante;

7.2.6.1.15. O equipamento deve ser montável em rack padrão 19", acompanhando os kits de fixação (orelhas/trilhos);

7.2.6.1.16. (Opcional - *Apenas se for o modelo 121G*) Possuir armazenamento interno SSD de no mínimo 480GB. *[Nota: O modelo 120G padrão não tem disco interno para logs, se quiser o 120G padrão, remova este item ou aceite logs em nuvem/gerência externa];*

7.2.6.2 FUNCIONALIDADES GERAIS E SISTEMA OPERACIONAL

7.2.6.2.1 A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), SD-WAN seguro e gerenciamento unificado;

7.2.6.2.2 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

7.2.6.2.3 O software deverá ser fornecido em sua versão mais atualizada e estável;

7.2.6.2.4 Suporte a Alta Disponibilidade (HA) nos modos Ativo-Passivo e Ativo-Ativo, com monitoramento de falha de link e sessão;

7.2.6.2.5 Interface de gerenciamento gráfica (Web GUI) intuitiva em português e Interface de Linha de Comando (CLI) completa;

7.2.6.2.6 Suporte a SNMPv2c, SNMPv3 e envio de logs via Syslog (TLS);

7.2.6.2.7 Suporte a Netflow ou sFlow;

7.2.6.2.8 Firewall Stateful com inspeção profunda de pacotes (DPI);

7.2.6.3 REDE E CONECTIVIDADE

7.2.6.3.1 Suporte total a IPv4 e IPv6 (Dual Stack);



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.6.3.2 Suporte a tunelamento IPv6 (6in4, 6to4, 4in6);

7.2.6.3.3 Suporte a roteamento Estático e Dinâmico (RIP, OSPFv2/v3, BGP4/BGP4+);

7.2.6.3.4 Suporte a Multicast (PIM-SM, PIM-DM, IGMP);

7.2.6.3.5 Suporte a 802.1Q (VLANs) e Link Aggregation (802.3ad / LACP);

7.2.6.3.6 Funcionalidade de Servidor DHCP, Cliente DHCP, DHCP Relay e DHCPv6 Prefix Delegation;

7.2.6.3.7 Suporte a Jumbo Frames nas interfaces;

7.2.6.3.8 Traffic Shaping (QoS) granular por política, aplicação, usuário ou interface (garantia de banda, limite máximo e priorização);

7.2.6.4 SD-WAN (SOFTWARE DEFINED WAN)

7.2.6.4.1 Funcionalidade de SD-WAN nativa integrada ao sistema operacional, sem necessidade de hardware ou licença adicional específica;

7.2.6.4.2 Balanceamento de links WAN baseado em algoritmos como: Source IP, Source-Destination IP, Spillover, Usage (Bandwidth) e medição de qualidade (SLA);

7.2.6.4.3 Monitoramento de saúde dos links (Health Check) em tempo real medindo Latência, Jitter e Packet Loss;

7.2.6.4.4 Capacidade de direcionar aplicações específicas (ex: Office365, Voz, Zoom) por links específicos baseados no SLA medido;

7.2.6.4.5 Suporte a FEC (Forward Error Correction) para otimização de tráfego em links instáveis;

7.2.6.5 PREVENÇÃO DE AMEAÇAS E SEGURANÇA

7.2.6.5.1 Controle de Aplicações: Capacidade de identificar e controlar mais de 3.000 aplicações, independente da porta ou protocolo (Camada 7), incluindo tráfego criptografado (SSL/TLS);

7.2.6.5.2 IPS (Intrusion Prevention System): Proteção baseada em assinatura e anomalia, com atualização automática de vacinas, permitindo bloqueio de exploits conhecidos e ataques de DoS/DDoS;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.6.5.3 Antivírus/Anti-Malware: Inspeção de fluxo em tempo real contra vírus, spyware, ransomware e malwares, com suporte a inspeção SSL;

7.2.6.5.4 Filtro Web (Web Filtering): Classificação de URLs em categorias (mínimo 70 categorias), permitindo bloqueio por categoria, URL específica, coringa (*) e reputação;

7.2.6.5.5 Sandboxing: Suporte a envio de arquivos suspeitos para análise em Sandbox (em nuvem ou on-premise) para detecção de Zero-Day (pode exigir licença específica);

7.2.6.5.6 Inspeção SSL/TLS: Capacidade de decriptar tráfego HTTPS (TLS 1.3) para inspeção de ameaças com alto desempenho, utilizando aceleração por hardware (ASIC);

7.2.6.6 VPN E ACESSO REMOTO

7.2.6.6.1 Suporte nativo a VPN IPSEC (Site-to-Site) e VPN SSL (Remote Access);

7.2.6.6.2 Cliente de VPN gratuito para instalação em estações de trabalho (Windows, MacOS, Linux, Android, iOS);

7.2.6.6.3 Suporte a autenticação de dois fatores (MFA/2FA) integrado (via Token físico, App ou E-mail);

7.2.6.6.4 Portal Web para VPN SSL (Clientless) para acesso a serviços internos via navegador;

7.2.6.6.5 Integração com AD/LDAP, Radius e Azure AD para autenticação de usuários de VPN;

7.2.6.7 IDENTIDADE E INTEGRAÇÃO

7.2.6.7.1 Identificação de usuários integrada ao Active Directory (AD) de forma transparente (FSSO) sem necessidade de instalar agentes em todas as estações;

7.2.6.7.2 Suporte a criação de regras baseadas em usuários e grupos do AD, e não apenas IPs;

7.2.6.7.3 Recurso de Captive Portal para autenticação de convidados;

7.2.6.7.4 (Opcional - ZTNA) Suporte a Zero Trust Network Access (ZTNA) integrado ao firewall.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.6.7.5 O equipamento deve possuir arquitetura baseada em Processadores de Segurança Dedicados (ASIC) de 5ª Geração (SP5 ou equivalente)

7.2.6.7.6 O hardware deve possuir aceleração nativa via ASIC para inspeção de tráfego criptografado (SSL/TLS 1.3), garantindo baixa latência sem sobrecarregar a CPU de gerenciamento.

7.2.6.7.7 O chipset de aceleração deve suportar VXLAN hardware acceleration, permitindo o processamento de túneis VXLAN com performance próxima a *wire-speed*.

7.2.6.7.8 O equipamento deve suportar a identificação e aceleração de 'Elephant Flows' via hardware, garantindo que conexões de longa duração e alto volume não impactem a performance de novas conexões.

7.5.7. Tipo 7 - Solução NGFW - (Ponta “A” – DETRAN/SEDE - INTERNET)

7.2.7.1 Solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares “Zero Day”, Filtro de URL, bem como controle de transmissão de dados e acesso a internet compondo uma plataforma de segurança integrada e robusta;

7.2.7.2 Por plataforma de segurança entende-se hardware e software integrados do tipo appliance;

7.2.7.3 Especificações Mínimas

7.2.7.3.1 A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento:

7.2.7.3.2 Throughput de 17 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

7.2.7.3.3 Throughput de 8.5 Gbps com as seguintes funcionalidade habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.3.4 Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como o atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos às sanções previstas em lei;

7.2.7.3.5 Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend);

7.2.7.3.6 Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até a camada 4.

7.2.7.3.7 Trusted Platform Module (TPM) 2.0

7.2.7.3.8 Suporte a, no mínimo, 3.800.000 de conexões simultâneas;

7.2.7.3.9 Suporte a, no mínimo, 110.000 novas conexões HTTP por segundo;

7.2.7.3.10 Fonte 120/240 AC

7.2.7.3.11 Redundância total de PSU hot-swappable

7.2.7.3.12 Disco Solid State Drive (SSD) redundante de, no mínimo, 480 GB.

7.2.7.3.13 No mínimo, 04 (quatro) interfaces de rede 1 Gbps em portas cobre;

7.2.7.3.14 No mínimo, 08 (oito) interfaces de rede 1 Gbps SFP / rede 10 Gbps SFP+

7.2.7.3.15 No mínimo, 04 (quatro) interfaces de rede 25 Gbps SFP28;

7.2.7.3.16 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;

7.2.7.3.17 1 (uma) interface do tipo console ou similar;

7.2.7.3.18 Estar licenciada para ou suportar sem o uso de licença, 10.000 (dez mil) clientes de VPN SSL simultâneos;

7.2.7.3.19 Estar licenciada para ou suportar sem o uso de licença, 3.000 (três mil) túneis de VPN IPSEC simultâneos;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.3.20 Deve suportar, no mínimo, 10 sistemas virtuais lógicos (Contextos) no firewall Físico;

7.2.7.3.21 Deve suportar DSPs e NPUs (Processadores de Segurança)

7.2.7.3.21 Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;

7.2.7.3.22 Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

7.2.7.3.23 Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;

7.2.7.3.24 A console de gerência e monitoração podem residir no mesmo appliance de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função;

7.2.7.3.25 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.

7.2.7.4 CARACTERÍSTICAS GERAIS

7.2.7.4.1 A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

7.2.7.4.2 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

7.2.7.4.3 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;

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

7.2.7.4.5 O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

7.2.7.4.6 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

7.2.7.4.7 O software deverá ser fornecido em sua versão mais atualizada, e manter atualizado e devidamente licenciado até o término do contrato.

7.2.7.4.8 Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

7.2.7.4.9 Suporte a 4094 VLAN Tags 802.1q;

7.2.7.4.10 Agregação de links 802.3ad e LACP;

7.2.7.4.11 Policy based routing ou policy based forwarding;

7.2.7.4.12 Roteamento multicast (PIM-SM);

7.2.7.4.13 DHCP Relay;

7.2.7.4.14 DHCP Server;

7.2.7.4.15 Jumbo Frames;

7.2.7.4.16 Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;

7.2.7.4.17 Suportar sub-interfaces ethernet lógicas;

7.2.7.4.18 Suporte a, no mínimo, 15 (quinze) roteadores virtuais na mesma instância de firewall;

7.2.7.4.19 O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;

7.2.7.4.20 Deve suportar os seguintes tipos de NAT:

7.2.7.4.21 Nat dinâmico (Many-to-1);



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.7.4.22 Nat dinâmico (Many-to-Many);
- 7.2.7.4.23 Nat estático (1-to-1);
- 7.2.7.4.24 NAT estático (Many-to-Many);
- 7.2.7.4.25 Nat estático bidirecional 1-to-1;
- 7.2.7.4.26 Tradução de porta (PAT);
- 7.2.7.4.27 NAT de Origem;
- 7.2.7.4.28 NAT de Destino;
- 7.2.7.4.29 Suportar NAT de Origem e NAT de Destino simultaneamente;
- 7.2.7.4.30 Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;
- 7.2.7.4.31 Deve implementar o protocolo ECMP;
- 7.2.7.4.32 Deve implementar balanceamento de link por hash do IP de origem;
- 7.2.7.4.33 Deve implementar balanceamento de link por hash do IP de origem e destino;
- 7.2.7.4.34 Deve implementar balanceamento de link através do método round-robin;
- 7.2.7.4.35 Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quatro links;
- 7.2.7.4.36 Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;
- 7.2.7.4.37 Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;
- 7.2.7.4.38 Deve implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;

7.2.7.4.39 Enviar log para sistemas de monitoração externos, simultaneamente;

7.2.7.4.40 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

7.2.7.4.41 Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

7.2.7.4.42 Proteção contra anti-spoofing;

7.2.7.4.43 Deve permitir bloquear sessões TCP que usem variações do 3-way handshake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;

7.2.7.4.44 Dever permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;

7.2.7.4.45 Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;

7.2.7.4.46 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

7.2.7.4.47 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

7.2.7.4.48 Suportar a OSPF graceful restart;

7.2.7.4.49 Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;

7.2.7.4.50 Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPsec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPsec, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNS), DNS Search List (DNSSL) e controle de aplicação;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.4.51 Os dispositivos de proteção devem 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);

7.2.7.4.52 Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

7.2.7.4.53 Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

7.2.7.4.54 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;

7.2.7.4.55 Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

7.2.7.4.56 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

c) Em modo transparente;

d) Em layer 3;

7.2.7.4.57 A configuração em alta disponibilidade deve sincronizar:

g) Sessões;

h) Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

i) Certificados de-criptografados;

j) Associações de Segurança das VPNs;

k) Tabelas FIB;

l) O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

7.2.7.4.58 As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

7.2.7.5 CONTROLE POR POLÍTICA DE FIREWALL

7.2.7.5.1 ZTNA embutido (Zero Trust Network Access)

7.2.7.5.2 Inline CASB (Cloud Access Security Broker)

7.2.7.5.3 FWaaS / SASE-ready

7.2.7.5.4 Inspeção SSL/TLS suportando TLS 1.3 por hardware

7.2.7.5.5 IPS com ML (Machine Learning) em tempo real

7.2.7.5.6 Antivírus com Deep Learning

7.2.7.5.7 Anti-botnet

7.2.7.5.8 DNS Security incrustado

7.2.7.5.9 Deverá suportar controles por zona de segurança.

7.2.7.5.10 Controles de políticas por porta e protocolo.

7.2.7.5.11 Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

7.2.7.5.12 Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

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

7.2.7.5.14 Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;

7.2.7.5.15 Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;

7.2.7.5.16 Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.5.17 Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).

7.2.7.5.18 Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

7.2.7.5.19 Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

7.2.7.5.20 Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);

7.2.7.5.21 Controle de inspeção e de-criptografia de SSH por política;

7.2.7.5.22 A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

7.2.7.5.23 A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);

7.2.7.5.24 É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise.

7.2.7.5.25 Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)

7.2.7.5.26 QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.

7.2.7.5.27 Suporte a objetos e regras IPV6.

7.2.7.5.28 Suporte a objetos e regras multicast.

7.2.7.5.29 Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.5.30 Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

7.2.7.6 CONTROLE DE APLICAÇÕES

7.2.7.6.1 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

7.2.7.6.2 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

7.2.7.6.3 Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

7.2.7.6.4 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;

7.2.7.6.5 Deve inspecionar o payload do pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;
Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

7.2.7.6.6 Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.

7.2.7.6.7 GUI moderna com dashboard em tempo real em HTML5

7.2.7.6.8 Cloud Management

7.2.7.6.9 Fabric View – mapa automático da rede



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.6.10 Análises de risco de configuração (Security Rating)

7.2.7.6.11 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

7.2.7.6.12 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivos dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

7.2.7.6.13 Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

7.2.7.6.14 Identificar o uso de táticas evasivas via comunicações criptografadas;

7.2.7.6.15 Atualizar a base de assinaturas de aplicações automaticamente;

7.2.7.6.16 Automação nativa

7.2.7.6.17 Automation Stitches

7.2.7.6.18 Threat Intelligence local + global

7.2.7.6.19 Reconhecer aplicações em IPv6;

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

7.2.7.6.21 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

7.2.7.6.22 Deve ser possível 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;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.6.23 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

7.2.7.6.24 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

7.2.7.6.25 Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

7.2.7.6.26 A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:

b) HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.

7.2.7.6.27 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

7.2.7.6.28 Deve alertar o usuário quando uma aplicação for bloqueada;

7.2.7.6.29 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

7.2.7.6.30 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;

7.2.7.6.31 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos;

7.2.7.6.32 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;

7.2.7.6.33 Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.6.34 Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

7.2.7.6.35 Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc).

7.2.7.6.36 Nível de risco da aplicação.

7.2.7.6.37 IoT Detection

7.2.7.6.38 Perfilamento dinâmico

7.2.7.6.39 Application Metadata & Behavior Analysis

7.2.7.6.40 Categoria e sub-categoria de aplicações.

7.2.7.6.41 Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

7.2.7.7 PREVENÇÃO DE AMEAÇAS

7.2.7.7.1 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante.

7.2.7.7.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

7.2.7.7.3 As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

7.2.7.7.4 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

7.2.7.7.5 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Antipyyware e Antivirus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.7.6 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

7.2.7.7.7 Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

7.2.7.7.8 Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware , possibilitando a criação de diferentes

7.2.7.7.9 Políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

7.2.7.7.10 Deve permitir o bloqueio de vulnerabilidades.

7.2.7.7.11 Deve permitir o bloqueio de exploits conhecidos.

7.2.7.7.12 Deve incluir proteção contra ataques de negação de serviços.

7.2.7.7.13 Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE;

7.2.7.7.14 Deverá possuir os seguintes mecanismos de inspeção de IPS:

7.2.7.7.15 Análise de padrões de estado de conexões;

7.2.7.7.16 Análise de decodificação de protocolo;

7.2.7.7.17 Análise para detecção de anomalias de protocolo;

7.2.7.7.18 Análise heurística;

7.2.7.7.19 IP Defragmentation;

7.2.7.7.20 Remontagem de pacotes de TCP;

7.2.7.7.21 Bloqueio de pacotes malformados.

7.2.7.7.22 Ser imune e ter a capacidade de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;

7.2.7.7.23 Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.7.24 Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

7.2.7.7.25 Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

7.2.7.7.26 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

7.2.7.7.27 Possuir assinaturas para bloqueio de ataques de buffer overflow;

7.2.7.7.28 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

7.2.7.7.29 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

7.2.7.7.30 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

7.2.7.7.31 É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;

7.2.7.7.32 Suportar bloqueio de arquivos por tipo;

7.2.7.7.33 Identificar e bloquear comunicação com botnets;

7.2.7.7.34 Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

7.2.7.7.35 Deve suportar referência cruzada com CVE;

7.2.7.7.36 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

7.2.7.7.37 O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.7.38 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antispyware;

7.2.7.7.39 Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;

7.2.7.7.40 Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

7.2.7.7.41 Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

7.2.7.7.42 Os eventos devem identificar o país de onde partiu a ameaça;

7.2.7.7.43 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

7.2.7.7.44 Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos.

7.2.7.7.45 Rastreamento de vírus em pdf.

7.2.7.7.46 Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)

7.2.7.7.47 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada regra de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

7.2.7.8 ANÁLISE DE MALWARES MODERNOS

7.2.7.8.1 Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada deve possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.8.2 O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

7.2.7.8.3 Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

7.2.7.8.4 Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;

7.2.7.8.5 Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;

7.2.7.8.6 Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits);

7.2.7.8.8 Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;

7.2.7.8.9 A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;

7.2.7.8.10 A análise de links em sand-box deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

7.2.7.8.11 Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;

7.2.7.8.12 O sistema de análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);

7.2.7.8.13 O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;

7.2.7.8.14 Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

7.2.7.8.15 Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

7.2.7.8.16 Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

7.2.7.8.17 Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.

7.2.7.8.18 Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;

7.2.7.8.19 Caso seja necessário licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

7.2.7.8.20 Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

7.2.7.8.21 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs MacOS (mach-O, DMG e PKG) no ambiente de sandbox;

7.2.7.8.22 Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos;

7.2.7.8.23 Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

7.2.7.8.24 Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.9 FILTRO DE URL

7.2.7.9.1 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

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

7.2.7.9.3 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança

7.2.7.9.4 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.

7.2.7.9.5 Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

7.2.7.9.6 Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

7.2.7.9.7 Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;

7.2.7.9.8 Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

7.2.7.9.9 Possui pelo menos 60 categorias de URLs;

7.2.7.9.10 A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;

7.2.7.9.11 Suporta a criação categorias de URLs customizadas;

7.2.7.9.12 Suporta a exclusão de URLs do bloqueio, por categoria;

7.2.7.9.13 Permite a customização de página de bloqueio;

7.2.7.9.14 Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Directory só possam enviar informações de login para sites autorizados na solução;

7.2.7.9.5 Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;

7.2.7.9.6 Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);

7.2.7.9.7 Suporta a inclusão nos logs do produto de informações das atividades dos usuários;

7.2.7.9.8 Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

7.2.7.10 IDENTIFICAÇÃO DE USUÁRIOS

7.2.7.10.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;

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

7.2.7.10.3 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

7.2.7.10.4 Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;

7.2.7.10.5 Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.10.6 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;

7.2.7.10.7 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

7.2.7.10.8 Suporte a autenticação Kerberos;

7.2.7.10.9 Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;

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

7.2.7.10.11 Deve identificar usuários através de leitura do campo x-forwarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

7.2.7.10.12 Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-forwarded-for;

7.2.7.10.13 O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos à organização;

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

7.2.7.10.15 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

7.2.7.11 QOS

7.2.7.11.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

7.2.7.11.2 Suportar a criação de políticas de QoS por:

7.2.7.11.3 Endereço de origem

7.2.7.11.4 Endereço de destino

7.2.7.11.5 Por usuário e grupo do LDAP/AD.

7.2.7.11.6 Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

7.2.7.11.7 Por porta;

7.2.7.11.8 O QoS deve possibilitar a definição de classes por:

7.2.7.11.9 Banda Garantida

7.2.7.11.10 Banda Máxima

7.2.7.11.11 Fila de Prioridade.

7.2.7.11.12 Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

7.2.7.11.13 Suportar marcação de pacotes Diffserv, inclusive por aplicação;

7.2.7.11.14 Deve implementar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inbound e outbound);

7.2.7.11.15 Disponibilizar estatísticas RealTime para classes de QoS.

7.2.7.11.16 Deve suportar QOS (traffic-shapping), em interface agregadas;

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

7.2.7.12 FILTRO DE DADOS



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.12.1 Permite a criação de filtros para arquivos e dados pré-definidos;

7.2.7.12.2 Os arquivos devem ser identificados por extensão e assinaturas;

7.2.7.12.3 Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);

7.2.7.12.4 Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

7.2.7.12.5 Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

7.2.7.12.6 Permitir listar o número de aplicações suportadas para controle de dados;

7.2.7.12.7 Permitir listar o número de tipos de arquivos suportados para controle de dados;

7.2.7.13 GEO-LOCALIZAÇÃO

7.2.7.13.1 Suportar a criação de políticas por Geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados.

7.2.7.13.2 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

7.2.7.13.3 Deve permitir visualizar nos logs e criar políticas para liberar e bloquear tráfego de países por: tipo de arquivo, aplicação e categoria de URL;

7.2.7.13.4 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

7.2.7.14 VPN

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

7.2.7.14.2 Suportar IPSec VPN;

7.2.7.14.3 Suportar SSL VPN;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.14.4 A VPN IPSEc deve suportar:

7.2.7.14.5 DES e 3DES;

7.2.7.14.6 Autenticação MD5 e SHA-1;

7.2.7.14.7 Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;

7.2.7.14.8 Algoritmo Internet Key Exchange (IKEv1 e v2);

7.2.7.14.9 AES 128, 192 e 256 (Advanced Encryption Standard)

7.2.7.14.10 Autenticação via certificado IKE PKI.

7.2.7.14.11 Deve possuir interoperabilidade com os seguintes fabricantes:

g) Cisco;

h) Checkpoint;

i) Juniper;

j) Palo Alto Networks;

k) Fortinet;

l) Sonic Wall;

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

7.2.7.14.13 A VPN SSL deve suportar:

7.2.7.14.14 SD-WAN avançado com medição ativa

7.2.7.14.15 Automação por IA

7.2.7.14.16 Segmentação baseada em identidade (Identity-based segmentation)

7.2.7.14.17 Suporte a IPv6 avançado (NAT64/DNS64/Teredo/6RD)

7.2.7.14.18 Dynamic Multicast NAT



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.14.19 Fabric Connector

7.2.7.14.20 O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

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

7.2.7.14.22 Atribuição de endereço IP nos clientes remotos de VPN SSL;

7.2.7.14.23 Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;

7.2.7.14.24 SSL-VPN com autenticação reforçada (SAML, Azure AD, MFA, FIDO2)

7.2.7.14.25 Suporte a IPsec com aceleração ASIC

7.2.7.14.26 Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;

7.2.7.14.27 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

7.2.7.14.28 Atribuição de DNS nos clientes remotos de VPN;

7.2.7.14.29 Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);

7.2.7.14.30 A solução de VPN deve verificar se o client que está conectado é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;
Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;

7.2.7.14.31 Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.14.32 Deve exibir mensagens de notificação customizadas toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;

7.2.7.14.33 Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;

7.2.7.14.34 Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

7.2.7.14.35 A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;

7.2.7.14.36 Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

7.2.7.14.37 Deve permitir a distribuição de certificado para o usuário remoto através do portal de VPN de forma automatizada;

7.2.7.14.38 Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;

7.2.7.14.39 Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;

7.2.7.14.40 Suporta leitura e verificação de CRL (certificate revocation list);

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

7.2.7.14.42 O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;

7.2.7.14.43 O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,

7.2.7.14.44 Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

7.2.7.14.45 Antes do usuário autenticar na estação;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.14.46 Após autenticação do usuário na estação;

7.2.7.14.47 Sob demanda do usuário;

7.2.7.14.48 Deverá manter uma conexão segura com o portal durante a sessão.

7.2.7.14.49 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OSx e Chrome OS;

7.2.7.14.50 O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;

7.2.7.14.51 Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;

7.2.7.14.52 Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;

7.2.7.15 CONSOLE DE GERÊNCIA E MONITORAÇÃO

7.2.7.15.1 Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

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

7.2.7.15.3 Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;

7.2.7.15.4 Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;

7.2.7.15.5 O gerenciamento deve permitir/possuir:

- i) Criação e administração de políticas de firewall e controle de aplicação;
- j) Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- k) Criação e administração de políticas de Filtro de URL;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- l) Monitoração de logs;
- m) Ferramentas de investigação de logs;
- n) Debugging;
- o) Captura de pacotes.
- p) Acesso concorrente de administradores;

7.2.7.15.6 Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;

7.2.7.15.7 Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.

7.2.7.15.8 Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;

7.2.7.15.9 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

7.2.7.15.10 Deve permitir usar palavras chaves e cores para facilitar a identificação de regras;

7.2.7.15.11 Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;

7.2.7.15.12 Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;

7.2.7.15.13 Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.15.14 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

7.2.7.15.15 Autenticação integrada ao Microsoft Active Directory e servidor Radius;

7.2.7.15.16 Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

7.2.7.15.17 Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

7.2.7.15.18 Criação de regras que fiquem ativas em horário definido;

7.2.7.15.19 Criação de regras com data de expiração;

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

7.2.7.15.21 Suportar Rollback de Sistema Operacional para a última versão local;

7.2.7.15.22 Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

7.2.7.15.23 Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;

7.2.7.15.24 Validação de regras antes da aplicação;

7.2.7.15.25 Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.

7.2.7.15.26 É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.

7.2.7.15.27 Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.15.28 É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

7.2.7.15.29 Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.

7.2.7.15.30 Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)

7.2.7.15.31 Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

7.2.7.15.32 Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

7.2.7.15.33 Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;

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

7.2.7.15.35 Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day" detectados em sand-box e tráfego bloqueado;

7.2.7.15.36 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

7.2.7.15.37 Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela.

7.2.7.15.38 Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

7.2.7.15.39 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.15.40 Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

7.2.7.15.41 Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;

7.2.7.15.42 Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;

7.2.7.15.43 Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;

7.2.7.15.44 Deve ser possível exportar os logs em CSV;

7.2.7.15.45 Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.
Rotação do log;

7.2.7.15.46 Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

7.2.7.15.47 Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;

7.2.7.15.48 Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

7.2.7.15.49 Situação do dispositivo e do cluster;

7.2.7.15.50 Principais aplicações;

7.2.7.15.51 Principais aplicações por risco;

7.2.7.15.52 Administradores autenticados na gerência da plataforma de segurança;

7.2.7.15.53 Número de sessões simultâneas;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.7.15.54 Status das interfaces;

7.2.7.15.55 Uso de CPU;

7.2.7.15.56 Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

7.2.7.15.57 Resumo gráfico de aplicações utilizadas;

7.2.7.15.58 Principais aplicações por utilização de largura de banda de entrada e saída;

7.2.7.15.59 Principais aplicações por taxa de transferência de bytes;

7.2.7.15.60 Principais hosts por número de ameaças identificadas;

7.2.7.15.61 Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;

7.2.7.15.62 Deve permitir a criação de relatórios personalizados;

7.2.7.15.63 Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

7.2.7.15.64 Gerar alertas automáticos via:

- d) Email;
- e) SNMP;
- f) Syslog;

7.2.7.15.65 A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.5.8. Tipo 8 - Solução WI-FI CONCENTRADOR - (Ponta “A” – DETRAN/SEDE)

7.2.8.1 Especificação Técnica Detalhada: Controladora de Acesso Wireless.

7.2.8.1.1 Características Físicas e Interfaces (Hardware)

7.2.8.1.1.1 O equipamento deve ser do tipo *appliance* físico dedicado (Box), de pequeno fator de forma, com altura de 1U e largura que permita fixação em rack padrão de 19 polegadas (acompanhado de abas/suportes de fixação);

7.2.8.1.1.2 Deverá possuir, no mínimo, 10 (dez) portas Ethernet 10/100/1000Base-T (RJ45) para conexão de serviços e gerência;

7.2.8.1.1.3 Deverá possuir, no mínimo, 2 (duas) portas de uplink 10 Gigabit Ethernet (SFP+) para conexão de alta velocidade ao Core da rede ou empilhamento lógico;

7.2.8.1.1.4 Deve possuir 1 (uma) porta de console RJ45 e 1 (uma) porta USB para manutenção e configuração local;

7.2.8.1.1.5 A arquitetura de processamento deve ser baseada em processadores multi-core dedicados para garantir o encaminhamento de dados sem gargalos;

7.2.8.1.1.6 Fonte de alimentação AC integrada, bivolt automático (100V~240V).

7.2.8.1.2 Capacidade e Escalabilidade

7.2.8.1.2.1 O equipamento deve suportar o gerenciamento nativo de, no mínimo, 256 (duzentos e cinquenta e seis) Access Points (APs), sendo possível a expansão via licenciamento sem troca de hardware;

7.2.8.1.2.2 Deve suportar a conexão simultânea de, no mínimo, 4.096 (quatro mil e noventa e seis) usuários/dispositivos clientes;

7.2.8.1.2.3. Deve possuir capacidade de *forwarding* (throughput de encaminhamento centralizado) de, no mínimo, 6 Gbit/s;

7.2.8.1.2.4. Deve suportar a criação de até 4.096 VLANs;

7.2.8.1.2.5. Deve suportar até 8.000 entradas ACL (Listas de Controle de Acesso);



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.8.1.2.6. Deve suportar até 4.096 entradas ARP;

7.2.8.1.3 Arquitetura e Modos de Encaminhamento

7.2.8.1.3.1. Deve suportar arquitetura de redes L2 e L3, permitindo o gerenciamento de APs localizados em redes remotas através de roteamento (MPLS/VPN);

7.2.8.1.3.2. Deve suportar os modos de operação: * Direct Forwarding (Local Forwarding): Onde o tráfego de dados do usuário flui do AP diretamente para o switch local, sem passar pela controladora (requisito essencial para sites remotos); * Tunnel Forwarding: Onde o tráfego é encapsulado em túnel CAPWAP (Control and Provisioning of Wireless Access Points) até a controladora;

7.2.8.1.3.3. Deve permitir a configuração mista, onde determinados SSIDs operam em modo Local e outros em modo Túnel no mesmo AP;

7.2.8.1.3.4. Suporte a redundância de alta disponibilidade (HA) nos modos: HSB (Hot Standby), Backup 1+1 e N+1, garantindo sincronismo de estado dos usuários e sessões em caso de falha da controladora principal;

7.2.8.1.4. Inteligência de Aplicação e QoS

7.2.8.1.4.1. [Trava de Software] O equipamento deve possuir mecanismo de Identificação e Controle de Aplicações (SAC - Smart Application Control) integrado, capaz de identificar e classificar tráfego de Camada 4 a Camada 7;

7.2.8.1.4.2. Deve possuir banco de assinaturas capaz de identificar mais de 6.000 (seis mil) aplicações distintas;

7.2.8.1.4.3. Deve permitir aplicar políticas de QoS (limite de banda, bloqueio ou priorização) baseadas na aplicação identificada (ex: bloquear P2P, limitar YouTube, priorizar Teams);

7.2.8.1.4.4. Suporte a *Airtime Fairness* para garantir justiça no tempo de transmissão entre clientes Wi-Fi antigos e novos;

7.2.8.1.5. Gerenciamento de Radiofrequência (RRM)

7.2.8.1.5.1. Deve implementar algoritmos de alocação dinâmica de canais (DCA) e controle de potência de transmissão (TPC) automáticos;

7.2.8.1.5.2. Deve possuir funcionalidade de detecção e mitigação de interferências de fontes não-Wi-Fi (Bluetooth, Micro-ondas, Telefones sem fio);



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.8.1.5.3. Suporte a Band Steering (priorização de 5GHz/6GHz) e Smart Roaming (forçando a desconexão de clientes com sinal fraco para que se conectem a APs melhores);

7.2.8.1.5.4. Suporte a balanceamento de carga de usuários baseado em tráfego ou quantidade de sessões entre APs adjacentes;

7.2.8.1.6. Segurança e Autenticação

7.2.8.1.6.1. Suporte completo a WPA, WPA2 e WPA3 (Personal e Enterprise, incluindo OWE e SAE);

7.2.8.1.6.2. Deve possuir servidor Portal Captivo Integrado (Built-in Portal), permitindo personalização de páginas de login sem necessidade de servidor externo;

7.2.8.1.6.3. O Portal integrado deve suportar autenticação via: Usuário/Senha Local, Voucher, SMS, Redes Sociais e Integração com LDAP/AD externo;

7.2.8.1.6.4. Deve suportar WIDS/WIPS para detecção de APs maliciosos (Rogue APs), ataques de *flood*, *spoofing* e *brute force*;

7.2.8.1.6.5. Deve suportar proteção de quadros de gerenciamento (PMF - 802.11w);

7.2.8.1.7. Gerenciamento e Manutenção

7.2.8.1.7.1. Deve oferecer interface de gerenciamento Web (HTTP/HTTPS) amigável para configuração completa do sistema;

7.2.8.1.7.2. Deve possuir CLI (Command Line Interface) padrão industrial acessível via SSH e Console;

7.2.8.1.7.3. Deve suportar integração com plataformas de gerência de rede centralizadas via SNMP v2/v3 e NETCONF/YANG;

7.2.8.1.7.4. Deve permitir atualização de firmware dos APs de forma automatizada e agendada, suportando atualização em lote sem paralisar toda a rede (Rolling update);

7.2.8.1.7.5. Deve suportar a funcionalidade de "Licença embutida" ou permitir o carregamento de licenças para a quantidade total de APs do projeto.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.5.9. Tipo 9 - Solução WI-FI ACESSO - (Ponta A e Ponta B – DETRAN/SEDE e CIRETRANS/POSTOS/SUB-REDE)

7.2.9.1 Características do Access Point WI-FI

7.2.9.1.1 Access Point Sem Fio Wi-Fi 6E, gerenciado por Plataforma de Gerência em Nuvem, para uso interno, sem antenas aparentes, que opere simultaneamente nas faixas de frequência de 2.4GHz, 5GHz e 6GHz, padrões 802.11b/g/n/a/ac/ax;

7.2.9.1.2 Deve possuir, no mínimo, 1 porta ethernet 100M/1000M/2.5G Base-T em conector RJ45 com suporte a alimentação PoE compatível com o padrão 802.3at e com reconhecimento automático de crossover MDI/MDIX;

7.2.9.1.3 Suporte a velocidades de no mínimo 4800 Mbps em 6 GHz, 2400 Mbps em 5GHz e 1150 Mbps em 2.4GHz;

7.2.9.1.4 Cada rádio deverá possuir, no mínimo, 4 antenas internas omnidirecionais, com ganho de, no mínimo, 5.4 dBi até 2.4 GHz, 6.4 dBi até 5 GHz, 7.2 dBi até 6 GHz.

7.2.9.1.5 Suporte a operação 4x4:4 MIMO;

7.2.9.1.6 Suportar a utilização de canais de 20, 40, 80 e 160 MHz;

7.2.9.1.7 Suportar, no mínimo, 16 (dezesesseis) SSIDs por rádio, com capacidade de configuração de VLAN e políticas de acesso independentes para cada SSID;

7.2.9.1.8 Possuir LED para a indicação do status de funcionamento do equipamento;

7.2.9.1.9 O equipamento deverá ser novo, sem uso anterior e não pode constar na situação de “solicitação de venda encerrada” (end of sale) ou “solicitação de pedido suspensa” (end of order) pelo fabricante no momento da proposta;

7.2.9.1.10 Deverá ser fornecido com a mais recente versão de hardware disponível na data da aquisição;

7.2.9.1.11 Deverá vir acompanhado de todos os acessórios para sua operacionalização, como cabos, softwares e manuais. Os manuais poderão ser disponibilizados no site do fabricante em língua portuguesa (Brasil) ou inglesa;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.9.1.12 Deverá possuir mecanismo de segurança física no padrão Kensington lock hard point ou similar;

7.2.9.1.13 A estrutura física do equipamento deverá permitir fixação em teto e em parede;

7.2.9.1.14 Deverá conter todas as ferragens necessárias para a sua fixação em teto e em parede;

7.2.9.1.15 Deve suportar DFS;

7.2.9.1.16 Suportar temperatura em modo de operação entre 0° to 40° C;

Características Gerais:

7.2.9.1.17 Deverá ser gerenciado de forma centralizada pelo Software de Gerência do mesmo fabricante do Access Point Sem Fio, para a configuração dos seus parâmetros Wi-Fi, QoS, políticas de acesso, políticas de segurança, monitoração do espectro de rádio frequência e demais funcionalidades, com conexão lógica via roteamento da camada de rede do modelo OSI, através de rede privada e pública;

7.2.9.1.18 Deve permitir ser gerenciado através de interface GUI local, através de um browser;

7.2.9.1.19 Deverá ser auto configurável através do Software de Gerência sem a necessidade de intervenção técnica para a sua configuração inicial (Zero Touch);

7.2.9.1.20 Deverá atualizar a sua versão de firmware através do Software de Gerência;

7.2.9.1.21 Deverá carregar e salvar as suas configurações através do Software de Gerência;

7.2.9.1.22 Caso a comunicação entre o Access Point (AP) e o Software de Gerência seja interrompida, o AP deve continuar operando, permitindo que os dispositivos e usuários já autenticados e associados à rede sem fio continuem acessíveis e que novos clientes possam obter acesso;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.9.1.23 Todo o tráfego de/para os dispositivos cliente deve ser encaminhado localmente e em hipótese alguma ser direcionado para o Software de Gerência em Nuvem;
- 7.2.9.1.24 Todo o tráfego de configuração, monitoria, gerência e estatísticas entre o Access Point e o Software de Gerência deverá ocorrer com a utilização de criptografia;
- 7.2.9.1.25 Suportar a pilha de protocolos TCP/IP;
- 7.2.9.1.26 Suportar os protocolos IPv4 e IPv6 simultaneamente;
- 7.2.9.1.27 Implementar VLAN Tagging IEEE 802.1q;
- 7.2.9.1.28 Implementar, localmente ou via software de gerência, o protocolo
- 7.2.9.1.29 NTP ou SNTP no modo cliente para a sincronização de horário;
- 7.2.9.1.30 Possuir cliente DHCP para a configuração automática dos seus parâmetros IP;
- 7.2.9.1.31 Permitir alimentação elétrica no padrão IEEE 802.3at Plus (PoE+), utilizando a porta do switch PoE+ onde estiver conectado;
- 7.2.9.1.32 Quando alimentado pela interface de rede via PoE+, não deve sofrer nenhuma perda de funcionalidade e operar no seu desempenho máximo;
- 7.2.9.1.33 Não possuir restrição de licenças para a quantidade de dispositivos conectados simultaneamente;
- 7.2.9.1.34 Implementar os padrões de segurança WPA2 Personal/Enterprise, WPA3 Personal, WPA3 Enterprise, OWE e Advanced Encryption Standard (AES);
- 7.2.9.1.35 Permitir habilitar e desabilitar a divulgação de cada SSID de forma independente;
- 7.2.9.1.36 Implementar Wireless Isolation para evitar que um dispositivo conectado a um SSID acesse os dados de outros dispositivos conectados no mesmo SSID;
- 7.2.9.1.37 Implementar filtros baseados em protocolos e em endereços MAC;
- Implementar o reuso de frequências (BSS coloring);



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.9.1.38 Implementar Target Wake Time para os clientes 802.11ax compatíveis;

7.2.9.1.39 Deve implementar OFDMA;

7.2.9.1.40 Deve suportar as funcionalidades de RADIUS Accounting, SNMP, Wireless Multimedia (WMM), Spanning Tree Protocol (STP), Bridge para LAN, Bridge para VLAN, Airtime Fairness, detecção de interferência, Fast roaming (802.11r), Band Steering, Autenticação via login social, Syslog e LLDP-MED;

7.2.9.1.41 Deve ser capaz de detectar Rogue SSID, Evil Twin SSID, BSSID Impersonate SSID, SSID Impersonate, Advanced Impersonate SSID e Adhoc SSID;

7.2.9.1.42 Disponibilizar sistema de hotspot vouchers baseado em tempo e volume de dados;

7.2.9.1.43 Deverá possuir acesso restrito por usuário e senha, com capacidade de criação de diferentes perfis de acesso onde seja possível determinar as funcionalidades atribuídas a cada perfil, existindo, no mínimo, um perfil com permissões de criação de usuários visitantes e um perfil com permissão para efetuar qualquer alteração;

7.2.9.1.44 Possuir listagem de clientes Wireless, indicando SSID, endereço IP e endereço MAC;

7.2.9.1.45 Listagem de APs e o status de cada Ponto de Acesso de forma individual, exibindo informações sobre o canal, grupo e endereço MAC;

7.2.9.1.46 Autenticação por Portal Web, onde conectados à rede são redirecionados para um Portal Web onde deverão se autenticar e então receber as políticas de acesso;

7.5.10. TIPO 10 - Switch Core/Distribuição L3 10 (Ponta A - DETRAN SEDE)

7.2.10.1 PORTAS:

7.2.10.1.1 Deve possuir, no mínimo, 48 (quarenta e oito) portas 10GE com suporte à inserção de transceivers do tipo SFP+.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.10.1.2 Deve possuir capacidade de associação das portas 10GE em grupo de duas portas, formando uma única interface lógica, compatível com a norma IEEE 802.3ad.

7.2.10.1.3 Deve possuir 6 (seis) portas 40GE QSFP+

7.2.10.1.4 Deve implementar VLANs por porta.

7.2.10.1.5 Deve implementar VLANs compatíveis com o padrão IEEE 802.1Q.

7.2.10.1.6 Deve possuir porta de console para ligação direta e através de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.

7.2.10.2 FONTE DE ALIMENTAÇÃO:

7.2.10.2.1 Deve possuir fontes de alimentação redundantes internas AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).

7.2.10.2.2 Deve possuir cabo de alimentação para a fonte com plugue de três pinos no novo padrão do Inmetro, norma ABNT NBR 14136.

7.2.10.3 ARQUITETURA:

7.2.10.3.1 Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.

7.2.10.3.2 Permitir o empilhamento (Switch Stackable) de no mínimo 4 (quatro) unidades por caminhos redundantes através de interfaces 40G ou superior. Deve possuir no máximo 1 Rack Unit (RU).

7.2.10.4 GERENCIAMENTO

7.2.10.4.1 Deve possuir LEDs para a indicação do status das portas e atividade

7.2.10.4.2 Deve implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.

7.2.10.4.3 Deve implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:

Sem autenticação e sem privacidade (noAuthNoPriv);

Com autenticação e sem privacidade (authNoPriv);

Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia AES ou SHA ou MD5 ou DES.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.10.4.4 Deve possuir suporte a MIB II, conforme RFC 1213.

7.2.10.4.5 Deve possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 1024 bytes.

7.2.10.4.6 Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.

7.2.10.4.7 Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas.

7.2.10.4.8 Deve implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events) conforme RFC 2819.

7.2.10.4.9 Deve implementar os protocolos LLDP (IEEE 802.3ab)

7.2.10.4.10 O equipamento deverá permitir empilhamento com velocidade de empilhamento de no mínimo 160Gbps full-duplex. Os módulos e/ou cabos necessários para o empilhamento deverão ser fornecidos.

7.2.10.4.11 A pilha deverá ser gerenciada através de um único endereço IP para gerência e administração e permitir agregação lógica de links utilizando qualquer porta da pilha, além de permitir espelhamento de portas de qualquer porta para qualquer porta da pilha.

7.2.10.4.12 Deve implementar Sflow ou Netflow.

7.2.10.4.13 O equipamento deve suportar OpenFlow 1.3 ou padrão similar para suporte à SDN;

7.2.10.4.14 O equipamento deve responder a pacotes de testes para teste da implementação dos níveis de serviço especificados (SLA). Devem ser suportadas no mínimo as seguintes operações de teste:

ICMP echo

TCP connect (em porta TCP que o administrador especifique)

UDP echo (em porta UDP que o administrador especifique)

UDP Jitter

7.2.10.4.15 Deve implementar Telnet para acesso à interface de linha de comando.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.10.4.16 Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet.

7.2.10.4.17 Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet e SSH.

7.2.10.4.18 Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.

7.2.10.4.19 Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.

7.2.10.4.20 Permitir a gravação de log externo (syslog).

7.2.10.4.21 Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.

7.2.10.4.22 Deve possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.

7.2.10.4.23 Permitir o espelhamento da totalidade do tráfego de uma porta ou de um grupo de portas para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.

7.2.10.4.24 Permitir o espelhamento da totalidade do tráfego de uma VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local.

7.2.10.4.25 Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas ("promíscuas"), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas ("promíscuas") de uma dada VLAN.

7.2.10.4.26 Deve permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.

7.2.10.5 PROTOCOLOS:



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.10.5.1 Deve implementar o protocolo SNTP ou NTPv3 (Network Time Protocol, versão 3).

7.2.10.5.2 Deve implementar padrão IEEE 802d (Spanning Tree Protocol) por VLAN.

7.2.10.5.3 Deve implementar padrão IEEE 802.1w (Rapid Spanning Tree Protocol) por VLAN.

7.2.10.5.4 Deve implementar padrão IEEE 802.1Q (Vlan Frame Tagging).

7.2.10.5.5 Deve implementar padrão IEEE 802.1p (Class of Service) para cada porta.

7.2.10.5.6 Deve implementar padrão IEEE 802.3ad, Link Aggregation Control Protocol (LACP).

7.2.10.5.7 Deve implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 48 instâncias simultâneas do protocolo Spanning-Tree;

7.2.10.6 DESEMPENHO:

7.2.10.6.1 Deve possuir capacidade para pelo menos 256.000 endereços na tabela MAC;

7.2.10.6.2 Deve implementar, no mínimo, 4000 vlans simultaneamente;

7.2.10.6.3 A capacidade de comutação do equipamento ofertado deve ser de pelo menos 1440 Gbps e taxa de encaminhamento de 1080 Mpps;

7.2.10.6.4 Deve possuir capacidade para, no mínimo, 40.000 endereços na tabela ARP.

Suportar Jumbo frames de no mínimo 9018 Bytes.

7.2.10.7 SEGURANÇA:

7.2.10.7.1 Deve implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseado em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS.

7.2.10.7.2 Deve implementar filtragem de pacotes (ACL - Access Control List).



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.10.7.3 Proteger a interface de comando do equipamento através de senha.

7.2.10.7.4 Deve implementar o protocolo SSH V2 para acesso à interface de linha de comando.

7.2.10.7.5 Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet e SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.

7.2.10.7.6 Permitir a implementação de filtros ACL ou funcionalidade que permita a aplicação de políticas, utilizando os seguintes parâmetros:

- i. Endereço MAC de origem e destino.
- ii. Endereço IP de origem e destino.
- iii. Porta TCP e UDP de origem e destino.
- iv. IP Precedence.

7.2.10.7.7 Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão.

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

7.2.10.7.9 Deve implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.

7.2.10.7.10 Deve possuir controle de broadcast, multicast e unicast por porta.

7.2.10.7.11 Deve possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2

7.2.10.7.12 Deve possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w).

7.2.10.7.13 Deve possuir análise do protocolo ARP (Address Resolution Protocol) e possuir proteção nativa contra ataques do tipo “ARP Poisoning”.

7.2.10.8 ROTEAMENTO:



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.10.8.1 Deve implementar roteamento estático.

7.2.10.8.1 Deve implementar roteamento dinâmico RIPv2 (RFC 2453, 2082)

7.2.10.8.1 Deve implementar protocolo de roteamento dinâmico OSPF (RFC 2328, 3101)

7.2.10.8.1 Deve implementar protocolo de roteamento BGPv4 (RFC 4271, 1997 e 2385).

7.2.10.8.1 Permitir o roteamento nível 3 entre VLANs.

7.2.10.8.1 Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol) conforme a RFC 2338;

7.2.10.8.1 O equipamento ofertado deve implementar Policy-Based Routing (PBR) permitindo a definição de políticas de roteamento baseadas em endereços de origem e outras condições especiais.

7.2.10.8.1 Suportar roteamento estático para IPv6.

7.2.10.8.1 Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6.

7.2.10.9 MULTICAST:

7.2.10.9.1 Deve implementar roteamento multicast PIM-DM, PIM-SM, PIM-SSM para IPV4 e IPV6;

7.2.10.9.2 Deve implementar o protocolo IGMP nas versões v1 (RFC 1112), v2 (RFC 2236) e v3 (RFC 3376).

7.2.10.9.3 Deve implementar o mecanismo IGMP Snooping (v1, v2, v3).

7.2.10.10 QUALIDADE DE SERVIÇO (QoS):

7.2.10.10.1 Deve possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.

7.2.10.10.2 Deve possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo).



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.10.10.3 Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.

7.2.10.10.4 Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nível 2) e DSCP ("Differentiated Services Code Point"- nível 3), conforme definições do IETF (Internet Engineering Task Force).

7.2.10.10.5 Suportar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing".

7.2.10.10.6 Deve ser possível a especificação de banda por classe de serviço.

7.2.10.10.7 Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.

7.2.10.10.8 Suportar mapeamento de prioridades nível 3 (DSCP) em prioridades nível 2, definidas pelo padrão (IEEE 802.1p).

7.2.10.10.9 Suportar diferenciação de QoS por VLAN.

7.2.10.10.10 Suporte aos mecanismos de QoS WRR (Weighted Round Robin).

7.2.10.10.11 Deve implementar pelo menos 8 (oito) filas de prioridade por porta de saída (egress port).

7.2.10.11 INTERNET PROTOCOL VERSÃO 6 (IPv6)

7.2.10.11.1 Deve implementar IPv6.

7.2.10.11.2 Permitir a configuração de endereços IPv6 para gerenciamento.

7.2.10.11.3 Permitir consultas de DNS com resolução de nomes em endereços IPv6.

7.2.10.11.4 Deve implementar ICMPv6 com as seguintes funcionalidades:

- i. ICMP request
- ii. ICMP Reply
- iii. ICMP Neighbor Discovery Protocol (NDP)
- iv. ICMP MTU Discovery



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.10.11.5 Deve implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, SNMP, e DNS sobre IPv6.

7.2.10.11.6 Deve implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.

7.5.11. Tipo 11 - Solução de Relatoria (1 unidade) (Ponta A - DETRAN SEDE)

- a) Possuir capacidade de receber ao menos 190 GBytes de logs diários
- b) Deve suportar receber logs de ao menos 200 dispositivos
- c) Possuir ao menos 12 TB de espaço em disco
- d) Possuir ao menos 2 interfaces de 10Gbps SFP+

Requisitos Mínimos de Funcionalidade – Solução de Relatoria

7.2.11.1 FUNCIONALIDADES GERAIS

7.2.11.1.1 Deve suportar acesso via SSH, WEB (HTTPS) e Telnet para o gerenciamento da solução;

7.2.11.1.2 Possuir comunicação cifrada e autenticada com usuário e senha para solução de relatórios, tanto como para a interface gráfica de usuário e console de administração por linha de comandos (SSH);

7.2.11.1.3 Permitir acesso simultâneo de administradores permitindo a criação de ao menos 2 (dois) perfis para administração e monitoração;

7.2.11.1.4 Suportar SNMP versão 2 e versão 3 na solução de relatórios;

7.2.11.1.5 Permitir virtualizar a solução de relatórios, onde cada administrador gerencie, visualize e edite apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;

7.2.11.1.6 Deve permitir a criação de administradores que acessem à todas as instâncias de virtualização da solução de relatórios;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.11.1.7 Deve permitir habilitar e desabilitar, para cada interface de rede da solução de relatórios, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;

7.2.11.1.8 Autenticação integrada a servidor Radius;

7.2.11.1.9 Geração de relatórios em tempo real, para a visualização de tráfego observado, nos formatos: mapas geográficos e tabela;

7.2.11.1.10 Geração de relatórios em tempo real, para a visualização de tráfego observado, no formato bolhas;

7.2.11.1.11 Autenticação integrada ao Microsoft Active Directory;

7.2.11.1.12 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

7.2.11.1.13 Deve possuir um assistente para adicionar dispositivos via interface gráfica usando o IP, login e senha dos mesmos;

7.2.11.1.14 Deve ser possível visualizar a quantidade de logs enviado de cada dispositivo monitorado;

7.2.11.1.15 Possuir mecanismo para que logs antigos sejam removidos automaticamente

7.2.11.1.16 Permitir a importação e exportação de relatórios;

7.2.11.1.17 Deve possuir a capacidade de criar relatórios nos formatos HTML;

7.2.11.1.18 Deve possuir a capacidade de criar relatórios nos formatos PDF;

7.2.11.1.19 Deve possuir a capacidade de criar relatórios nos formatos XML;

7.2.11.1.20 Deve possuir a capacidade de criar relatórios nos formatos CSV;

7.2.11.1.21 Deve ser possível exportar os logs em CSV;

7.2.11.1.22 Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.11.1.23 Os logs gerados pelos appliances devem ser centralizados nos servidores de gerência, mas a solução deve oferecer também a possibilidade de utilização de um syslog externo ou similar;

7.2.11.1.24 A solução deve possuir relatórios pré definidos;

7.2.11.1.25 Possuir envio automático de logs para um servidor FTP externo a solução;

7.2.11.1.26 Possibilitar a duplicação de relatórios existentes e editá-los logo após;

7.2.11.1.27 Possuir a capacidade de personalização de capas para os relatórios;

7.2.11.1.28 Permitir de forma centralizada visualizar os logs recebidos por um ou vários dispositivos externos incluindo a capacidade de uso de filtros nas pesquisas deste log;

7.2.11.1.29 Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados;

7.2.11.1.30 Possuir a capacidade de personalização de gráficos como barra, linha e tabela para inserção aos relatórios;

7.2.11.1.31 Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em realtime;

7.2.11.1.32 Dever ser possível fazer download dos arquivos de logs recebidos;

7.2.11.1.33 Deve possuir agendamento para gerar e enviar automaticamente relatórios

7.2.11.1.34 Permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente pelo administrador, adaptando-o às suas necessidades;

7.2.11.1.35 Permitir o envio de maneira automática de relatórios por e-mail;

7.2.11.1.36 Deve permitir a escolha do email a ser enviado para cada relatório escolhido;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.11.1.37 Permitir programar a geração de relatórios, conforme calendário definido pelo administrador;
- 7.2.11.1.38 Deve ser possível visualizar através de gráficos em tempo real o consumo de disco e taxa de geração de logs dos dispositivos gerenciados;
- 7.2.11.1.39 Deve ser possível definir filtros nos relatórios;
- 7.2.11.1.40 Deve ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros;
- 7.2.11.1.41 Permitir que relatórios criado sejam no idioma Português;
- 7.2.11.1.42 Gerar alertas automáticos via Email, SNMP e Syslog baseados em eventos como ocorrência como log, severidade de log, entre outros;
- 7.2.11.1.43 Deve permitir o envio automático de relatórios criado a um servidor de SFTP ou FTP externo a solução;
- 7.2.11.1.44 Deve ser capaz de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios;
- 7.2.11.1.45 Ter a capacidade de visualizar na GUI da solução de relatórios informações do sistema como licenças, memória, disco, uso de CPU, taxa de logs por segundo recebidos, total de logs diários recebidos, alertas gerados entre outros;
- 7.2.11.1.46 Deve possuir uma ferramenta para análise de desempenho para cada relatório gerado, com o objetivo de detectar problemas de performance de sistema de acordo com o relatório criado;
- 7.2.11.1.47 Permitir que a solução importe arquivos de log, de dispositivos compatíveis conhecidos e não conhecidos pelo sistema, para posterior geração de relatórios;
- 7.2.11.1.48 Deve ser possível definir o espaço que cada instância de virtualização poderá utilizar para armazenamento de logs;
- 7.2.11.1.49 A solução deve servir como um servidor de syslog e aceitar logs de diferentes fabricantes
- 7.2.11.1.50 Deve possuir a informação da quantidade de logs armazenado e estatística de tempo de retenção restante;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.11.1.51 Deve suportar duplo fator de autenticação (token) para os administradores do sistema de relatórios;

7.2.11.1.52 Deve permitir aplicar políticas de senhas para os administradores do sistema como tamanho mínimo de caracteres a usar;

7.2.11.1.53 Deve permitir ver em tempo real os logs recebidos;

7.2.11.2 RELATÓRIOS

7.2.11.2.1 Deve permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

7.2.11.2.2 Deve possuir um Indicador de Comprometimento (IoC), que mostre usuários finais com utilização web suspeita, devendo informar no mínimo: endereço ip do usuário, hostname, sistema operacional, veredito (classificação geral de ameaça), número de ameaças detectadas;

7.2.11.2.3 Deve possuir relatório de PCI DSS Compliance;

7.2.11.2.4 Deve possuir relatório de utilização de aplicações SAAS;

7.2.11.2.5 Deve possuir relatório detalhado de prevenção de perda de dados (DLP);

7.2.11.2.6 Deve possuir relatório de VPN;

7.2.11.2.7 Deve possuir relatório de Sistemas de prevenção de intrusão (IPS);

7.2.11.2.8 Deve possuir relatório de reputação do cliente;

7.2.11.2.9 Deve possuir relatório de análise de segurança do usuário;

7.2.11.2.10 Deve possuir relatório de avaliação da ameaça cibernética;

7.2.11.2.11 Deve possuir relatório de WiFi PCI Compliance;

7.2.11.2.12 Deve possuir relatório a informação de AP's e SSID's autorizados, também clientes WiFi;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.11.2.13 Deve possuir relatório de equipamentos terminais de solução de segurança gerenciada;

7.2.11.2.14 Deve possuir relatório de análise de segurança e uso de web, se há uma plataforma de cache;

7.2.11.2.15 Deve possuir relatório de análise de aplicações web, se há uma plataforma de segurança web.

7.2.12 Tipo 12 - Solução de Gerência Centralizada (1 unidade) Ponta A DETRAN SEDE)

- a) Deve permitir gerenciar ao menos 300 dispositivos
- b) Deve possuir fontes de alimentação redundantes
- c) Deve suportar RAID
- d) Deve possuir porta de console serial DB-9 ou RJ-45
- e) Possuir ao menos 2 interfaces de 1Gbps
- f) Possuir ao menos 2 Interfaces de 10 Gbps
- g) Possuir ao menos 24 TB de espaço em disco

7.2.12.1 CARACTERÍSTICAS GERAIS

7.2.12.1.1 A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

7.2.12.1.2 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

7.2.12.1.3 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

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

7.2.12.1.5 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

7.2.12.1.6 A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;
Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;

7.2.12.1.7 Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;

7.2.12.1.8 Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;

7.2.12.1.9 Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

7.2.12.1.10 Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

7.2.12.1.11 Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

7.2.12.1.12 Os dispositivos de proteção de rede devem suportar sFlow;

7.2.12.1.13 Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

7.2.12.1.14 Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

7.2.12.1.15 Deve suportar NAT dinâmico (Many-to-1);

7.2.12.1.16 Deve suportar NAT dinâmico (Many-to-Many);

7.2.12.1.17 Deve suportar NAT estático (1-to-1);

7.2.12.1.18 Deve suportar NAT estático (Many-to-Many);

7.2.12.1.19 Deve suportar NAT estático bidirecional 1-to-1;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.1.20 Deve suportar Tradução de porta

(PAT); 7.2.12.1.21 Deve suportar NAT de Origem;

7.2.12.1.22 Deve suportar NAT de Destino;

7.2.12.1.23 Deve suportar NAT de Origem e NAT de Destino simultaneamente;

7.2.12.1.24 Deve poder combinar NAT de origem e NAT de destino na mesma política

7.2.12.1.25 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

7.2.12.1.26 Deve suportar NAT64 e NAT46;

7.2.12.1.27 Deve implementar o protocolo ECMP;

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

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

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

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

7.2.12.1.32 Deve permitir monitorar via 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;

7.2.12.1.33 Enviar log para sistemas de monitoração externos, simultaneamente;

7.2.12.1.34 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

7.2.12.1.35 Proteção anti-spoofing;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.1.36 Implementar otimização do tráfego entre dois equipamentos;

7.2.12.1.37 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

7.2.12.1.38 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

7.2.12.1.39 Suportar OSPF graceful restart;

7.2.12.1.40 Os dispositivos de proteção devem 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);

7.2.12.1.41 Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

7.2.12.1.42 Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

7.2.12.1.43 Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

7.2.12.1.44 Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

7.2.12.1.45 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

7.2.12.1.46 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

7.2.12.1.47 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

7.2.12.1.48 A configuração em alta disponibilidade deve sincronizar: Sessões;

7.2.12.1.49 A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

7.2.12.1.50 A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.1.51 A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;

7.2.12.1.52 O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

7.2.12.1.53 Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;

7.2.12.1.54 Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;

7.2.12.1.55 Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

7.2.12.1.56 O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

7.2.12.1.57 Controle, inspeção e descryptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

7.2.12.1.58 Deve apoiar um tecido de segurança para fornecer uma solução de segurança holística abrangendo toda a rede;

7.2.12.1.59 O tecido de segurança deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;

7.2.12.1.60 Deve existir um Serviço de Suporte que ofereça aos clientes uma verificação de saúde recorrente com um relatório de auditoria mensal personalizado de seus appliances NGFW e inalámbrica;

7.2.12.2 CONTROLE POR POLITICA DE FIREWALL

7.2.12.2.1 Deverá suportar controles por zona de segurança;

7.2.12.2.2 Controles de políticas por porta e protocolo;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.2.3 Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

7.2.12.2.4 Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

7.2.12.2.5 Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;

7.2.12.2.6 Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;

7.2.12.2.7 Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise);

7.2.12.2.8 Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);

7.2.12.2.9 Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não superem a velocidade de upload;

7.2.12.2.10 Deve suportar o protocolo padrão da indústria VXLAN;

7.2.12.3 CONTROLE DE APLICAÇÕES

7.2.12.3.1 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

7.2.12.3.2 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

7.2.12.3.3 Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

7.2.12.3.4 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory,



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

7.2.12.3.5 Deve inspecionar o payload do pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

7.2.12.3.6 Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

7.2.12.3.7 Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

7.2.12.3.8 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

7.2.12.3.9 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;

7.2.12.3.10 Identificar o uso de táticas evasivas via comunicações criptografadas;

7.2.12.3.11 Atualizar a base de assinaturas de aplicações automaticamente;

7.2.12.3.12 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;

7.2.12.3.13 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

7.2.12.3.14 Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.3.15 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

7.2.12.3.16 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

7.2.12.3.17 Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

7.2.12.3.18 A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;

7.2.12.3.19 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

7.2.12.3.20 Deve alertar o usuário quando uma aplicação for bloqueada;

7.2.12.3.21 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

7.2.12.3.22 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

7.2.12.3.23 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;

7.2.12.3.24 Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos

7.2.12.3.25 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

7.2.12.3.26 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.3.27 Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

7.2.12.3.28 Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente

7.2.12.4 PREVENÇÃO DE AMEAÇAS

7.2.12.4.1 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

7.2.12.4.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

7.2.12.4.3 As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

7.2.12.4.4 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

7.2.12.4.5 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

7.2.12.4.6 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

7.2.12.4.7 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

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

7.2.12.4.9 Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

7.2.12.4.10 Deve permitir o bloqueio de vulnerabilidades;

7.2.12.4.11 Deve permitir o bloqueio de exploits conhecidos;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.12.4.12 Deve incluir proteção contra-ataques de negação de serviços;
- 7.2.12.4.13 Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de padrões de estado de conexões;
- 7.2.12.4.14 Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;
- 7.2.12.4.15 Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;
- 7.2.12.4.16 Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise heurística;
- 7.2.12.4.17 Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;
- 7.2.12.4.18 Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP,
- 7.2.12.4.19 Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;
- 7.2.12.4.20 Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
- 7.2.12.4.21 Detectar e bloquear a origem de portscans;
- 7.2.12.4.22 Bloquear ataques efetuados por worms conhecidos;
- 7.2.12.4.23 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- 7.2.12.4.24 Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 7.2.12.4.25 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 7.2.12.4.26 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.4.27 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

7.2.12.4.28 Suportar bloqueio de arquivos por tipo;

7.2.12.4.29 Identificar e bloquear comunicação com botnets;

7.2.12.4.30 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;

7.2.12.4.31 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

7.2.12.4.32 Deve 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;

7.2.12.4.33 Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

7.2.12.4.34 Os eventos devem identificar o país de onde partiu a ameaça;

7.2.12.4.35 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

7.2.12.4.36 Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

7.2.12.4.37 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

7.2.12.4.38 O Firewall deve permitir que se analise a implantação de Tecido de Segurança para identificar potenciais vulnerabilidades e destaque as práticas recomendadas que podem ser usadas para melhorar a segurança e o desempenho geral da rede;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.4.39 Caso o firewall possa ser coordenado por software de segurança do computador do usuário final (laptop, desktop, etc.) deve ter um perfil onde se possa executar a análise de vulnerabilidade nestes equipamentos de usuário e assegurar que estes executem versões compatíveis;

7.2.12.4.40 Análise de postura de segurança devem existir para permitir que o software de segurança do endpoint aplique proteção em tempo real, antivírus, filtragem da Web e controle de aplicativos no endpoint;

7.2.12.4.41 Fornecem proteção contra-ataques de dia zero por meio de estreita integração com os componentes Security Fabric, incluindo NGFW, Sandbox (on-premise e nuvem);

7.2.12.5 FILTRO DE URL

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

7.2.12.5.2 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

7.2.12.5.3 Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

7.2.12.5.4 Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;

7.2.12.5.5 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

7.2.12.5.6 Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

7.2.12.5.7 Possuir pelo menos 60 categorias de URLs;

7.2.12.5.8 Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

7.2.12.5.9 Permitir a customização de página de bloqueio;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.5.10 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site)

7.2.12.5.11 Além do Explicit Web Proxy, suportar proxy Web transparente;

7.2.12.6 IDENTIFICAÇÃO DE USUÁRIOS

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

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

7.2.12.6.3 Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2;

7.2.12.6.4 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;

7.2.12.6.5 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

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

7.2.12.6.7 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.6.8 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft

7.2.12.6.8 Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

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

7.2.12.6.10 Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;

7.2.12.6.11 Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;

7.2.12.7 QOS E TRAFFIC SHAPING

7.2.12.7.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

7.2.12.7.2 Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

7.2.12.7.3 Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

7.2.12.7.4 Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

7.2.12.7.5 Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

7.2.12.7.6 Suportar a criação de políticas de QoS e Traffic Shaping por porta

7.2.12.7.7 O QoS deve possibilitar a definição de tráfego com banda garantida;

7.2.12.7.8 O QoS deve possibilitar a definição de tráfego com banda máxima;

7.2.12.7.9 O QoS deve possibilitar a definição de fila de prioridade;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.7.10 Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

7.2.12.7.11 Suportar marcação de pacotes Diffserv, inclusive por aplicação;

7.2.12.7.12 Suportar modificação de valores DSCP para o Diffserv;

7.2.12.7.13 Suportar priorização de tráfego usando informação de Type of Service;

7.2.12.7.14 Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

7.2.12.7.15 Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

7.2.12.8 FILTRO DE DADOS

7.2.12.8.1 Permitir a criação de filtros para arquivos e dados pré-definidos;

7.2.12.8.2 Os arquivos devem ser identificados por extensão e tipo;

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

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

7.2.12.8.5 Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

7.2.12.8.6 Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

7.2.12.9 GEO LOCALIZAÇÃO

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

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



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.9.3 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

7.2.12.10 VPN

7.2.12.10.1 .Suportar VPN Site-to-Site e Cliente-To-Site;

7.2.12.10.2 Suportar IPSec VPN;

7.2.12.10.3 Suportar SSL VPN;

7.2.12.10.4 A VPN IPSEc deve suportar 3DES;

7.2.12.10.5 A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

7.2.12.10.6 A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

7.2.12.10.7 A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

7.2.12.10.8 A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

7.2.12.10.9 A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

7.2.12.10.10 Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

7.2.12.10.11 Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

7.2.12.10.12 Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

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

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



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.10.15 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

7.2.12.10.16 Atribuição de DNS nos clientes remotos de VPN;

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

7.2.12.10.18 Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

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

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

7.2.12.10.21 Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes do usuário autenticar na estação;

7.2.12.10.22 Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Após autenticação do usuário na estação;

7.2.12.10.23 Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Sob demanda do usuário;

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

7.2.12.10.25 O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

7.2.12.11 WIRELESS CONTROLLER

7.2.12.11.1 Deve ser capaz de gerenciar de maneira centralizada outros pontos de acesso do mesmo fabricante;

7.2.12.11.2 Suporte ao serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

7.2.12.11.3 Suportar IPv4 e IPv6 por SSID;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.11.4 Permitir escolher se o tráfego de cada SSID será enviado à controladora ou comutado diretamente pela interface do ponto de acesso em determinada VLAN;

7.2.12.11.5 Permitir definir quais redes serão acessadas através da controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;

7.2.12.11.6 Suporte a monitoração e supressão de ponto de acesso indevido;

7.2.12.11.7 Prover autenticação para a rede wireless através de bases externas como LDAP ou RADIUS;

7.2.12.11.8 Permitir autenticar usuários da rede wireless de forma transparente em domínio Windows;

7.2.12.11.9 Deverá permitir a visualização dos clientes wireless conectados por usuário;

7.2.12.11.10 Deverá permitir a visualização dos clientes wireless conectados por IP;

7.2.12.11.11 Deverá permitir a visualização dos clientes wireless conectados por tipo de autenticação;

7.2.12.11.12 Deverá permitir a visualização dos clientes wireless conectados por canal;

7.2.12.11.13 Deverá permitir a visualização dos clientes wireless conectados por largura de banda utilizada;

7.2.12.11.14 Deverá permitir a visualização dos clientes wireless conectados por potência do sinal;

7.2.12.11.15 Deverá permitir a visualização dos clientes wireless conectados tempo de conexão;

7.2.12.11.16 Deverá prover suporte a Fast Roaming em autenticação com Captive Portal;

7.2.12.11.17 Deve suportar configuração de Captive Portal por SSID;

7.2.12.11.18 Permitir configurar o bloqueio de tráfego entre os clientes conectados a um SSID e AP específico;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.12.11.19 Ser compatível com Wi-Fi Protected Access (WPA) e WPA2 por SSID, utilizando-se de algoritmo AES e/ou TKIP;
- 7.2.12.11.20 Deverá suportar 802.1x através de RADIUS na controladora wireless;
- 7.2.12.11.21 Permitir configurar parâmetros de rádio, como banda e canal, na controladora wireless;
- 7.2.12.11.22 A controladora deve possuir método de descoberta de novos Pontos de Acesso de maneira automática;
- 7.2.12.11.23 A controladora deve possuir método de descoberta de novos Pontos de Acesso baseados em IP estático;
- 7.2.12.11.24 A controladora deve possuir método de descoberta de novos Pontos de Acesso baseados em DHCP;
- 7.2.12.11.25 A controladora deve possuir método de descoberta de novos Pontos de Acesso por DNS;
- 7.2.12.11.26 A controladora deve possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast;
- 7.2.12.11.27 A controladora deve possuir método de descoberta de novos Pontos de Acesso baseados em Multicast;
- 7.2.12.11.28 A controladora deve fornecer lista contendo Pontos de Acesso autorizados e Pontos de Acesso indevidos (Rogue);
- 7.2.12.11.29 Possuir proteção contra-ataques do tipo ARP Poisoning na controladora wireless;
- 7.2.12.11.30 Implementar Protected Management Frames de acordo com a norma da aliança WiFi e o padrão 802.11ac;
- 7.2.12.11.31 Possuir WIDS integrado com detecção de ataques ASLEAP;
- 7.2.12.11.32 Possuir WIDS integrado com detecção de ataques do tipo Association Frame Flooding;
- 7.2.12.11.33 Possuir WIDS integrado com detecção de ataques de authentication Frame Flooding;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.11.34 Possuir WIDS integrado com detecção de ataques de Broadcast De-authentication;

7.2.12.11.35 Possuir WIDS integrado com detecção de ataques de EAPOL Packet flooding;

7.2.12.11.36 Possuir WIDS integrado com detecção de ataques de Invalid MAC OUI;

7.2.12.11.37 Possuir WIDS integrado com detecção de ataques de Long Duration Attack;

7.2.12.11.38 Possuir WIDS integrado com detecção de ataques de Null SSID probe response;

7.2.12.11.39 Possuir WIDS integrado com detecção de ataques de Spoofed De-authentication;

7.2.12.11.40 Possuir WIDS integrado com detecção de ataques de Weak WEP IV Detection;

7.2.12.11.41 Possuir WIDS integrado com detecção de ataques de Wireless Bridge;

7.2.12.11.42 Implementar canais de provisionamento automático dos Access Points, de forma a minimizar interferência entre eles;

7.2.12.11.43 Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

7.2.12.11.44 Permitir definir em quais horários determinado SSID estará disponível;

7.2.12.11.45 A controladora wireless deverá oferecer Firewall integrado UTM, baseado em identidade do usuário;

7.2.12.11.46 Possibilitar definir número máximo de clientes permitidos por SSID;

7.2.12.11.47 Possibilitar definir número máximo de clientes permitidos por AP;

7.2.12.11.48 Possibilitar definir número máximo de clientes permitidos por Radio;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.12.11.49 Deve permitir criar, gerenciar e disponibilizar redes wireless mesh;
- 7.2.12.11.50 Possuir mecanismo de criação automática e/ou manual de usuários visitantes e senhas, que possam ser enviadas por email ou SMS aos usuários, e com ajuste de tempo de expiração da senha;
- 7.2.12.11.51 A comunicação entre o ponto de acesso e a controladora wireless deve poder ser efetuada de forma criptografada usando o protocolo DTLS;
- 7.2.12.11.52 Deve possuir mecanismo de ajuste de potência do sinal de forma a reduzir interferência entre canais entre dois pontos de acesso gerenciados;
- 7.2.12.11.53 Possuir mecanismo de balanceamento de tráfego/usuários entre pontos de acesso;
- 7.2.12.11.54 Possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou radios dos pontos de acesso;
- 7.2.12.11.55 Deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;
- 7.2.12.11.56 Permitir que sejam desabilitados clientes wireless que possuam taxa de transmissão baixa;
- 7.2.12.11.57 Permitir bloquear clientes wireless que tenham sinal fraco, definindo um limiar de sinal a partir do qual tais clientes serão ignorados;
- 7.2.12.11.58 Deve permitir configurar o valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;
- 7.2.12.11.59 Deve permitir selecionar individualmente em cada ponto de acesso quais os SSIDs que serão propagados;
- 7.2.12.11.60 Deve permitir associação dinâmica de VLANs aos usuários autenticados via RADIUS num SSID;
- 7.2.12.11.61 Deve permitir associação dinâmica de VLANs aos usuários autenticados via vlan pooling;
- 7.2.12.11.62 Deve permitir visualizar as aplicações e ameaças por dispositivo wireless;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 7.2.12.11.63 Deve permitir identificar os clientes wifi que apresentem algum risco baseado em aplicações;
- 7.2.12.11.64 Deve permitir identificar os clientes wifi que apresentem algum risco baseado em endereço de destino;
- 7.2.12.11.65 Deve permitir identificar os clientes wifi que apresentem algum risco baseado em ameaças;
- 7.2.12.11.66 Deve permitir identificar os clientes wifi que apresentem algum risco baseado em sessões;
- 7.2.12.11.67 A controladora wireless deve suportar uma licença que permita pelo menos 10000 assinaturas de aplicações para reconhecimento do tráfego;
- 7.2.12.11.68 A controladora wireless deve possuir interface de gerência integrada no próprio equipamento;
- 7.2.12.11.69 A controladora wireless deve possuir a funcionalidade de Fast-de roaming para aos enlaces mesh entre os nós secundários e principais;
- 7.2.12.11.70 A controladora wireless deve suportar aceleração de tráfego do protocolo CAPWAP através de um processador de rede específico para a função;
- 7.2.12.11.71 A controladora wireless deve suportar aceleração de encapsulamento de túnel de tráfego de bridge wireless através de um processador de rede específico para a função;
- 7.2.12.11.72 A controladora wireless deve suportar protocolo LLDP;
- 7.2.12.11.73 Deve permitir técnica de detecção de APs intrusos On-wire através de endereço MAC exato;
- 7.2.12.11.74 Deve permitir técnica de detecção de APs intrusos On-wire através de endereço MAC adjacente;
- 7.2.12.11.75 Deve permitir a visualização dos usuários conectados em forma de topologia lógica de rede representando a quantidade de dados transmitidos e recebidos;
- 7.2.12.11.76 A controladora wireless deve permitir combinar redes WiFi e redes cabeadas com um software switch integrado;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.11.77 A controladora wireless deve permitir criar um captive portal no software switch integrado para redes WiFi e redes cabeadas;

7.2.12.11.78 A controladora wireless deve permitir gerenciar switches de acesso do mesmo fabricante da solução ofertada;

7.2.12.11.79 Deverá suportar a conversão de Multicast a Unicast para melhorar o rendimento do airtime;

7.2.12.11.80 No ambiente de alta disponibilidade, deve existir a função dos controladores wireless primário e secundário na unidade AP, permitindo que a unidade decida a ordem em que o AP seleciona uma unidade controladora e como a unidade AP conecta à unidade controladora backup se a controladora primária falhar;

7.2.12.11.81 Deve fornecer capacidade para criar várias chaves pré-compartilhadas de acesso protegido WiFi (WPA-PSKs) para que o compartilhamento de PSK entre dispositivos não seja necessário.

7.2.12.12 Requisitos Mínimos de Funcionalidade – Solução Gerência Centralizada.

7.2.12.12.1 Deve permitir e estar licenciado para operar em alta disponibilidade (HA) sincronizando as mudanças na base de dados entre as estações de gerência;

7.2.12.12.2 Caso a solução seja virtualizada, deverá ser compatível com ambiente VMware ESXi 5.5 e 6.0;

7.2.12.12.3 Caso a solução seja virtualizada, deverá ser compatível com ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2;

7.2.12.12.4 Caso a solução seja virtualizada, deverá ser compatível com ambiente Citrix XenServer 6.0+;

7.2.12.12.5 Caso a solução seja virtualizada, deverá ser compatível com ambiente Open Source Xen 4.1+;

7.2.12.12.6 Caso a solução seja virtualizada, deverá ser compatível com ambiente KVM;

7.2.12.12.7 Caso a solução seja virtualizada, deverá ser compatível com ambiente Amazon Web Services (AWS);



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.12.8 Não deve possuir limite na quantidade de múltiplas vCPU caso entregue como appliance virtual;

7.2.12.12.9 Não deve possuir limite para suporte a expansão de memória RAM caso entregue como appliance virtual;

7.2.12.12.10 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

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

7.2.12.12.12 Permitir acesso concorrente de administradores;

7.2.12.12.13 Possuir interface baseada em linha de comando para administração da solução de gerência;

7.2.12.12.14 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

7.2.12.12.15 Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;

7.2.12.12.16 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

7.2.12.12.17 Gerar alertas automáticos via Email;

7.2.12.12.18 Gerar alertas automáticos via SNMP;

7.2.12.12.19 Gerar alertas automáticos via Syslog;

7.2.12.12.20 Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora;

7.2.12.12.21 Deve ser permitido ao administrador transferir os backups para um servidor FTP;

7.2.12.12.22 Deve ser permitido ao administrador transferir os backups para um servidor SCP



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.2.12.12.23 Deve ser permitido ao administrador transferir os backups para um servidor SFTP;

7.2.12.12.24 As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante;

7.2.12.12.25 Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS;

7.2.12.12.26 Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa TACACS;

7.2.12.12.27 Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de usuários de base externa LDAP;

7.2.12.12.28 Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa RADIUS;

7.2.12.12.29 Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de Certificado Digital X.509 (PKI);

7.2.12.12.30 Deve suportar sincronização do relógio interno via protocolo NTP;

7.2.12.12.31 Deve registrar as ações efetuadas por quaisquer usuários;

g.2.12.12.32 Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade;

g.2.12.12.33 Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;

g.2.12.12.34 Deve permitir habilitar e desabilitar, para cada interface de rede da solução de gerência, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;

g.2.12.12.35 Deve permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;

g.2.12.12.36 A solução de gerência deve permitir criar administradores que tenham acesso à todas as instâncias de virtualização;

g.2.12.12.37 Deve suportar XML API;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- g.2.12.12.38 Deve suportar JSON API;
- g.2.12.12.39 O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;
- g.2.12.12.40 O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- g.2.12.12.41 O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;
- g.2.12.12.42 Permitir localizar quais regras um objeto está sendo utilizado;
- g.2.12.12.43 Deve atribuir sequencialmente um número a cada regra de firewall;
- g.2.12.12.44 Deve atribuir sequencialmente um número a cada regra de DOS;
- 7.2.12.12.45 Permitir criação de regras que fiquem ativas em horário definido;
- g.2.12.12.46 Permitir backup das configurações e rollback de configuração para a última configuração salva;
- g.2.12.12.47 Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- g.2.12.12.48 Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
- g.2.12.12.49 Deve permitir que todos os firewalls sejam controlados de forma centralizada utilizando apenas um servidor de gerência;
- g.2.12.12.50 Cada servidor de gerência deve ser hospedado em um equipamento independente, não exercendo funções de firewall;
- g.2.12.12.51 A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta;
- g.2.12.12.52 A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

g.2.12.12.53 Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;

g.2.12.12.54 Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas as mesmas somente sejam aplicadas após aprovação de outro administrador;

g.2.12.12.55 Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;

g.2.12.12.56 Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência;

g.2.12.12.57 Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware;

g.2.12.12.58 Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos;

g.2.12.12.59 Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

g.2.12.12.60 Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;

g.2.12.12.61 Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência

g.2.12.12.62 Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada;

g.2.12.12.63 Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos;

g.2.12.12.64 Deve permitir criar regras de NAT64 e NAT46 de forma centralizada;

g.2.12.12.65 Permitir criar regras anti DoS de forma centralizada;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

g.2.12.12.66 Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

g.2.12.12.67 Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia;

g.2.13. Tipo 13 Sistema ininterrupto de energia elétrica (Nobreak):

g.2.13.1 Especificações Técnicas Mínimas

a.2.13.13.1 Forma de onda do inversor: Senoidal por aproximação;

7.2.12.13.2 Função Battery Saver. Microprocessador: RISC/FLASH de alta velocidade.

7.2.12.13.3 Tensão de entrada: Bivolt automático com seleção 115/127/220V

7.2.12.13.4 Tensão de saída de 115V~

a.2.12.13.5 Potência mínima de 2000 VA

a.2.12.13.6 Padrão para rack 19"

a.2.12.13.7 Mínimo de Tomadas: 5 no padrão NBR 14136.

a.2.12.13.8 Gerenciável

a.2.12.13.9 Deve permitir monitoramento via SNMP

7.2.12.13.10 Cartão de Gerenciamento SNMP externo

7.2.12.13.11 Led: 1 Led que indica o modo de operação. 6 níveis de proteção.

7.2.12.13.12 Conector: Tipo engate rápido para expansão de autonomia.

7.2.12.13.13 Filtro de linha.

7.2.12.13.14 Estabilizador interno com 4 estágios de regulação.

7.2.12.13.15 Forma de onda senoidal por aproximação (retangular PWM).

a.2.12.13.16 DC Start: permitir que o nobreak seja ligado na ausência de rede elétrica.

a.2.12.13.17 Battery Saver: evitar o consumo desnecessário das cargas da bateria, preservando a sua vida útil.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- a.2.12.13.18 Autodiagnóstico de bateria: informar quando a bateria precisa ser substituída.
- a.2.12.13.19 Recarga automática das baterias em 4 estágios, mesmo com o nobreak desligado.
- a.2.12.13.20 Recarregador Strong Charger: possibilitar a recarga das baterias mesmo com níveis muito baixos de carga.
- a.2.12.13.21 Conector do tipo engate rápido para conexão do módulo de bateria externo ao nobreak.
- a.2.12.13.22 Com 02(duas) baterias internas 12Vdc /7Ah, autonomia de no mínimo 1 hora.
- a.2.12.13.23 Função True RMS: indicada para todos os tipos de rede, principalmente redes instáveis.
- a.2.12.13.24 Microprocessador RISC/FLASH de alta velocidade: aumentar a 7.2.12.13.25 confiabilidade e o desempenho do circuito eletrônico interno.
- a.2.12.13.26 Autoteste: ao ser ligado, o nobreak testa os circuitos internos, garantindo assim o seu funcionamento ideal.
- a.2.12.13.27 Interativo - regulação on-line.
- a.2.12.13.28 Inversor sincronizado com a rede (sistema PLL).
- a.2.12.13.29 Circuito desmagnetizador: garantir o valor de tensão adequado para equipamentos de informática.
- a.2.12.13.30 Led colorido no painel frontal: indicar as condições de funcionamento do nobreak - modo rede, modo inversor/bateria, final de autonomia, subtensão, sobretensão, entre outras informações.
- a.2.12.13.31 Alarme audiovisual: sinalização de eventos como queda de rede, subtensão e sobretensão, fim do tempo de autonomia e final de vida útil da bateria, entre outras informações.
- a.2.12.13.32 Botão liga/desliga temporizado com função Mute: evitar o acionamento ou desacionamento acidental, além de desabilitar o alarme sonoro após a sinalização de algum evento.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

a.2.12.13.33 Porta fusível externo com unidade reserva.

7.2.12.13.34 Proteção:

- a) Curto-circuito no inversor;
- b) Surtos de tensão entre fase e neutro;
- c) Sub/sobretensão da rede elétrica. Na ocorrência destas, o nobreak passa a operar em modo bateria;
- d) Sobreaquecimento no inversor e no transformador;
- e) Potência excedida com alarme e posterior desligamento;
- f) Descarga total das baterias.

7.6. Especificações mínimas de Sistema Gerenciamento de link:

- i. A solução deverá atender as seguintes características mínimas:
- ii. Suportar os seguintes sistemas operacionais para monitoramento:
 - 1. Windows Server 2003 32/64 Bits
 - 2. Windows Server 2008 32/64 Bits
 - 3. Windows Server 2008 R2 64 Bits
 - 4. Windows Server 2012 64 Bits
 - 5. Windows Server 2012 R2 64 Bits
 - 6. Windows XP, Vista, 7, 8 32/64 Bits
 - 7. Linux/Unix
 - 8. MacOS
- iii. Sistemas Operacionais para Instalação da solução:
 - 1. Windows Server 2003 32/64 Bits



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

2. Windows Server 2008 32/64 Bits
 3. Windows Server 2008 R2 64 Bits
 4. Windows Server 2012
 5. Windows Server 2012 R2
 6. Windows 7 e 8
-
- iv. Suportar função de auto-descoberta de sensores para a rede;
 - v. Suportar configuração manual do dispositivo ou sensor;
 - vi. Monitoramento sem agente para a rede local;
 - vii. Suportar interface web compatível com os principais navegadores do mercado;
 - viii. Suportar visualização dos dados monitorados de várias instalações do produto em uma única aplicação;
 - ix. Permitir criptografia de conexão SSL para dados remotos e locais;
 - x. Possuir tecnologia de notificações de alertas, enviar e-mail, SMS / Pager, syslog, e Trap SNMP, solicitação HTTP, entrada de log de eventos, reproduzir arquivos de som, alarme Amazon SNS, ou outras tecnologias via arquivo de script;
 - xi. Monitorar redes separadas dentro da empresa (por exemplo, DMZ e LAN)
 - xii. Possuir alertas de limite de valor máximos e mínimos;
 - xiii. Agendamento de janela de manutenção por grupo ou por sensor;
 - xiv. Possuir sistemas de abertura de tickets automáticos por eventos no próprio software;
 - xv. Criar relatórios em formato HTML ou PDF;
 - xvi. Agendar tarefas de criação de relatórios, podendo ser executado como ad-hoc ou em intervalos regulares (diária, semanal, mensal);
 - xvii. Possuir dados de monitoramento históricos e exportação dos mesmos em HTML, CSV ou XML;
 - xviii. Permitir integração das bases de informação de monitoramento com outras aplicações via API de programação;
 - xix. Servidor web protegido por SSL (HTTPS) para a Web, Windows, iOS, Android e GUI;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- xx. Interfaces Web personalizáveis;
- xxi. Interface de administração em Português Brasil;
- xxii. Monitoramento distribuído - Instalação de vários pontos de monitoramento na organização, fazendo monitoramento local e passando os resultados para o servidor central sem custo adicional;
- xxiii. Possuir monitoramento de largura de banda usando WMI, NetFlow, jFlow, Packet Sniffing;
- xxiv. Monitoramento de Servidores e Estações de trabalho Windows com no mínimo os seguintes parâmetros:
 - a) Uso de CPU
 - b) Espaço em Discos
 - c) Uso de Memória
 - d) Uso de arquivo de paginação
 - e) Interface de Rede – Tráfego de entrada e saída
 - f) Tempo de atividade
- xxv. Monitoramento de Servidores e estações Linux com no mínimo os seguintes parâmetros:
 - g) Uso de CPU
 - h) Espaço em Discos
 - i) Uso de Memória
 - j) Tráfego de Rede
- xxvi. Monitoramento de protocolos:
 - a) HTTP (conteúdo, serviço e transação)
 - b) DNS
 - c) FTP e TFTP
 - d) IMAP (com tempo de envio e recepção com protocolo SMTP)
 - e) POP3 (com tempo de envio e recepção com protocolo SMTP)



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

g) SMTP

h) LDAP

i) SNTP

xxvii. QoS

xxviii. Monitorar Voip utilizando IP-SLA e QoS;

xxix. Monitoramento de Websites com registro de tempos de carregamento;

xxx. Permitir a criação de sensores customizados:

a) SNMP

b) WMI

c) SSH Script

d) HTTP

e) IPFIX

g) sFLOW

h) jFLOW

i) NETFLOW

xxxi. Monitoramento pré configurados de aplicações:

a) Windows IIS

b) Apache

c) Oracle Database

d) SQL Server 2005, 2008, 2012

e) SharePoint

f) MYSQL

g) Exchange

h) Serviços de Terminal (RDS/RDS)

xxxii. Monitoramento de ambientes virtualizados com os seguintes componentes prontos:

a) Vmware

a.1) Máquina Virtual

a.2) Desempenho de host



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

a.3) Armazenamento

b) MS Hypre-V Server

b.1) Máquina Virtual

b.2) Desempenho de Host

b.3) Armazenamento

c) Citrix Xen Server

c.1) Máquina Virtual

c.2) Desempenho de Host

xxxiii. Amazon Cloud

xxxiv. Permitir criação de consultas WMI Customizadas;

xxxv. Possibilitar a importação de dados MIBs;

xxxvi. Console de gerenciamento para dispositivos móveis com sistemas operacionais

xxxvii. iOS e Android;

xxxviii. Possibilidade de instalação em cluster para alta disponibilidade sem custo adicional;

xxxix. Licenciamento centralizado, aquisição dos sensores que independe da quantidade de localidade;

xl. Possuir seu próprio sistema de banco de dados, e-mail e servidor Web;

xli. Oferecer interfaces múltiplas para Web compatíveis com Windows / IOS App / Android App / HTML;

xlvi. Suporte e garantia prestados diretamente pelo fabricante da solução pelo período contratado;

xlvi. Possuir cluster de failover completo em todas as licenças para o monitoramento de alta disponibilidade;

xlv. Criação de Mapas de Rede personalizados com integração de sensores

xlv. Integração com sistema de mapa geográfico para georreferenciamento de dispositivos.

7.4 SOFTWARE DE GERENCIA DE REDES

7.4.1 Características Gerais

7.4.1.1 O Sistema de Gerência NMS deve possuir de forma integrada funcionalidades de



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

gerência de serviços, redes e elementos, com suporte para até 250 dispositivos, com até cinco acessos simultâneos.

7.4.1.2 O sistema deve apresentar Compatibilidade com modelo FCAPS do ITU-T

7.4.1.3 A aplicação deve ser compatível com os Sistemas operacionais Linux e Windows

7.4.1.4 O sistema deve ser modular, ou seja, apresentar possibilidade de instalar base de dados, servidor de aplicação, servidor Web e servidores de console em servidores físicos diferentes

7.4.1.5 O sistema deve ser compatível com as versões do Banco de dados Oracle 11 e 12

7.4.1.6 O instalador do Sistema deve fazer todas as verificações de requisitos necessárias para a correta instalação e operação do Sistema, bloqueando a instalação em caso de requisitos não-atendidos (HD, memória, versão e edição do sistema operacional, versão e status dos bancos de dados)

7.4.1.7 O sistema de gerência deve permitir ser instalado com alta disponibilidade, ou seja, provendo redundância, fail-over e load balancing para os serviços de gerência e acesso aos equipamentos da rede

7.4.1.8 O sistema deve ter Processamento paralelo e distribuído dos pollings dos equipamentos na rede, permitindo utilização máxima dos recursos de hardware disponíveis e ampliação da capacidade de equipamentos gerenciados através de escalabilidade horizontal (adição de novos servidores)

7.4.1.9 O sistema deve apresentar Visualização do estado de polling de conjuntos de equipamentos

7.4.1.10 O sistema deve possuir arquitetura extensível para novas interfaces south-bound

7.4.1.11 O sistema deve possuir arquitetura extensível para novas interfaces north-bound visando integração com outros sistemas (ex.: OSS)

7.4.1.12 Adição e edição de equipamentos e links via API REST

7.4.1.13 Permitir forward de traps SNMP para sistema north-bound (ex.: OSS)



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.4.1.14 Suportar SNMPv1, v2c e v3

7.4.1.15 Suportar operação Multiusuário

7.4.1.16 Permitir configuração de dados cadastrais dos equipamentos, e disponibilização desses dados nos relatórios de inventário

7.4.1.17 Oferecer busca com filtros por equipamentos, links e circuitos

7.4.1.18 A contratada deve apresentar Manual completo do sistema em português e inglês

7.4.1.19 O Sistema de apresentar Sistema de backup e recuperação automatizado

7.4.1.20 O Sistema deve permitir representação de equipamentos não-gerenciados (customizados) no mapa, com criação de links e customização de slots, portas e tipos de portas presentes

7.4.2 Representação Topológica e Descoberta de Redes

7.4.2.1 Apresentar mapa topológico hierarquizado, permitindo organização da rede em pastas e sub-pastas

7.4.2.2 Permitir propagação de status através do mapa topológico (se há uma falha na rede, ela é propagada até o nível mais alto da hierarquia topológica)

7.4.2.3 Permitir criação e visualização de links no mapa topológico

7.4.2.4 Permitir descoberta e adição múltipla de equipamentos, a partir de sub-rede ou range de Ips definido pelo usuário

7.4.2.5 Permitir criação de menus customizados a partir do mapa, para disparo de comandos do sistema operacional ou scripts

7.4.2.6 Permitir nos mapas topológicos - zoom in e zoom out



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.4.2.7 Permitir nos mapas topológicos - opção de auto-organização dos nodos (que representam os equipamentos)

7.4.3 Gerência de Falhas

7.4.3.1 Suportar Traps SNMPv1, v2c e v3

7.4.3.2 Suportar SNMP InformRequest

7.4.3.3 Permitir correlação de eventos por causa-raiz a partir das traps

7.4.3.4 Permitir Ack e terminação de eventos

7.4.3.5 Permitir construção de views customizadas filtrando eventos específicos (por equipamento, por severidade)

7.4.3.6 Permitir configuração de ações automatizadas a partir de eventos: e-mail, scripts e sons

7.4.3.7 Permitir exportação de eventos para CSV

7.4.3.8 Apresentar sumário com nome, modelo, descrição, número serial e status das placas e portas dos equipamentos

7.4.3.9 Status de elemento

7.4.3.10 Permitir visualização dos dados de status detalhados dos equipamentos (ex.: transceivers, digital diagnostic de transceivers)

7.4.3.11 Visualização de lista de alarmes, resumizando as falhas existentes no equipamento

7.4.3.12 Teste de conectividade (ping e protocolos de acesso utilizados pelo sistema de gerência, como SNMP, NETCONF, HTTP, SSH e Telnet)

7.4.3.13 Permitir customização da severidade de eventos e alarmes



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.4.3.14 Permitir visualizar e buscar as ONUs GPON (da rede toda, ou por equipamento), com todos os dados de status e configuração (estado operacional, ONUs descobertas, número serial, perfis configurados, banda configurada, firmware, nível de potência ótica TX/RX, etc)

7.4.3.15 Permitir monitoração de conectividade, identificando e informando ao usuário de forma rápida a perda ou retorno de conectividade com qualquer equipamento da rede

7.4.4 Gerência de Configuração

7.4.4.1 Configuração de elemento

7.4.4.2 Permitir configuração de elemento

7.4.4.3 Permitir funcionalidade preparada para qualquer nova versão de FW das linhas suportadas, sem necessidade de upgrade da plataforma, permitindo o suporte em campo a novos FWs em zero dias, no tocante à plataforma de gerência

7.4.4.4 Suportar configuração simultânea de múltiplas estruturas e/ou campos de configuração em uma única operação de usuário, criando e/ou editando itens, seja através de definição de range, ou da seleção dos itens desejados a alterar

7.4.4.5 Suportar auditoria completa de aplicações de configuração, com detalhamento dos objetos/parâmetros de configuração alterados no equipamento (ex.: VLAN, porta, ONU, etc)

7.4.4.6 Permitir uso do usuário e senha logados no sistema na conexão realizada com os equipamentos para aplicação de configuração

7.4.4.7 Suporte a YANG e NETCONF

7.4.4.8 Suportar Upgrade de Firmware em massa

7.4.4.9 Suportar Backup de configuração sob demanda ou agendável, para um ou múltiplos equipamentos.

7.4.4.10 Exportação e importação de backups de configuração para arquivo



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.4.4.11 Permitir provisionamento de circuitos fim-a-fim

7.4.4.12 Permitir provisionamento incluindo equipamentos não-gerenciados (customizados) no caminho

7.4.4.13 Permitir visualização de configuração em modo CLI (configuração em modo texto)

7.4.4.14 Templates CLI

7.4.4.15 Permitir criação e aplicação de templates CLI (configuração em modo texto) sobre SSH e Telnet em múltiplos equipamentos

7.4.4.16 Permitir opção de restrições de templates por modelo de equipamento e por versão de FW, para controle no momento da aplicação dos templates

7.4.4.17 Permitir criação em modo de desenvolvimento, homologação e produção, para controle da permissão de aplicação dos templates

7.4.4.18 Permitir funcionalidade preparada para qualquer nova versão de FW das linhas suportadas, sem necessidade de upgrade da plataforma e versão de Software, permitindo o suporte em campo a novos FWs em zero dias, no tocante à plataforma de gerência

7.4.4.19 Permitir suporte multivendor

7.4.4.20 Permitir suporte a linguagem de templates permitir a construção de qualquer conjunto de comandos (loops, condicionais, etc)

7.4.4.21 Permitir variáveis tipadas para restringir opções e facilitar operação (tipos texto, inteiro, seleção, read-only, com definição de valor default, ranges, regex e comandos para aplicação na rede no momento de configuração da variável)

7.4.4.22 Permitir exportação e Importação de templates

7.4.4.23 Permitir inclusão e/ou bloqueio de opções a partir de comandos lidos diretamente dos equipamentos



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.4.4.24 Permitir variáveis de equipamento (configuram nome ou IP de cada equipamento selecionado, e permitem criar fluxos com comandos CLI de sintaxe distinta conforme o modelo de cada equipamento selecionado)

7.4.4.25 Suportar auditoria detalhada de operações realizadas pelo usuário, incluindo todos os comandos aplicados com o retorno dado pelos equipamentos comando a comando

7.4.4.26 Permitir uso do usuário e senha logados no sistema na conexão realizada com os equipamentos para aplicação de templates CLI

7.4.5 Gerência de Desempenho

7.4.5.1 Permitir monitoração de tráfego em tempo real

7.4.5.2 Permitir gerenciar Taxa de upstream/downstream

7.4.5.3 Permitir gerenciar Erros in/out

7.4.5.4 Permitir gerenciar Pacotes perdidos

7.4.5.5 Permitir gerenciar Pacotes de broadcast, multicast e unknown

7.4.5.6 Permitir gerenciar Uso de CPU e memória

7.4.5.7 Permitir gerenciar Taxa de upstream/downstream de ONUs GPON

7.4.5.8 Permitir gerenciar potência ótica de ONUs GPON

7.4.6 Inventário

7.4.6.1 Suportar fazer Inventário físico de equipamentos

7.4.6.2 Suportar fazer Inventário físico de slots

7.4.6.3 Suportar fazer Inventário físico de portas

7.4.6.4 Suportar fazer Inventário físico de links



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.4.6.5 Suportar fazer Inventário físico de transceivers

7.4.6.6 Suportar fazer Inventário físico de ONUs

7.4.6.7 Permitir relatório de eventos

7.4.6.8 Permitir agendamento de relatórios, com granularidade mínima de 15 minutos

7.4.6.9 Permitir criação de relatórios favoritos

7.4.6.10 Permitir exportação de relatórios para formatos CSV, HTML, PDF, XLS e XLSX

7.4.6.11 Permitir envio de relatórios agendado por e-mail, FTP, SFTP e pasta de arquivos

7.4.6.12 Permitir rate-limit no inventário físico de portas

7.4.7 Gerência de Segurança

7.4.7.1 Suportar LDAP - Autenticação (suporte a OpenLDAP e Microsoft AD)

7.4.7.2 Suportar LDAP - Autorização (suporte a OpenLDAP e Microsoft AD)

7.4.7.3 Suportar acesso externo Web centralizado (single sign-on) (suporte a NetIQ Access Manager)

7.4.7.4 Permitir Configuração de user/senha/porta/retries/timeout, distinta por protocolo de acesso gerência => equipamento, para a rede toda e específica por equipamento, permitindo inclusive edição dos parâmetros específicos para múltiplos equipamentos simultaneamente

7.4.7.5 Suportar auditoria de operações realizadas pelos usuários no sistema, com usuário, data/hora e operação realizada

7.4.7.6 Suportar auditoria de Login (com sucesso ou com falha) e Logout (com sucesso)

7.4.7.7 Incluir IP do Usuário em registros de auditoria



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

7.4.7.8 Suportar permissão de Administrador (super-usuário)

7.4.7.9 Suportar permissões por usuário ou por grupo de usuários

7.4.7.10 Suportar permissões por modelo de equipamento, localidade no mapa topológico e por funcionalidades específicas (ex.: provisionamento de circuitos)

7.4.7.11 Apresentar opção de uso de CAPTCHA

7.4.7.12 Apresentar opção de integração com sistema de gerência externo single sign-on (sistemas do tipo Access Manager) para funcionalidades Web

7.4.7.13 Permitir configuração de timeout de sessão por usuário ou grupo de usuários

7.4.7.14 Permitir configuração de número de usuários simultâneos máximo para determinados grupos de usuários

7.4.7.15 Permitir configurações administrativas de segurança: mínimo e máximo de caracteres para nome de usuário e senha

7.4.7.16 Permitir configurações administrativas de segurança: obrigatoriedade de mudança de senha no primeiro login

7.4.7.17 Permitir configurações administrativas de segurança: bloqueio de conta de usuário após erro de senha por determinado número de vezes configurável

7.4.7.18 Permitir configurações administrativas de segurança: aging de senha com tempo configurável

7.4.7.19 Permitir janela para visualização de créditos a softwares de terceiros

7.5 Dos serviços de gerenciamento de ativos de rede:

7.5.1 A contratada será responsável pelos serviços de gerenciamento dos ativos de rede previstos no item 07 deste documento:

- 7.5.1.1 Gerenciamento de firewall;
- 7.5.1.2 Gerenciamento de roteadores;
- 7.5.1.3 Gerenciamento de switch;
- 7.5.1.4 Gerenciamento de wi-fi

7.5.2 O serviço de gerenciamento de ativos de rede, também deverá prover, monitorar, proteger, e manter os canais de transmissão de dados deste documento, sendo o gerenciamento de rede crucial para as equipes de TI identificarem e resolverem



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

proativamente problemas de rede, otimizar o desempenho, garantir a disponibilidade das transmissões de dados e, por fim, apoiar a continuidade e os resultados de negócios.

7.5.3 O serviço de gerenciamento de ativos de rede, também deverá executar as seguintes rotinas operacionais:

- 7.5.3.1 Gestão da política de backup e restauração dos ativos de rede do item 7
- 7.5.3.2 Disponibilidade e desempenho
- 7.5.3.3 Documentação de configuração
- 7.5.3.4 Gerência de mudanças
- 7.5.3.5 Planejamento de capacidades
- 7.5.3.6 Gerência de problemas
- 7.5.3.7 Controle de inventário
- 7.5.3.8 Gerenciamento de acesso a rede;
- 7.5.3.9 Gerenciamento de plano de resposta a incidentes;

8. DOS SERVIÇOS DE NOC, SOC E CSIRT PARA A REDE DE TELECOM

8. INFRAESTRUTURA

8.4. A CONTRATANTE cederá internamente em seus sites o espaço físico necessário e a infraestrutura básica (ar refrigerado, piso e iluminação).

8.2 Serão de responsabilidade da CONTRATADA os demais custos de infraestrutura inerentes à instalação: armário de telecomunicações; cabeamento e tubulação de entrada interna e para os equipamentos do tipo access point WI-FI, aterramento, quadro elétrico interno com disjuntor, circuito elétrico e protetor de surto para os equipamentos eletrônicos. Esta infraestrutura deverá ter o padrão mínimo aceitável pelas Normas vigentes, sendo esta exigência mandatória tanto para a sede do DETRAN-PA como para toda e qualquer CIRETRAN, POSTO DE SERVIÇO e DEMAIS PONTOS DE CLIENTES DO DETRAN - PA ficando a critério da CONTRATANTE proceder a fiscalização dos serviços executados.

8.3. A CONTRATADA deverá instalar um equipamento (No Break) um equipamento (Firewall tipo appliance), um roteador e no mínimo dois equipamentos tipo Access point WI-FI em cada Site remoto do DETRAN/PA (CIRETRAN, POSTO DE SERVIÇO, SOLUÇÃO



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

MÓVEL DE FISCALIZAÇÃO e demais pontos de clientes DO DETRAN/PA), ficando o critério de indicar o local de instalação dos equipamentos de Access point WI-FI sob a responsabilidade do DETRAN/PA contemplado neste edital, conforme especificação constante na letra (g) do item 3.2 deste Anexo.

8.4. Os materiais a serem utilizados na instalação devem ser de qualidade e propriedades físicas de acordo com as práticas de engenharia e normas técnicas em vigor, ou seja, devem ser aderentes às respectivas normas estabelecidas por Órgãos nacionais ou internacionais, acordados por ocasião da contratação do serviço.

8.5. A CONTRATADA deve prover o meio físico necessário para a interligação da Rede de Comunicação Digital até os circuitos de chegada nos sites central e remoto, incluindo os roteadores, quando necessários (Anexo IV), e as interfaces físicas para a integração nos ambientes determinados sobre o qual terá responsabilidade exclusiva, exceto quando pertencente ao cliente.

8.6 A CONTRATADA deve prover o meio físico em fibra ótica, com cabo de no mínimo 12 fibras apagadas e dedicadas ao detran, com 2 Backbones por caminhos distintos entre o DETRAN SEDE e o SITE de CONTINGÊNCIA com capacidade de 10gb, contemplando todos os equipamentos e acessórios necessários para o enlace.

8.6.1 O site de CONTINGÊNCIA, a critério da CONTRATANTE, será instalado na região metropolitana de Belém, sendo os 02 Backbones de interligação entre o DETRAN SEDE e o Site de CONTINGÊNCIA deverão ter capacidade de 10 Gb cada, do tipo determinísticos e simétricos, e deve atender a latência de 5ms (cinco milissegundos), conforme o item 6.3.1 deste documento.

8.7. A CONTRATADA deverá fornecer e instalar para os equipamentos da solução um Rack e opcionais necessários (bandeja, PDU, régua, etc) de no mínimo 20 U's para suporte de toda a infraestrutura de telecomunicações do site central (Ponta A) e deverá ser responsável também pela instalação de todos os conjuntos de equipamentos para acesso sem fio (Access points WI-FI e Switchs descritos no item 7.2 bem como todo o cabeamento e conectores (transceiver) lógico e elétrico necessário. Os pontos de instalação dos Access points WI-FI na sede do DETRAN/PA deverão ser instalados tanto na parte interna da sede como parte externa, sendo que estes locais serão informados posteriormente, após a



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

assinatura do contrato com a licitante vencedora, conforme a demanda e necessidade de cobertura de sinal WI-FI nas dependências da sede do DETRAN/PA. Estes Access points serão utilizados para atender os funcionários do DETRAN/PA em suas rotinas diárias e usuários.

8.8. ATESTADO DE PARTICIPAÇÃO NA VISITA TÉCNICA, fornecido pelo gerente ou responsável pelo DETRAN-PA onde realizou a visita atestando que tomou conhecimento de todas as informações e das condições para o cumprimento das obrigações objeto da licitação:

- a) A Visita Técnica ficará a critério do licitante, que poderá escolher um ou mais locais para fazer a visita nos locais de instalação dos equipamentos, de acordo com o descrito neste documento e deverá ser realizada pelo representante da empresa Licitante, devendo ser pré-agendada pelos interessados com 48 (quarenta e oito) horas de antecedência, através do e-mail dti@detran.pa.gov.br, sendo a confirmação respondida pelo mesmo meio.
- b) Na data e horário agendado, o responsável pela empresa, munido de documento com foto que o identifique, bem como, da comprovação de seu vínculo profissional com a licitante (cópia do contrato de trabalho, contrato social da empresa ou termo de autorização), deverá apresentar-se ao servidor representante do Departamento Estadual de Trânsito do Pará, DETRAN-PA.
- c) Essa Visita Técnica servirá para constatar as condições técnicas e operacionais, e, conjuntamente com os documentos que integram o presente edital, subsidiará o levantamento necessário ao perfeito desenvolvimento da execução dos serviços, assim como, à elaboração da proposta.
- d) Eventuais problemas observados na fase de vistoria e de elaboração da proposta deverão ser apontados formalmente a CPL- Comissão Permanente de licitação, antes da data prevista para a abertura do certame. Após esta data, nenhuma reclamação será aceita, não cabendo a licitante alegar o



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

desconhecimento das condições e do grau de dificuldade existentes como justificativa para se eximir das obrigações assumidas em decorrência deste Edital.

e) Caso a empresa opte por não realizar a visita técnica, deverá elaborar e apresentar à Comissão de Licitação, **Declaração renunciando à Visita Técnica** aos locais e as instalações para a prestação dos serviços e responsabilizando-se por manter as garantias da proposta comercial.

f) A proponente interessada deverá comprovar mediante apresentação de **Atestado de Capacidade Técnica** fornecido por pessoa jurídica de direito público ou privado para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação. Entende-se por compatível o percentual mínimo de 30% dos quantitativos estimados neste documento, contendo o atestado técnico as seguintes informações:

f1- Que a licitante fornece ou forneceu a prestação de serviço para **REDE DE COMUNICAÇÃO DIGITAL PRIVATIVA E INDEPENDENTE** descritos nos itens 5, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 6, 6.1, 6.1.1, 6.1.2, 6.1.3, 6.2, 6.2.1, 6.2.2, 6.2.3, 6.3, 6.4, 6.4.1, 6.4.2, 7 e 7.2 do ANEXO I.

f2- Que a licitante fornece ou forneceu a prestação de serviço para **SERVIÇO DE ACESSO PORTÁTIL E MÓVEL VIA SATÉLITE** descritos nos itens 12, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8 e 12.9. do ANEXO I.

f3- que a licitante fornece ou forneceu a prestação de serviço para **SERVIÇO DE SOLUÇÃO DE TELECOMUNICAÇÃO MÓVEL DE POSTO DE FISCALIZAÇÃO** descritos nos itens 14, 14.1, 14.1.1, 14.1.3, 14.3 e 14.3.1 do ANEXO I.

F4- que a licitante fornece ou forneceu a prestação de serviço para **SERVIÇO DE GERENCIAMENTO DE ATIVOS DE REDE** descritos nos itens 7.5.1.1 ao 7.5.1.4 e dos itens 7.5.3.1 a 7.5.3.9 do ANEXO I.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- g) No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.
- h) Fica resguardada ao Pregoeiro da Licitação a faculdade de executar diligências, para aferir veracidade das informações constantes dos atestados apresentados.
- i) O(s) atestado(s) de capacidade técnica deverá ser apresentado em papel timbrado, no qual deve ser informado, para fins de diligência: telefone, endereço, número do contato e duração, bem como os dados do responsável pela elaboração do atestado.
- j) A licitante deverá apresentar Declaração de que tem disponibilidade de equipamentos, veículos, pessoal técnico especializado, essenciais para o adequado cumprimento do objeto licitado.

k) DOCUMENTAÇÃO TÉCNICO-OPERACIONAL

k1-Licença SCM (serviço de comunicação multimídia) expedido pela ANATEL e que se encontre na condição de válida, com autorização para prestação dos serviços dentro do território do estado do Pará ou dentro de todo o território brasileiro, podendo a comprovação ser feita através de consulta no site da ANATEL, ou, através da apresentação do termo SCM da empresa licitante;

k2-Apresentação da certidão negativa de débitos de receitas administradas pela ANATEL (FUST, FUNTEL, TFF e contribuição para o fomento da radio fusão pública) que esteja vigente na data da abertura desta licitação, podendo a comprovação ser feita através de consulta no site da ANATEL;

k3- Registro válido, junto ao CREA (Conselho regional de Engenharia e Agronomia) do estado onde a empresa possua sua matriz.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

k4-Comprovação de que a empresa licitante possui em seu quadro técnico engenheiro com formação na área de telecomunicações, devendo o vínculo



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

de trabalho ser comprovado através de contrato de prestação de serviços, carteira de trabalho ou declaração de contratação futura;

k5 – Registro do engenheiro de telecomunicações da empresa licitante junto ao CREA (Conselho regional de Engenharia e Agronomia).

9. PENALIDADES PARA A REDE DE COMUNICAÇÃO DIGITAL PRIVATIVA E INDEPENDENTE

9.4. Caso ocorra degradação do tipo, aumento no tempo de resposta, ou aumento na taxa de erro, ou aumento na latência (entende-se por degradação como sendo toda interferência que venha causar sucessivas retransmissões de pacotes no circuito de dados), acumulativa superior a 4 (quatro) horas no período de 30 (trinta) dias, a CONTRATADA será penalizada com multa compensatória sobre o valor mensal do circuito a cada hora pelas interrupções temporárias a serem descontadas no preço da fatura do circuito, cumulativa até o máximo de 10% (dez por cento) do valor total da fatura mensal do circuito, conforme a tabela abaixo:

<i>Criticidade</i>	<i>Multa por hora</i>
<i>1</i>	<i>0,1%</i>
<i>2</i>	<i>0,25%</i>
<i>3</i>	<i>0,5%</i>
<i>4</i>	<i>0,75 %</i>
<i>5</i>	<i>1 %</i>

Tabela 2 - Aplicação de Penalidades por Degradação

9.2 Para aplicação do disposto neste item a CONTRATANTE terá que registrar junto a Central de Atendimento da CONTRATADA a ocorrência de degradação. Após o registro a CONTRATADA terá o período de 04 (quatro) horas para circuitos da Região Metropolitana



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

de Belém e 12 (doze) horas para os demais circuitos para testes e recuperação dos mesmos. Terminados estes prazos as multas compensatórias serão praticadas conforme a criticidade acima definida, considerando o período total de degradação registrado conforme o item 6.3.2 deste anexo.

9.3. Haverá desconto dos valores na fatura da CONTRATADA, nos termos deste item, conforme critérios de cálculo estabelecidos em caso de interrupção da prestação do serviço, que não sejam causadas por:

- a) Caso fortuito ou força maior (entende-se como caso fortuito como sendo qualquer ocorrência que não seja proveniente de qualquer ação humana).
- b) Operação inadequada, falha ou mau funcionamento de equipamentos não mantidos pela CONTRATADA.
- c) Falha de equipamento de propriedade ou sob responsabilidade da CONTRATADA, ocasionada pela CONTRATANTE ou seus clientes.
- d) Falha na infraestrutura da CONTRATANTE.
- e) Realização de testes, ajustes e manutenção necessários à prestação do serviço, devidamente comunicados à CONTRATANTE com antecedência mínima de 5 (cinco) dias úteis ou em caso comprovado de urgência, conforme item 6.4.5 deste documento.
- f) Impedimento, por qualquer motivo, do acesso de pessoal técnico da CONTRATADA às dependências da CONTRATANTE, onde estejam localizados os equipamentos da CONTRATADA ou por estes mantidos, desde que devidamente comunicados à CONTRATANTE.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

g) Falta de energia elétrica nas dependências da CONTRATANTE.

9.4. A CONTRATADA trabalhará de forma proativa informando à CONTRATANTE sobre o andamento do processo de recuperação em até 30 (trinta) minutos após o registro do problema e a cada intervalo de 2 (duas) horas, informando inclusive a estimativa de tempo para a completa solução do problema.

9.5. Falhas em equipamentos ou serviços de propriedade ou responsabilidade da CONTRATADA que impliquem em suspensão dos serviços prestados pela CONTRATANTE, motivarão a aplicação de multas compensatórias e descontos referentes à hora parada, ressalvado as condições listadas no item 9.4.

9.6. A CONTRATADA deverá executar a recuperação do circuito com problema em prazo determinado na coluna “Tempo Máximo de Reparo” do Anexo IV deste edital. Caso a CONTRATADA não consiga cumprir o prazo determinado pela CONTRATANTE para resolução do problema, incidirão multas compensatórias de 1% (um por cento) do valor mensal do circuito, para cada hora de paralisação, cumulativa até o máximo de 10% (dez por cento) do valor total da fatura mensal do circuito. Fica a critério da CONTRATANTE o desconto sobre a fatura mensal ao qual o circuito em questão esteja inserido, ou seu respectivo pagamento em conta, no prazo de até 30 (trinta) dias consecutivos.

Item	Critérios
Penalidade sobre o tempo de interrupção no circuito (fim-a-fim). Previsto para o não cumprimento do “Tempo Máximo de Reparo”	A cada hora de interrupção, após decorrido o tempo máximo de reparo constante no anexo IV, nas 2 (duas) primeiras horas
	A cada hora de interrupção contada após as 2 (duas) primeiras horas

Tabela 3 - Aplicação de Penalidades por Tempo Máximo de Reparo



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

9.7. O desconto referente à Hora Parada do Circuito será aplicado ao valor do circuito parado sob responsabilidade da CONTRATADA, conforme fórmula abaixo. Fica a critério da CONTRATANTE o desconto sobre a fatura mensal ao qual o circuito em questão esteja inserido, ou seu respectivo pagamento em conta, no prazo máximo de 30 (trinta) dias consecutivos.

de Horas Paradas.
$$\text{Valor do desconto por Hora Parada} = (\text{Valor do circuito} / 720) \text{ Quant.}$$

$$\text{Valor do desconto mensal} = \text{Quant. de Horas Paradas} \times \text{Valor do desconto por Hora Parada.}$$

Para efeito de cálculo, as penalidades deverão ser aplicadas baseadas em horas fracionadas.

10. GARANTIA E ASSISTÊNCIA TÉCNICA PARA A REDE DE COMUNICAÇÃO DIGITAL PRIVATIVA E INDEPENDENTE

10.4. A CONTRATADA deve prestar suporte operacional, através de sua equipe técnica disponível, para todas as unidades da Rede de Comunicação Digital.

10.5. A CONTRATADA deverá apresentar na fase de habilitação, declaração de que possui infraestrutura física dedicada ao suporte técnico e operacional mínima, própria ou alugada, na região metropolitana de Belém (PA), considerando-se como tal a existência de equipe técnica especializada própria, instalações físicas e equipamentos apropriados para o perfeito atendimento e manutenção dos serviços ofertados.

10.6. A Central de Assistência Técnica (call center) da CONTRATADA deve estar à disposição para recebimento de abertura de chamado técnico no período de atendimento do DETRAN/PA (das 08:00 as 18:00) de segunda a sexta, durante a execução do contrato.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

10.7. A Central de Assistência Técnica (call center) da CONTRATADA deve permitir comunicações de inoperância através de telefone franqueado (toll free) com atendimento em língua portuguesa, e através de endereço eletrônico (web ou e-mail), inclusive com a disponibilização de sistema web para acompanhamento, pela CONTRATANTE, das reclamações registradas.

10.8. A CONTRATADA deve dispor de uma estrutura capacitada para o atendimento às reclamações, acionando automaticamente às equipes de manutenção e o gerenciamento da recuperação do serviço.

10.9. Após a assinatura do contrato, a CONTRATADA deve apresentar todos os procedimentos e informações necessárias ao acionamento do seu serviço de suporte e solução de problemas, incluindo o comprovante de propriedade do imóvel através de escritura registrada em cartório ou contrato de aluguel onde a empresa está localizada dentro da região metropolitana de Belém, conforme descrito no item 10.2. O número de telefone 0800, em nome da contratada, nome e fabricante do software de gestão e controle para atendimento de chamado técnico licenciado em nome da contratada, conforme descrito no item 10.4.

11. IMPLANTAÇÃO DOS CIRCUITOS DE COMUNICAÇÃO DE DADOS PARA A REDE DE COMUNICAÇÃO DIGITAL PRIVATIVA E INDEPENDENTE

11.4. Os prazos de implantação dos circuitos de comunicação de dados deverão obedecer à coluna “Prazo de ativação dos circuitos” da planilha de circuitos do **Anexo IV, contados a partir da assinatura do contrato e emissão da ordem de serviço para ativação dos mesmos**. Caso a CONTRATADA não atenda aos prazos supracitados poderão, garantida a prévia defesa, ser aplicadas as sanções previstas no item 9.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

11.4.1. As eventuais alterações de velocidade terão prazos para sua execução de 2 (dois) dias úteis para circuitos terrestres e 60 (sessenta) dias para circuitos via satélite, a contar da data da solicitação formal emitida pela CONTRATANTE, salvo condições especiais levantadas pela CONTRATADA e com anuência da CONTRATANTE. Os eventuais remanejamentos (dentro da mesma localidade) terão prazo para sua execução de 30 (trinta) dias a contar da data da solicitação formal emitida pela CONTRATANTE, salvo condições especiais levantadas pela CONTRATADA e com anuência da CONTRATANTE.

11.1.2 Os serviços deverão ser entregues mediante Ordem de Serviço emitida pela DTI - Diretoria de Tecnologia e Informática, respeitando os prazos contidos na PPlanilha 1 do Anexo IV, coluna "Prazo de Ativação dos Circuitos (Dias Corridos), Após entrega de cada Ítem a Equipe Técnica da DTI procederá com testes no prazo máximo de 5 dias corridos e emitirá um TERMO DEFINITIVO DE ENTREGA.

11.5. O não cumprimento dos prazos citados no item anterior incorrerá em penalidades previstas no item 9.

11.6. Na implantação da substituição dos circuitos ativos da CONTRATANTE, a CONTRATADA deverá garantir o menor tempo possível de interrupção do circuito e transição segura, em concordância com a CONTRATANTE.

11.7. O faturamento dos circuitos referente ao mês que ocorrer a implantação/desativação terá seus valores proporcionais aos dias de utilização. Considera-se como data de desativação o 15º (décimo quinto) dia consecutivo após a data da formalização da CONTRATANTE junto a CONTRATADA.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

11.8. Qualquer intercorrência que possa existir durante o processo de desativação, deverá ser comunicada à CONTRATANTE até 5 (cinco) dias antes do vencimento do prazo de desativação. Caso, isso não ocorra e passados os 15 dias a CONTRATANTE se desobriga de qualquer responsabilidade sobre os bens de terceiros, desde que a intercorrência não seja de responsabilidade da CONTRATANTE.

11.9. As alterações de velocidades dos circuitos contratados deverão seguir a composição de custos de planilha específica constante neste documento, elaborada para compor valores de upgrade de velocidade em 100 % de sua capacidade, para todas os circuitos contratados a ser aplicadas após o 1º ano de contrato.

11.10. Em casos de emergência, durante o 1º ano de contrato, onde seja necessário o aumento de velocidade do link de determinada localidade, ficará a cargo da CONTRATANTE a qualquer momento solicitar à CONTRATADA o aumento de velocidade do link contratado.

12. CARACTERÍSTICAS TÉCNICAS PARA O SERVIÇO DE ACESSO PORTÁTIL E MÓVEL VIA SATÉLITE

12.4. A CONTRATADA deverá fornecer uma infraestrutura de Rede de Comunicação do tipo portátil e móvel, utilizando tecnologia de acesso via satélite permitindo que o DETRAN/PA tenha total autonomia para acessar a rede mundial de computadores, permitir o acesso a sua base de dados, em tempo real, utilizando link com banda mínima de download, independentemente de sua localização dentro do território do Estado do Pará.

12.5. O serviço de acesso portátil e móvel via satélite deve ter garantia de desempenho, privacidade e suporte a diversos protocolos, além de permitir a utilização de endereçamento IP privativo.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

12.6. O serviço de acesso portátil e móvel deve estar disponível 24 horas, 7 dias da semana, 365 dias do ano.

12.7. O serviço de acesso portátil e móvel será contratado com o fornecimento de todos os equipamentos e softwares necessários para a execução do serviço, sob a forma de locação mensal por kit de acesso portátil e móvel.

12.8. A manutenção e suporte técnico serão de responsabilidade da CONTRATADA sem ônus para o DETRAN/PA, salvo nos casos, onde, o dano, furto, falha técnica e ou defeito seja motivado por negligência, abuso, imperícia de funcionário do DETRAN-PA e ou seus prepostos ou casos fortuitos.

12.9. A CONTRATADA deverá fornecer mão de obra de técnico, pertencente ao seu quadro de funcionários sempre que o DETRAN/PA julgar necessário à sua presença, com o objetivo de prestar suporte técnico em qualquer localidade dentro do Estado Do Pará, sendo os custos de diárias, transportes, alimentação e hospedagem custeado pela CONTRATADA.

12.10. Durante o período do contrato, quando o DETRAN/PA solicitar um técnico da CONTRATADA para prestar suporte, a solicitação deverá ser feita com 24 (vinte e quatro horas) úteis de antecedência.

12.11. O serviço de acesso portátil e móvel deverá permitir que seja possível executar a transmissão de imagens.

12.12. A CONTRATADA deverá entregar os equipamentos na sede do DETRAN/PA dos tipos 1 e tipo 2, do **item 13**, no prazo de 30 (trinta) dias, contados a partir da assinatura do contrato e emissão da ordem de serviço nas quantidades ali estabelecidas, por tipo de equipamento, juntamente com seus notebooks e acessórios.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

13. ESPECIFICAÇÕES TÉCNICAS MÍNIMAS DOS EQUIPAMENTOS DO TIPO 1 E TIPO 2, RESPECTIVAMENTE, PORTÁTIL E VEICULAR DE ACESSO VIA SATÉLITE E SEUS ACESSÓRIOS.

13.4. Equipamento tipo 01- Portátil: terminal portátil capaz de fornecer conexão do tipo banda larga, via satélite, utilizando antena do tipo fixa, própria para ser utilizada de forma estacionária (local fixo), capaz de enviar e receber dados, voz e imagem com as seguintes características mínimas:

13.1.1 Peso do terminal não superior a 11 (onze) quilos, podendo ser transportado em maleta.

13.1.1 Possuir interfaces do tipo cabo ethernet do tipo RJ45 entre antena e roteador.

13.1.1 Alimentação do tipo AC 100 até 240 volts

13.1.1 Possuir tecnologia wi-fi do tipo 802.11 a/b/g/n/ac/ax, com padrão de segurança WPA2

13.1.1 Capacidade de download de 20 mbps.

13.1.1 Capacidade de upload de 10 mbps

13.1.1 Capacidade de trabalhar com VPN.

13.1.1 Capacidade de enviar e receber imagem de vídeo por streaming.

13.1.1 Resistência contra água e poeira categoria IP67 para a antena.

Todas as especificações acima descritas são mínimas.

13.5. Equipamento tipo 02 - Veicular: terminal móvel capaz de fornecer conexão do tipo banda larga via satélite, capaz de enviar e receber dados, voz e imagem, próprio para ser montado sobre o teto de veículos automotores com capacidade de funcionamento para a



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

transmissão e recebimento de dados, mesmo com o veículo em movimento, com as características mínimas abaixo:

13.2.1 Peso do terminal para ser instalado dentro do veículo não superior a 11(onze) quilos.

13.2.2 Possuir antena externa, própria para ser fixada sobre o teto do veículo utilizando sistema de fixação magnética ou por parafusos.

13.2.3 Possuir capacidade de alinhar a sua antena de forma automática em relação ao satélite, mesmo com o veículo em movimento, sem interferência humana.

13.2.4 Possuir tecnologia wi-fi do tipo 802.11 a/b/g/n/ac/ax, com padrão de segurança WPA2

13.2.5 Possuir capacidade de manter de forma contínua a transmissão e recepção de dados com o veículo em movimento e em velocidade superior a 100 km por hora.

Possuir interfaces do tipo ethernet, RJ45.

13.2.6 Alimentação do tipo DC, podendo operar com inversor veicular de 12 volts

13.2.7 Capacidade de download de 20 Mbps

13.2.8 Capacidade de upload de 10 Mbps

13.2.9 Capacidade de trabalhar com VPN.

13.2.10 Resistência contra água e poeira categoria IP67 para a antena.

13.2.11 Todas as especificações acima descritas são mínimas.

13.6. Acessórios que deve acompanhar cada terminal dos itens 13.1 e 13.2:

13.3.1 Maleta para transporte.

13.3.2. 1 (um) Computadores tipo notebook com Processador 12ª Geração Intel® Core™ i7-1255U (10-core, cache de 12MB, até 4.7GHz), tela de 15 polegadas, câmera HD de 720p a 30 FPS com microfone único integrado, Teclado não retro iluminado em português (Brasil), 2 portas USB 3.2 Type-A de 1ª geração, 1 porta



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

USB 2.0, 1 tomada de alimentação, 1 porta para headset (combinação de fones de ouvido e microfone), 1 porta HDMI 1.4 (a resolução máxima compatível com HDMI é de 1920 x 1080 a 60 Hz. Sem saída 4K/2K), sistema operacional Windows 11 pro, armazenamento SSD de 512GB PCIe NVMe M.2, Wireless 802.11ac 1x1 Wi-Fi, placa de rede wireless com Bluetooth, carregador e bolsa para transporte.

**14. CARACTERÍSTICAS TÉCNICAS DO SERVIÇO DE SOLUÇÕES DE
TELECOMUNICAÇÃO MÓVEL DE POSTO DE FISCALIZAÇÃO:**

14.4. A CONTRATADA deverá fornecer uma solução para o DETRAN/PA para que o mesmo possa oferecer para a sua equipe de fiscalização integrada a DTO (Diretoria técnica operacional) toda a infraestrutura necessária para que os agentes de fiscalização de trânsito possam executar suas atividades de orientação e fiscalização dos condutores e seus veículos que circulam em estradas e rodovias que estão sob a jurisdição do DETRAN-PA, de forma autônoma e continuada 24 horas por dia, 365 dias do ano.

A infraestrutura descrita neste documento deve contemplar todos os requisitos técnicos e operacionais que garantam o abrigo dos agentes contra intempéries das condições climáticas (vento forte, temporal, calor tórrido, chuva, etc.), a comunicação dos agentes com a sede do DETRAN/PA, a manutenção de suas necessidades fisiológicas, o suporte e manutenção continuada de todos os equipamentos fornecidos pela contratada dedicados para o envio e recebimento de dados, voz e imagem a partir dos equipamentos utilizados pelos agentes de trânsito e inerentes às atividades desenvolvidas pelos mesmos em campo, assim como, o fornecimento logístico para o transporte e instalação da solução e todo e qualquer equipamento dedicado a mesma.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

14.4.1. A infraestrutura de telecomunicação dedicada para esta solução deverá possuir obrigatoriamente as mesmas características técnicas para os circuitos terrestres fornecidas para as unidades do DETRAN (CIRETRANS) instaladas nos municípios dentro do território do estado do Pará, conforme descrito nos itens 5, 6, 6.3 e 6.4 do ANEXO I.

14.4.2. As soluções de fiscalizações móveis dos tipos A e B deverão obrigatoriamente serem atendidas por um circuito terrestre, com link dedicado, com capacidade de 20 mbps, item 4, descrito na planilha 2 do ANEXO V, conforme descrito no item 14.1.1 e um circuito do tipo satelital como redundância tipo 1, descrito no item 13, ANEXO I, com seus valores descritos nas planilhas 6 e 7 do ANEXO V.

14.4.2.1. As soluções de fiscalizações móveis dos tipos D, E, F e G deverão possuir o circuito satelital do tipo 2, descrito no item 13 do ANEXO I de forma continuada, montadas sobre caminhão e o ou viaturas, próprias para serem utilizadas de modo itinerante, com seus valores descritos nas planilhas 6 e 7 do ANEXO V.

14.4.3. A CONTRATADA deverá possuir estrutura própria para o transporte das soluções de fiscalização móveis para os modelos A,B e C composta por caminhão do tipo cavalo mecânico do tipo 6x2, equipado com equipamento próprio para içamento das soluções moveis de fiscalização do tipo munk, devendo a lança do munk ter no mínimo 15 metros de comprimento, com capacidade mínima de carga de 10 toneladas nesta configuração com capacidade para poder embarcar e desembarcar as unidades em qualquer localidade designada pelo DETRAN sempre que for solicitado, semirreboque do tipo carga seca, própria para o transporte de contêiner de até 12 metros de comprimento, equipada com 08 travas de segurança em sua estrutura para fixar container de 6 metros ou 12 metros, devendo os equipamentos serem de propriedade da contratada assim como o motorista ser funcionário da mesma, não sendo possível a subcontratação dos mesmos tendo em vista que a CONTRATADA deverá manter o serviço disponível para atendimento do DETRAN de forma continuada para o pronto atendimento dentro do prazo de 12 horas úteis, a partir da solicitação feita pelo DETRAN para efetuar a movimentação de uma solução de fiscalização móvel de um ponto A para um ponto B dentro do território do estado do Pará.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

14.4.3.1. O DETRAN irá pagar um valor único e específico para a CONTRATADA pelo deslocamento e instalação de uma solução móvel de fiscalização dos modelos A, B e C, quando for demandada, devendo a CONTRATADA manter sua infraestrutura descrita no item 14.1.3. de forma sempre disponível, não cabendo ao DETRAN o pagamento de qualquer valor referente a disponibilização desta infraestrutura a título de locação mensal, assim como, não terá qualquer responsabilidade pelo abastecimento de óleo combustível, alimentação do motorista, ajudante, despesas com diárias de hotel e ou quaisquer outros custos envolvidos na atividade dedicada para a execução da logística na movimentação de uma solução móvel de fiscalização, salvo, o valor específico descrito na planilha de preços 9 do ANEXO V, independentemente da distância entre a sede do DETRAN com a solução de fiscalização móvel dentro do território do estado do Pará, incluindo na logística também o transporte rodo/fluvial, quando existir a necessidade.

Toda e qualquer movimentação de uma solução móvel de fiscalização será feita mediante emissão de ordem de serviço.

14.4.4. A CONTRATADA deverá fornecer as soluções de fiscalização móveis dos modelos D, E e F, descrito no item 14.2.5, sob a forma de locação mensal para todos os itens, incluindo os itens veiculares (Cavalo Mecânico, semireboque, caminhão truck) descritas da planilha de valores 8 do ANEXO V.

14.5. Das características físicas e técnicas da solução de telecomunicação móvel de fiscalização:

14.2.1 As soluções móveis estão classificadas em 6 (seis) modelos com características físicas distintas, porém, com os mesmos propósitos quanto a sua natureza (fornecer a



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

infraestrutura necessária para a execução das rotinas de fiscalização de veículos e condutores) pelos agentes do DETRAN.

14.2.2. A quantidade de itens contidos nas soluções de telecomunicações móveis de fiscalização A, B, C, D, E e F, tanto na parte interna como parte externa, tais como câmera de CFTV, computador, mobiliário e etc. estão descritos nas quantidades mínimas, podendo o DETRAN solicitar o incremento de suas quantidades de acordo com suas necessidades.

14.2.3. Todos os equipamentos dedicados para serem usados de forma específica para um tipo solução de telecomunicação móvel ou de forma comum entre as soluções, contidas em quantidades, por tipo de solução de telecomunicação móvel, descritas no item 15 e seus subitens, com seus valores específicos na planilha de valores 8 do ANEXO V, contendo todas as especificações técnicas para cada equipamento dedicado para cada um dos modelos A, B, C, D, E e F descritos no item 14.2.5 formam o valor global de cada modelo.

14.2.4. Cada solução de fiscalização móvel deve possuir as medidas, características e equipamentos em suas medidas e quantidades mínimas, descritas conforme abaixo:

14.2.5. DAS CARACTERÍSTICAS PARA SOLUÇÃO MÓVEL DE FISCALIZAÇÃO DOS TIPOS A, B, C, D, E e F:

Item 14.2.5.1.MODELO A – Deve ser composta por 2 (duas) unidades confeccionadas em aço, com medidas externas medindo 12 metros de comprimento x 4.7 metros de largura depois de montados em paralelo, sendo necessário acoplar duas unidades medindo 12 de comprimento x 2.35 metros de largura x 2.35 metros de altura no sentido horizontal com o objetivo de ampliar a largura, do tipo fixo, área total: 56,4 m², o vão interno deve ser livre de paredes em toda a extensão dos 12 mts das duas unidades, permitindo o aproveitamento total da área para melhor disposição de mobiliários e circulação dos agentes e usuários, deve possuir 1 (uma) porta de acesso, confeccionada em aço, com trava de segurança com chave do tipo tetra para a solução na parte mais larga da solução, voltada para a via , medindo altura de 2.10mts com 1mt de largura, deve possuir 2(duas) janelas instaladas na mesma parede onde a porta de acesso está



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

instalada, devendo cada janela estar disposta à 2 metros da porta de acesso com as medidas de 1.60 metros de largura com 1 metro de altura feitas com vidro temperado e protegidas com grade metálica pela parte externa, possuir isolamento térmico do tipo atóxica e resistente ao fogo em todas as paredes externas e forro, com espessura de 10mm, deve possuir revestimento do piso do tipo vinílico na cor cinza claro, resistente a chamas e antiderrapante, deve possuir revestimento das paredes em pvc na cor branca, resistente ao fogo, deve possuir iluminação no teto com 4 luminárias redondas ou quadradas na cor branca, com 18 watts de potência cada uma, dispostas conforme desenho técnico, deve possuir 10 tomadas dedicadas a equipamentos de informática de 110/220 volts, 10 amperes, dispostas conforme detalhamento de desenho técnico, deve possuir 4 tomadas elétricas dedicadas para eletrodomésticos de 110/220 volts, 10 amperes, 1 (uma) tomada elétrica de 110 volts, 20 amperes disposta conforme detalhamento de desenho técnico, deve possuir 10 (dez) pontos de rede lógica dispostas, conforme detalhamento de desenho técnico, deve possuir abrigo para 2 (duas) VTR, medindo 6mts x 6mts x 2.5mts de altura, construída em estrutura metálica e revestida com telhas metálicas do tipo galvalume, com piso de concreto ou bloquete de concreto com 8cm de espessura, deve possuir cobertura metálica com telha térmica do tipo sanduíche (com revestimento metálico e ambas as faces) na parte frontal da solução para proteger agentes e usuários contra radiação solar e chuva medindo 12 metros de comprimento x com 3 metros de largura, montada sobre a parede frontal da solução com a porta de acesso, conforme desenho técnico, deve possuir 2 (dois) extintores de incêndio do tipo pó químico, classe ABC, de 6 quilos, com suporte para piso, deve possuir 2 (dois) extintores de incêndio do tipo CO2 de 6 quilos com suporte para piso, deve possuir demarcação no piso para os extintores de incêndio na cor vermelho medindo 70cm x 70cm, deve possuir 3 (três) aparelhos de ar-condicionado do tipo split, de 18.000 btus cada, deve ter as unidades condensadoras montadas na parte superior ou parede lateral traseira da solução, deve possuir quadro de disjuntores compatível com a carga elétrica para as tomadas elétrica e lógicas, aparelhos de ar-condicionado, iluminação, equipamentos de telecomunicações, equipamentos de vídeo monitoramento,



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

devendo os disjuntores serem individuais para cada aparelho de ar-condicionado, individual para o grupo de luminárias, tomadas elétricas e tomadas lógicas, equipamentos de telecomunicações e equipamentos de vídeo monitoramento composto por 2 câmeras tipo bullet, fixas, para uso interno, 3 câmeras bullet, fixas para uso externo, 4 computadores do tipo notebook, 1 (uma) impressora laser, deve possuir 1 (uma) tv led de 55 polegadas fixada na parede, conforme desenho técnico, deve possuir geladeira de 330 litros, deve possuir bebedouro de água de coluna, deve possuir mobiliário em quantidade, conforme demanda para acomodar o número necessário de agentes e usuários (condutores), deve possuir 1 (um) ponto de acesso wi-fi para uso interno dos agentes e usuários (condutores), deve possuir 1 (um) ponto de acesso wi-fi para uso externo montado em poste para uso dos agentes quando estiverem na via, deve possuir 1 (uma) solução descrita no item **13.1. Equipamento tipo 01**, deve possuir grupo gerador a diesel de 12kva, deve possuir programação visual em conformidade com o layout ou arte gráfica fornecida pelo DETRAN, deve possuir 1 (um) link terrestre de intranet de 20 mbps, item4, descrito na planilha 2 do ANEXO V

Item 14.2.5.2. MODELO B – Deve ser composta por 3 (três) unidades confeccionadas em aço, com medidas externas medindo 12 metros de comprimento x 2.35 metros de largura x 2.35 metros de altura cada uma das 3 unidades, sendo 2 unidades destinadas para execução de rotinas administrativas e fiscalização e 1 uma unidade dedicada para repouso e dormitório dos agentes, devendo as duas unidades administrativas serem montados em paralelo sendo necessário acoplar duas unidades medindo 12mts x 2.35mts no sentido horizontal com o objetivo de ampliar a largura, do tipo fixo, área total: 56,4 m², o vão interno deve ser livre de paredes em toda a extensão dos 12mts das duas unidades, permitindo o aproveitamento total da área para melhor disposição de mobiliários e circulação dos agentes e usuários, deve possuir 1(uma) porta de acesso, confeccionada em aço, com trava de segurança com chave do tipo tetra para a solução na parte mais larga da solução, voltada para a via, medindo altura de 2.10mts com 1mt de largura, deve possuir 2(duas) janelas instaladas na mesma parede onde a porta de acesso está instalada, devendo cada janela estar disposta à 2 metros da porta de



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

acesso com as medidas de 1.60 metros de largura com 1 metro de altura feitas com vidro temperado e protegidas com grade metálica pela parte externa, possuir isolamento térmico do tipo atóxica e resistente ao fogo em todas as paredes externas e forro, com espessura de 10mm, deve possuir revestimento do piso do tipo vinílico na cor cinza claro, resistente a chamas e antiderrapante, deve possuir revestimento das paredes em pvc na cor branca, resistente ao fogo, deve possuir iluminação no teto com 4 luminárias redondas ou quadradas na cor branca, com 18watts de potência cada uma, dispostas conforme desenho técnico, deve possuir 10 tomadas dedicadas a equipamentos de informática de 110/220 volts, 10 amperes, dispostas conforme detalhamento de desenho técnico, deve possuir 4 tomadas elétricas dedicadas para eletrodomésticos de 110volts, 10 amperes, 1 (uma) tomada elétrica de 110 volts, 20 amperes disposta conforme detalhamento de desenho técnico, deve possuir 10 (dez) pontos de rede lógica dispostas, conforme detalhamento de desenho técnico, deve possuir abrigo para 2 (duas) VTR, medindo 6mts x 6mts x 2.5mts de altura, construída em estrutura metálica e revestida com telhas metálicas do tipo galvalume, com piso de concreto ou bloquete de concreto com 8cm de espessura, deve possuir cobertura metálica com telha térmica do tipo sanduíche (com revestimento metálico e ambas as faces) na parte frontal da solução para proteger agentes e usuários contra radiação solar e chuva medindo 12 metros de comprimento x com 3 metros de largura, montada sobre a parede frontal da solução com a porta de acesso, conforme desenho técnico, deve possuir 2 (dois) extintores de incêndio do tipo pó químico, classe ABC, de 6 quilos, com suporte para piso, deve possuir 2 (dois) extintores de incêndio do tipo CO2 de 6 quilos com suporte para piso, deve possuir demarcação no piso para os extintores de incêndio na cor vermelho medindo 70cm x 70cm, deve possuir 3 (três) aparelhos de ar-condicionado do tipo split, de 18.000 btus cada, deve ter as unidades condensadoras montadas na parte superior ou parede lateral traseira da solução, deve possuir quadro de disjuntores compatível com a carga elétrica para as tomadas elétrica e lógicas, aparelhos de ar-condicionado, iluminação, equipamentos de telecomunicações, equipamentos de vídeo monitoramento, devendo os disjuntores serem individuais para



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

cada aparelho de ar-condicionado, individual para o grupo de luminárias, tomadas elétricas e tomadas lógicas, equipamentos de telecomunicações e equipamentos de vídeo monitoramento composto por 2 câmeras tipo bullet, fixas, para uso interno, 3 câmeras bullet, fixas para uso externo, 4 computadores do tipo notebook, 1 (uma) impressora laser, deve possuir 1 (uma) tv led de 55 polegadas fixada na parede, conforme desenho técnico, deve possuir geladeira de 330 litros, deve possuir bebedouro de água de coluna, deve possuir mobiliário em quantidade, conforme demanda para acomodar o número necessário de agentes e usuários (condutores), deve possuir 1 (um) ponto de acesso wi-fi para uso interno para uso dos agentes e usuários (condutores), deve possuir 1 (um) ponto de acesso wi-fi para uso externo montado em poste para uso dos agentes quando estiverem na via, deve possuir, deve possuir uma solução descrita no item **13.1. Equipamento tipo 01 com**, deve possuir grupo gerador a diesel de 12kva, deve possuir programação visual em conformidade com o layout ou arte gráfica fornecida pelo DETRAN e ;

Deve possuir a terceira unidade dedicada para área de repouso e dormitório para os agentes, podendo a critério do DETRAN ter essa unidade montada sobre uma das unidades administrativas ou no nível do solo, dependendo a área disponível do terreno, cabendo a CONTRATADA executar a instalação do mesmo, conforme estes critérios, devendo a unidade possuir o comprimento externo com 12mts x com largura de 2,35mts, deve possuir escada de acesso feita de metal com corrimão em ambos os lados com ângulo de inclinação não superior a 45 graus, com largura não inferior a 80cm de largura quando a unidade for montado sobre a unidade administrativa e fiscalização, deve possuir 1(uma) porta de acesso, confeccionada em aço medindo 2.10 metros de altura x 90cm de largura, com trava de segurança com chave do tipo tetra com toldo para proteção contra chuva, medindo 2 (dois) metros de largura x 1.5 metros de comprimento, confeccionado em aço, incluído sua cobertura em telha do tipo galvalume, deve possuir 2(duas) janelas instaladas na mesma parede onde a porta de acesso está instalada, devendo cada janela estar disposta à 2 metros da porta de acesso com as medidas de 1.60 metros de largura com 1 metro de altura feitas com



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

vidro temperado e protegidas com grade metálica pela parte externa, possuir isolamento térmico do tipo atóxica e resistente ao fogo em todas as paredes externas e forro, com espessura de 10mm, deve possuir revestimento do piso do tipo vinílico na cor cinza claro, resistente a chamas e antiderrapante, deve possuir revestimento das paredes em pvc na cor branca, resistente ao fogo, deve possuir iluminação no teto com 4 luminárias redondas ou quadradas na cor branca, com 18watts de potência cada uma, dispostas conforme desenho técnico, deve possuir 4 tomadas dedicadas a equipamentos de informática de 110/220 volts, 10 amperes, dispostas conforme detalhamento de desenho técnico, deve possuir 6 (seis) tomadas elétricas dedicadas para eletrodomésticos de 110/220 volts, 10 amperes, dispostas conforme detalhamento de desenho técnico, deve possuir, deve possuir 1 (uma) tomada 110/220 volts, 20 amperes dedicada para o forno de microondas, 1 (um) roteador wi-fi montado sob o teto, 1 (uma) mesa redonda, 4 (quatro) cadeiras, 4 (quatro camas) 4 (quatro) travesseiros, 4 (quatro) mesa de cabeceira, 1 (um) sofá, 1 (uma) geladeira, 2(dois) ar condicionado split de 12.000 btus, 1 (uma) tv de 55 polegadas, 1 (um) forno de microondas, 1 (uma) cafeteira, 1 (um) bebedouro de água de coluna, deve possuir 1 (um) extintor de incêndio do tipo pó químico, classe ABC, de 6 quilos, com suporte para piso, deve possuir 1 (um) extintor de incêndio do tipo CO2 de 6 quilos com suporte para piso, deve possuir demarcação no piso para os extintores de incêndio na cor vermelho, deve possuir 1 (um) deve possuir piso externo (base de apoio) em concreto ou bloquete, quando o mesmo for montado no nível do solo, devendo o piso possuir 14 metros de comprimento por 4 metros de largura, deve possuir 1 (um) link terrestre de intranet de 20mbps, item4, descrito na planilha 2 do ANEXO V.

Item 14.2.5.3. MODELO C – Deve ser composta por 1 (uma) unidade confeccionada em aço, medindo 6 metros de comprimento x 2.35 metros de largura x 2.35 metros de altura dedicado para banheiro feminino e masculino, devendo possuir isolamento térmico do tipo atóxica e resistente ao fogo em todas as paredes internas e forro, com espessura de 10mm, deve possuir revestimento do piso do tipo vinílico na cor cinza claro,



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

resistente a chamas e antiderrapante, deve possuir revestimento das paredes em pvc na cor branca, resistente ao fogo, deve possuir iluminação no teto com 2 (duas) luminárias redondas ou quadradas na cor branca, com 18watts de potência cada uma, deve possuir uma divisória separando a solução ao meio, permitindo a disponibilidade de 2 (dois) banheiros completos e separados para uso feminino e masculino, devendo a divisória separar os ambientes desde o piso até o teto com isolamento total entre os ambientes, deve possuir 2 (duas) portas de acesso confeccionadas em aço, medindo 2.10mts de altura x 90cm de largura, com fechadura específica para fechamento somente pela parte de dentro do ambiente, deve possuir toldo para proteção contra chuva, medindo 2 (dois) metros de largura x 1.5 metros de comprimento, confeccionado em aço, incluído sua cobertura em telha do tipo galvalume, deve possuir 2 chuveiros com box em vidro temperado, deve possuir 2 vasos sanitário com caixa acoplada, deve possuir 2 pias com cuba de sobrepor, deve possuir armário para receber a pia, deve possuir espelho montado sobre o armário, deve possuir 4 (quatro) exaustores, sendo 2 (dois) para cada banheiro, deve possuir grade de ventilação com tela anti inseto confeccionada em aço com venezianas medindo 50cm x 25cm para circulação de ar, deve possuir caixa d'água com capacidade para 1.000 litros com sistema de bóia de nível automático, montada sobre a estrutura da solução, deve possuir fossa do tipo séptica, deve possuir poço artesiano de 4 polegadas com bomba d'água submersa, deve possuir 2 (dois) porta papel higiênico, deve possuir 2 (dois) porta toalhas de rosto, deve possuir 2 (dois) porta toalhas de banho, deve possuir 4 (quatro) cabide para suporta roupa, deve possuir 2 (duas) lixeiras, deve possuir programação visual na parte externa, conforme determinada pelo DETRAN

Item 14.2.5.4. MODELO D – Deve ser composta por 1 (uma) unidade, tipo container em aço, montado sobre semirreboque carga seca, própria para transporte de container com as travas de fixação do mesmo sobre seu piso, com medidas externas medindo 12mts de comprimento x 2.35mts de largura x 2.35 metros de altura, deve possuir 1(uma) porta de acesso pela parte traseira em relação a rampa de acesso do semirreboque, confeccionada em aço, com trava de segurança com chave do tipo tetra, medindo altura



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

de 2.10mts com 1mt de largura, deve possuir toldo de cobertura sobre a porta confeccionado em aço com 2 metros de largura por 1 metro de profundidade, deve possuir isolamento térmico do tipo atóxica e resistente ao fogo em todas as paredes externas e forro, com espessura de 10mm, deve possuir revestimento do piso do tipo vinílico na cor cinza claro, resistente a chamas e antiderrapante, deve possuir revestimento das paredes em pvc na cor branca, resistente ao fogo, deve possuir iluminação no teto com 4 luminárias redondas ou quadradas na cor branca, com 18watts de potência cada uma, dispostas conforme desenho técnico, deve possuir 10 tomadas dedicadas a equipamentos de informática de 110/220 volts, 10 amperes e dispostas conforme detalhamento de desenho técnico, deve possuir 4 tomadas elétricas dedicadas para eletrodomésticos de 110/220 volts, 10 amperes, 1 (uma) tomada elétrica de 110/220 volts de 20 amperes disposta conforme detalhamento de desenho técnico, deve possuir 10 (dez) pontos lógicos dispostos, conforme desenho técnico, deve possuir 2 (dois) extintores de incêndio do tipo pó químico, classe ABC, de 6 quilos, com suporte para piso, deve possuir 2 (dois) extintores de incêndio do tipo CO2 de 6quilos com suporte para piso, deve possuir demarcação no piso para os extintores de incêndio na cor vermelho medindo 70cm x 70cm, deve possuir 2 (dois) aparelhos de ar-condicionado do tipo split, de 18.000 btus cada, deve ter as unidades condensadoras montadas na parte superior ou parede da solução que fica atrás da cabine do cavalo mecânico, deve possuir quadro de disjuntores compatível com a carga elétrica para as tomadas elétrica e lógicas, aparelhos de ar-condicionado, iluminação, equipamentos de telecomunicações, equipamentos de vídeo monitoramento, devendo os disjuntores serem individuais para cada aparelho de ar-condicionado, individual para o grupo de luminárias, tomadas elétricas e tomadas lógicas, equipamentos de telecomunicações e equipamentos de vídeo monitoramento composto por 2 câmeras tipo bullet, fixas, para uso interno, 3 câmeras bullet, fixas para uso externo, 4 computadores do tipo desk top, 1 (uma) impressora laser, deve possuir 1 (uma) tv led de 55 polegadas fixada na parede, conforme desenho técnico, deve possuir 4 mesas retangulares medindo 1.35 metros de largura x 60 cm de comprimento x 75 cm de altura, cor cinza, pés de metal, com 2



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

gavetas, deve possuir 6 cadeiras para escritório, deve possuir bebedouro de água de coluna, deve possuir 4 armários, mobiliário, deve possuir 1 (um) ponto de acesso wi-fi para uso interno para uso dos agentes e usuários (condutores), deve possuir 1 (um) ponto de acesso wi-fi para uso externo montado sobre o teto da solução para uso dos agentes quando estiverem na via, deve possuir uma solução descrita no item **13.2. Equipamento tipo 02** - deve possuir grupo gerador a diesel de 10kva, deve possuir 1 banheiro equipado com vaso sanitário, 1 mictório, 1 pia de sobrepor, 1 armário, 2 exaustores, 2 entradas e saídas de ar para circulação com grade do tipo veneziana e protegida com tela em aço contra mosquitos medindo 30cm x 30cm, possuir 1 luminária de teto de led com potência de 18w com luz branca, interruptor individual para acionamento dos exaustores e luminária, deve possuir um reservatório de água potável com capacidade de 500 litros, montado na parte externa da solução para abastecer pia, vaso sanitário e mictório, deve possuir caixa coletora de água servida proveniente do banheiro montado no chassi do semirreboque com capacidade para 2.000 litros com válvula para drenagem por sucção ou por gravidade, deve possuir programação visual em conformidade com o layout ou arte gráfica fornecida pelo DETRAN, o semirreboque deve possuir suspensão a ar, ser de 2 eixos, possuir rampas eletro-hidráulica fechada em chapa xadrez de aço, possuir válvula nivelamento doca, deve possuir 8 pinos lock , possuir inclinação traseira, possuir 2 conj. de pés mecânicos acionados por manivela (1 dianteiro/ 1 traseiro), deve possuir 1 (uma) cavalo mecânico para executar o reboque do conjunto da solução.

Item 14.2.5.5. MODELO E– Deve ser composta por 1 (uma) unidade, tipo container em aço ou alumínio montado sobre caminhão com chassi, próprio para receber esse tipo de estrutura fixada sobre chassi, com medidas externas medindo 6 metros de comprimento x 2.30 metros de largura x 2.35 metros de altura, deve possuir 1 porta confeccionada em aço ou alumínio, com trava de segurança com chave do tipo tetra , medindo altura de 2.10 mts com 1mt de largura, deve possuir 1(uma) plataforma hidráulica montada na parte traseira do chassi para servir como plataforma de acesso



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

para a solução de telecomunicação móvel de fiscalização porta de acesso pela parte traseira em relação a rampa hidráulica, deve possuir escada dobrável para ser utilizada para acesso a plataforma com ângulo não superior a 45 graus, com corrimão do lado direito, deve possuir isolamento térmico do tipo atóxica e resistente ao fogo em todas as paredes, incluído o teto, com espessura de 10mm, deve possuir revestimento do piso do tipo vinílico na cor cinza claro, resistente a chamas e antiderrapante, deve possuir revestimento das paredes em pvc na cor branca, resistente ao fogo, deve possuir iluminação no teto com 3 luminárias redondas ou quadradas na cor branca, com 18watts de potência cada uma, dispostas conforme desenho técnico, deve possuir 4 tomadas dedicadas a equipamentos de informática de 110/220 volts, 10 amperes e dispostas conforme detalhamento de desenho técnico, deve possuir 2 tomadas elétricas dedicadas para eletrodomésticos de 110/220 volts, 10 amperes, disposta conforme detalhamento de desenho técnico, deve possuir 4 (quatro) pontos lógicos dispostos, conforme desenho técnico, deve possuir 1 (um) extintor de incêndio do tipo pó químico, classe ABC, de 6 quilos, com suporte para piso, deve possuir 1 (um) extintor de incêndio do tipo CO2 de 6quilos com suporte para piso, deve possuir demarcação no piso para os extintores de incêndio na cor vermelho medindo 70cm x 70cm, deve possuir 1 (um) aparelho de ar-condicionado do tipo split, de 18.000 btus montado na parede oposta a parede da porta de acesso, deve ter a unidade condensadora montada embutida na parte superior da solução que fica atrás da cabine do caminhão, deve possuir quadro de disjuntores compatível com a carga elétrica para as tomadas elétrica e lógicas, aparelho de ar-condicionado, iluminação, equipamentos de telecomunicações, equipamentos de vídeo monitoramento, devendo os disjuntores serem individuais para o aparelho de ar-condicionado, individual para o grupo de luminárias, tomadas elétricas e tomadas lógicas, equipamentos de telecomunicações e equipamentos de vídeo monitoramento composto por 2 câmeras tipo bullet, fixas, para uso interno, 4 câmeras bullet, fixas para uso externo, montadas sobre o teto dispostas em cada um dos cantos da solução capturando imagens ao redor da solução, 2 computadores do tipo notebook, 1 (uma) impressora laser, deve possuir 1 (uma) tv led de 55 polegadas fixada na parede,



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

conforme desenho técnico, deve possuir 3 mesas retangulares medindo 1.35 metros de largura x 60 cm de comprimento x 75 cm de altura, cor cinza, pés de metal, com 2 gavetas, deve possuir 6 cadeiras para escritório, deve possuir bebedouro de água de coluna, deve possuir 1 armário, mobiliário, deve possuir 1 (um) ponto de acesso wi-fi para uso interno para uso dos agentes e usuários (condutores), deve possuir 1 (um) ponto de acesso wi-fi para uso externo montado sobre o teto da solução para uso dos agentes quando estiverem na via, deve possuir, deve possuir grupo gerador a diesel de 7 kva montado abaixo da solução e fixado no chassi do caminhão, deve possuir 2 exaustores, 2 entradas e saídas de ar para circulação com grade do tipo veneziana e protegida com tela em aço contra mosquitos medindo 30cm x 30cm montadas nas laterais da solução deve possuir uma solução descrita no item **13.2. Equipamento tipo 02** – montada sobre o teto, deve possuir sistema para travar todos mobiliários ao piso da solução para manter os mesmos fixos durante o deslocamento da solução.

Item 14.2.5.6. MODELO F– Deve ser composta por 1 (uma) unidade, tipo container em aço, montado sobre semirreboque carga seca, própria para transporte de container com as travas de fixação do mesmo sobre seu piso, com medidas externas medindo 12 metros de comprimento x 2.35 metros de largura x 2.35 metros de altura, deve possuir 1(uma) porta de acesso pela parte traseira em relação a rampa de acesso do semirreboque, confeccionada em aço, com trava de segurança com chave do tipo tetra, medindo altura de 2.10mts com 1mt de largura, deve possuir toldo de cobertura sobre a porta confeccionado em aço com 2 metros de largura por 1 metro de profundidade, deve possuir isolamento térmico do tipo atóxica e resistente ao fogo em todas as paredes externas e forro, com espessura de 10 mm, deve possuir revestimento do piso do tipo vinílico na cor cinza claro, resistente a chamas e antiderrapante, deve possuir revestimento das paredes em pvc na cor branca, resistente ao fogo, deve possuir iluminação no teto com 4 luminárias redondas ou quadradas na cor branca, com 18watts de potência cada uma, dispostas conforme desenho técnico, deve possuir 6 (seis) tomadas dedicadas a equipamentos de informática de 110/220 volts, 10 amperes e



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

dispostas conforme detalhamento de desenho técnico, deve possuir 2 (duas) tomadas elétricas dedicadas para eletrodomésticos de 110/220 volts, 10 amperes, dispostas conforme detalhamento de desenho técnico, deve possuir 6 (seis) pontos lógicos dispostos, conforme desenho técnico, deve possuir 2 (dois) extintores de incêndio do tipo pó químico, classe ABC, de 6 quilos, com suporte para piso, deve possuir 2 (dois) extintores de incêndio do tipo CO2 de 6quilos com suporte para piso, deve possuir demarcação no piso para os extintores de incêndio na cor vermelho medindo 70cm x 70cm, deve possuir 2 (dois) aparelhos de ar-condicionado do tipo split, de 18.000 btus cada, deve ter as unidades condensadoras montadas na parte superior ou parede da solução que fica atrás da cabine do cavalo mecânico, deve possuir quadro de disjuntores compatível com a carga elétrica para as tomadas elétrica e lógicas, aparelhos de ar-condicionado, iluminação, equipamentos de telecomunicações, equipamentos de vídeo monitoramento, devendo os disjuntores serem individuais para cada aparelho de ar-condicionado, individual para o grupo de luminárias, tomadas elétricas e tomadas lógicas, equipamentos de telecomunicações e equipamentos de vídeo monitoramento composto por 2 câmeras tipo bullet, fixas, para uso interno, 4 câmeras bullet, fixas para uso externo, 4 computadores do tipo note book, 4 (quatro) no break, 1 (uma) impressora laser, deve possuir 1 (uma) tv led de 55 polegadas fixada na parede, conforme desenho técnico, deve possuir 4 mesas de escritório retangulares medindo 1.35 metros de largura x 60 cm de comprimento x 75 cm de altura, cor cinza, pés de metal, com 2 gavetas, deve possuir 6 cadeiras para escritório, deve possuir bebedouro de água de coluna, deve possuir 1 armário, mobiliário, deve possuir 1 (um) ponto de acesso wi-fi para uso interno para uso dos agentes e usuários (condutores), deve possuir 1 (um) ponto de acesso wi-fi para uso externo montado sobre o teto da solução para uso dos agentes quando estiverem na via, deve possuir, deve possuir grupo gerador a diesel de 10kva, 2 exaustores, 2 entradas e saídas de ar para circulação com grade do tipo veneziana e protegida com tela em aço contra mosquitos medindo 30cm x 30cm montadas com altura de 2 metros em relação ao piso, devendo ser em cada uma das paredes laterais da solução situadas na parte frontal da solução



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

em relação a cabine do cavalo mecânico e os 2 exaustores montados na parte traseira ao lado da porta de acesso com altura de 2.1 metros em relação do piso com interruptor individual para acionamento dos exaustores e luminária, deve possuir uma solução descrita no **item 13.2. Equipamento tipo 02** – sobre o teto da solução, deve possuir sistema para travar todos mobiliários ao piso da solução para manter os mesmos fixos durante o deslocamento da solução, possuir programação visual em conformidade com o layout ou arte gráfica fornecida pelo DETRAN, deve possuir 1 (um) semirreboque com suspensão a ar, ser de 2 eixos, possuir rampas eletro-hidráulica fechada em chapa xadrez de aço, possuir válvula nivelamento doca, possuir 8 pinos lock , possuir inclinação traseira, possuir 2 conj. de pés mecânicos acionados por manivela (1 dianteiro/ 1 traseiro), deve possuir cavalo mecânico para executar o reboque do conjunto da solução, deve possuir 1 (um) caminhão do tipo cavalo mecânico.

14.6. Da logística e infraestrutura da base da solução de telecomunicação móvel de fiscalização dos tipos A, B e C:

14.3.1. A CONTRATADA será a única responsável pelo transporte das soluções móveis de fiscalização dos tipos A, B e C até o seu local de destino designado pelo DETRAN/PA para que o mesmo possa ser instalado e posto em operação, conforme descrito nos itens 14.1.3. e 14.1.4, devendo a contratada providenciar além do transporte a adequação do espaço físico designado para a devida instalação, conforme segue:

14.3.2. Preparação do piso onde a solução móvel será instalada, devendo o piso ser de concreto armado ou bloquete de concreto com 8 cm de altura, onde a área total a ser coberta deverá ser de no mínimo de 300 metros quadrados, cabendo ao DETRAN o fornecimento da área compatível para que a CONTRATADA possa executar as adequações necessárias para a instalação de uma ou mais unidades, incluindo ainda todo e qualquer serviço de terraplanagem;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

14.3.3. Perfuração de Poço artesiano conforme as normas técnicas 12212 e 12244 da ABNT com 4 polegadas de diâmetro, compatível com a necessidade da captura e produção mínima diária de 3.000 litros de água, bomba d'água submersa com seu quadro de comando com capacidade de produção de 3.000 litros diário, abrigo para o quadro de comando contra intempéries dotado de porta de acesso para o mesmo, sistema de tratamento de água Filtro de Zeólita para Remoção de Ferro e Manganês com retrolavagem compatível com a demanda de até 3.000 litros por dia, com capacidade para eliminar odor e impurezas como ferro e dureza, sistema de abastecimento de água com caixa d'água feita em polietileno com 1000 litros de capacidade, montada sobre a estrutura móvel de fiscalização ou ao lado da mesma em estrutura de concreto, com acionamento automático da bomba submersa para manutenção do nível através de boia de nível;

14.3.4. A CONTRATADA deverá fornecer sistema de coleta de água servida com uso de fossa séptica com filtro biológico compatível ao uso diário por 6 adultos, 7 dias da semana, conforme a norma ABNT 7229;

14.3.5. A CONTRATADA deverá instalar uma cobertura feita em polietileno de alta densidade em material sintético, cor preta ou cinza, semi permeável, capaz de bloquear até 80% dos raios de sol com o objetivo de melhor conforto térmico para os usuários e agentes de fiscalização, quando estiverem fazendo abordagem na área de pátio de uma solução, devendo esta cobertura possuir no mínimo 110 metros quadrados , devendo esta cobertura possuir 2.5 metros de altura a partir do solo, ser montada com uso de estrutura metálica na cor branca ou cinza claro, fixada no solo com uso de parafusos do tipo parabolt;

14.3.5.1. O local de instalação desta cobertura será de acordo com o layout e posicionamento da solução de fiscalização móvel, cabendo a CONTRATADA seguir as orientações do DETRAN;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

14.3.6. Caberá a contratada providenciar todo o encaminhamento do cabeamento elétrico entre a unidade consumidora de energia fornecida pela distribuidora de energia Equatorial até o quadro de disjuntores da solução de fiscalização móvel na bitola compatível com a carga elétrica, devendo este cabeamento ser encaminhado via subterrânea com eletrodutos, utilizando cabos com fios de cobre eletrolítico nu ou alumínio 1350, encordoamento classe 2 compacto, com bloqueio longitudinal de umidade – conforme NBR NM 280 (IEC 60228), Isolação: composto termofixo de EPR (borracha de etileno propileno) ou XLPE (polietileno reticulado), processados simultaneamente em tripla extrusão com vulcanização a seco;

Blindagem da isolação: composto termofixo semicondutor, de fácil remoção a frio ou termicamente aderido à isolação;

Blindagem metálica: coroa de fios de cobre nu, seção mínima de 16mm²;

Cobertura: composto termoplástico de PVC/ST2 não propagante de chama ou PE/ST7 resistente às intempéries;

14.3.7. A CONTRATADA deverá instalar 02 (dois) conjuntos de proteção de descargas atmosféricas, conforme a norma ABNT NBR 5419 no espaço físico para a instalação de uma solução de fiscalização móvel;

14.3.8. Caberá a CONTRATADA realizar todas as manutenções preventivas/corretivas, limpezas ou ajustes necessários para o funcionamento de forma continuada de todos os itens descritos acima de forma periódica (mensalmente);

14.3.9. O abastecimento de óleo diesel para os geradores é de responsabilidade do DETRAN;

14.3.10. O DETRAN pagará um valor único e específico a título de remuneração para a CONTRATADA com o termo (Taxa de instalação) descrita no **ANEXO V, PLANILHA 9 DE PREÇOS DE REFERÊNCIA** todas as atividades necessárias para o cumprimento



**GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ**

das atividades descritas nos itens 14.3, 14.3.1, 14.3.2, 14.3.3, 14.3.4, 14.3.5, 14.3.6, 14.3.7

14.7. Da logística e infraestrutura da base da solução de telecomunicação móvel de fiscalização dos tipos D, E e F:

14.7.1. Caberá a CONTRATADA que todas as soluções de telecomunicações móveis de fiscalização dos tipos D, E e F possam ser encaminhadas para realizarem suas revisões periódicas preventivas e corretivas quando necessário, cabendo a CONTRATADA realizar a retirada da mesma na sede do DETRAN e devolução da mesma, após a conclusão de suas manutenções.

14.7.2. A responsabilidade pelo **fornecimento, condutor (motorista), combustível (óleo diesel)** para os **veículos** utilizados na operação das soluções, bem como o **combustível** para os **geradores de energia elétrica**, é inteiramente da **CONTRATADA**

14.7.3. O DETRAN pagará um valor único e específico sob a forma de locação mensal para cada tipo de solução D, E e F, conforme descrito na **PLANILHA 8 do ANEXO V**.

15. DAS ESPECIFICAÇÕES TÉCNICAS DOS EQUIPAMENTOS DEDICADOS PARA SEREM UTILIZADOS NAS SOLUÇÕES DE TELECOMUNICAÇÕES MÓVEIS DE FISCALIZAÇÃO E REGRA PARA COMPOSIÇÃO DE VALORES

15.4. Este capítulo tem como objetivo especificar todos itens que são necessários para que cada solução de telecomunicação móvel de fiscalização descrita nos itens 14.2., 14.2.1, 14.2.3, 14.2.4 e 14.2.5 possam operar em conformidade com seus propósitos e objetivos, esclarecendo que um ou mais itens descritos abaixo são de uso comum ou não entre os tipos de soluções, existindo somente um único tipo de equipamento para realizar uma determinada tarefa ou função afim de se tornar muito mais fácil e eficiente o



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

uso dos mesmos pelos agentes assim como permitir a manutenção mais rápida também dos mesmos, quando necessários.

15.2.1. Todo e qualquer item descrito neste capítulo possui um preço específico para efeito de composição do custo mensal de qualquer um dos tipos das soluções A, B, C, D, E e F assim como para efeito de reembolso para os casos onde o dano ou perda do mesma seja motivado por abuso, negligência, mau uso e ou furto, motivados por servidores do DETRAN ou seus prepostos, exceto quando causados por funcionários ou prepostos da CONTRATADA.

Os valores para estes itens estão descritos na **PLANILHA DE PREÇOS 10 do ANEXO V.**

15.2.2. Os valores mensais descritos na planilha de preços 8, ANEXO V, possuem os valores globais para cada um dos tipos de soluções A, B, C, D, E e F, onde, o valor global por solução compõem não só o valor da solução física em si, mas sim, cada item ou equipamento que não faça parte da sua estrutura física metálica, seus revestimentos internos, sua rede elétrica e sua rede lógica tais como mobiliários, equipamentos de informática, ar-condicionado ,tv, grupo gerador de energia, bomba submersa, geladeira, bebedouro, extintores de incêndio, caminhão e semirreboque carga seca.

O valor global contido na planilha 8 do ANEXO V deverá compreender exatamente a somatória de todos os itens e equipamentos descritos por tipo de solução A, B, C, D, E e F com suas respectivas quantidades e tipo de serviços de telecomunicação descritas no item **14.2.5. DAS CARACTERÍSTICAS PARA SOLUÇÃO MÓVEL DE FISCALIZAÇÃO DOS TIPOS A, B, C, D, E e F** com os seus valores específicos descritos na **PLANILHA DE PREÇOS 10 do ANEXO V.**



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.3. DAS ESPECIFICAÇÕES TÉCNICAS DOS EQUIPAMENTOS:

15.3.1 Geladeira / refrigerador de uma porta, tipo de degelo frost free, capacidade da geladeira de 290 litros, capacidade do freezer de 40 litros, cor branca, 110 volts.

15.3.2 Bebedouro de coluna para garrafão de 20 litros, cor branca, 110 volts, capacidade para fornecer até 3.5 litros de água gelada por hora.

15.3.3 Cadeira giratória com base injetada em resina, apoio de braços reguláveis na altura, ajuste de altura do assento, encosto e assento revestido em tecido na cor azul marinho, rodízio com rodinhas de 55 mm.

15.3.4 Mesa para escritório com tampo em MDF com 18 mm na cor cinza medindo 130cm de largura x 75cm de altura x 60 cm de profundidade, pés em aço na cor branca e 2 gavetas.

15.3.5 Mesa redonda para 4 pessoas com tampa em MDF com 18 mm, medindo 120cm, cor cinza, pés em aço na cor branca com 78 cm de altura.

15.3.6 Armário multiuso 2 portas, 1 gaveta na cor branca com 85 cm de altura, 60 cm de largura e 44 cm de profundidade.

15.3.7 Ar-condicionado split de parede de 12.000 btus, somente frio, 220 volts, cor branca.

15.3.8 Ar-condicionado split de parede de 18.000 btus, somente frio, 220 volts, cor branca.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.3.9 Impressora laser com capacidade de impressão de até 20 páginas por minuto no tamanho de papel A4, resolução de 1.200 dpi, conectividade via usb 2.0, capacidade de 140 folhas da bandeja de entrada, 110 volts.

15.3.10 Computador tipo notebook de 15 polegadas com processador Intel® Core™ i7 (de até 4.50GHz), sistema operacional Windows 11 pro em português, memória de 8GB DDR4 (1x8GB) 2666MT/s, armazenamento SSD de 512GB PCIe NVMe M.2, tela Full HD de 15.6" (1920 x 1080), 120 Hz, WVA, Teclado não retroiluminado em português (Brasil).

15.3.11 Televisão de 55 polegadas de led, tipo smart, resolução 4k (3,840 x 2,160), 1 porta usb, 2 portas hdmi, 1 controle remoto, alto falantes com 15 w rms.

15.3.12 Câmera fixa para ambiente interno (Câmeras posicionadas internas para áreas administrativas e de atendimento ao público) com as seguintes especificações técnicas mínimas:

15.3.12.1 Deve ser câmera do tipo bullet

15.3.12.2 Resolução de 3072 × 1740 no stream principal com possibilidade de alteração de resolução;

15.3.12.3 Sensor de imagem de 1/2.6" ou superior;

15.3.12.4 Codificação de vídeo H.264, H.265 ou padrões de compressão similares;

15.3.12.5 Utilizar de sensor de diodo emissor de luz com comprimento de onda dentro do espectro de luz compreendido entre 790nm e 1mm, com distância mínima de 40m;

15.3.12.6 Possuir troca automática entre horários do dia compreendidos em diurno e noturno



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.3.12.7 Possibilidade de imagem á cores com intensidade luminosa ambiente de no mínimo 5 lux, conforme ABNT para iluminação pública;

15.3.12.8 Possuir lente fixa ao corpo da câmera do tipo de foco variável com motor independente proporcionando um zoom óptico de no mínimo 5x;

15.3.12.9 Possuir motorização na lente onde a mesma pode ajustar o diafragma de acordo com o nível de luz no ambiente de forma automática.

15.3.12.10 Possuir funcionalidade onde o obturador irá expor o sensor de imagem à luz duas vezes no mínimo, para gerar dois quadros diferentes e com isso entregar esses quadros mesclados de forma a ter uma melhor visibilidade do ambiente do fundo e dos objetos mais próximos da lente;

15.3.12.11 Deve possuir no mínimo os seguintes analíticos de vídeo na borda para monitoramento e alarmes:

Cruzamento de linha.

Detecção de intrusão.

Entrada e saída de região de forma independente.

Captura de faces no vídeo em tempo real.

Contagem de pessoas em tempo real.

15.3.12.12 Todas as análises de vídeo embarcadas precisam ter filtragem de alarmes ativados por humanos para melhor resposta do sistema.

15.3.12.13 Todos os analíticos citados devem ser processados internamente no equipamento, de modo a agilizar e otimizar a entrega do pacote de dados para a central de monitoramento.

15.3.12.14 Possuir os protocolos mínimos de comunicação pela rede: QoS IPv4 UDP ICMP SMTP ARP 802.1X TCP/IP RTSP HTTP IGMP SFTP DNS DHCP RTP HTTPS WebSocket SSL/TLS UPnP SRTP FTP DDNS WebSockets IPv6 SNMP NTP PPPoE;

15.3.12.15 Possuir o protocolo padrão de comunicação entre sistemas de videomonitoramento, com no mínimo os perfis do tipo T, S & G;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 15.3.12.16 Possuir interface Fast ethernet de comunicação pela rede;
- 15.3.12.17 Alimentação energética compreendida na tensão de 12v, podendo também ser entregue equipamento alimentado através da tecnologia PoE 802.3at, Classe 4, não sendo superior a 16W por motivos de segurança e estabilidade elétrica;
- 15.3.12.18 Invólucro constituído de material não-ferroso e que esteja de acordo com as normas de proteção IEC 60529-2013 (Total em sólidos e imersão por 1min) e IEC 62262:2002 (Máximo de carga de 20J)
- 15.3.12.19 Deverá possuir slot para armazenamento local em cartão micro SD/SDHC/SDXC com capacidade de no mínimo 512GB;
- 15.3.12.20 Deverá possuir função que, em caso de desconexão de rede, inicie a gravação no armazenamento local (Cartão de memória), e sincronize tal gravação, automaticamente, com os gravadores de rede ou VMS;
- 15.3.12.21 Deverá ser fornecido todos os acessórios de fixação para perfeita instalação e acomodação do cabeamento de instalação, o acessório deverá ser do
- 15.3.12.22 Deverá ser fornecido as devidas licenças de software para o recebimento das análises de vídeos processadas localmente na borda, além dos alertas emitidos pelo equipamento.
- 15.3.12.23 Possuir os protocolos mínimos de comunicação pela rede: iSCSI DHCP DDNS SNMP RTSP DNS IPv6 NFS HTTP TCP/IP OTAP SADP NTP IPv4 UPnP ISUP HTTPS SMTP;
- 15.3.12.24 Possuir o protocolo padrão de comunicação entre sistemas de videomonitoramento, com no mínimo os perfis do tipo S & G;
- 15.3.12.25 Possuir 2 (duas) interfaces Gigabit ethernet de comunicação pela rede;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.3.12.26 Deve ser fornecida com a licença de uso para Software de Gerenciamento de Vídeo

15.4 Wi-fi interno deve possuir;

15.4.1 Próprio para ambiente interno

15.4.1.1 Access Point Sem Fio Wi-Fi 6E, gerenciado por Plataforma de Gerência em Nuvem, para uso interno, sem antenas aparentes, que opere simultaneamente nas faixas de frequência de 2.4GHz, 5GHz e 6GHz, padrões 802.11b/g/n/a/ac/ax;

15.4.1.2 Deve possuir, no mínimo, 1 porta ethernet 100M/1000M/2.5G Base-T em conector RJ45 com suporte a alimentação PoE compatível com o padrão 802.3at e com reconhecimento automático de crossover MDI/MDIX;

15.4.1.3 Suporte a velocidades de no mínimo 4800 Mbps em 6GHz, 2400 Mbps em 5GHz e 1150 Mbps em 2.4GHz;

15.4.1.4 Cada rádio deverá possuir, no mínimo, 4 antenas internas omnidirecionais, com ganho de, no mínimo, 5.4 dBi at 2.4 GHz, 6.4 dBi at 5 GHz, 7.2 dBi at 6GHz.

15.4.1.5 Suporte a operação 4x4:4 MIMO;

15.4.1.6 Suportar a utilização de canais de 20, 40, 80 e 160 MHz;

15.4.1.7 Suportar, no mínimo, 16 (dezesseis) SSIDs por rádio, com capacidade de configuração de VLAN e políticas de acesso independentes para cada SSID;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.4.1.8 Possuir LED para a indicação do status de funcionamento do equipamento;

15.4.1.9 O equipamento deverá ser novo, sem uso anterior;

15.4.1.10 Deverá ser fornecido com a mais recente versão de hardware disponível na data da aquisição;

15.4.1.11 Deverá vir acompanhado de todos os acessórios para sua operacionalização, como cabos, softwares e manuais. Os manuais poderão ser disponibilizados no site do fabricante em língua portuguesa (Brasil) ou inglesa; Deverá possuir mecanismo de segurança física no padrão Kensington lock hard point ou similar;

15.4.1.12 A estrutura física do equipamento deverá permitir fixação em teto e em parede;

15.4.1.13 Deverá conter todas as ferragens necessárias para a sua fixação em teto e em parede;

15.4.1.14 Deve suportar DFS;

15.4.1.15 Suportar temperatura em modo de operação entre 0° a 40° C;

15.4.1.16. Deverá ser gerenciado de forma centralizada pelo Software de Gerência do mesmo fabricante do Access Point Sem Fio, para a configuração dos seus parâmetros Wi-Fi, QoS, políticas de acesso, políticas de segurança, monitoração do espectro de rádio frequência e demais funcionalidades, com



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

conexão lógica via roteamento da camada de rede do modelo OSI, através de rede privada e pública;

15.4.1.17 Deve permitir ser gerenciado através de interface GUI local, através de um browser;

15.4.1.18 Deverá ser auto configurável através do Software de Gerência sem a necessidade de intervenção técnica para a sua configuração inicial (Zero Touch);

15.4.1.19 Deverá atualizar a sua versão de firmware através do Software de Gerência;

15.4.1.20 Deverá carregar e salvar as suas configurações através do Software de Gerência;

15.4.1.21 Caso a comunicação entre o Access Point (AP) e o Software de Gerência seja interrompida, o AP deve continuar operando, permitindo que os dispositivos e usuários já autenticados e associados à rede sem fio continuem acessíveis e que novos clientes possam obter acesso;

15.4.1.22 Todo o tráfego de/para os dispositivos cliente deve ser encaminhado localmente e em hipótese alguma ser direcionado para o Software de Gerência em Nuvem;

15.4.1.23 Todo o tráfego de configuração, monitoria, gerência e estatísticas entre o Access Point e o Software de Gerência deverá ocorrer com a utilização de criptografia;

15.4.1.24 Suportar a pilha de protocolos TCP/IP;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.4.1.25 Suportar os protocolos IPv4 e IPv6 simultaneamente;

15.4.1.26 Implementar VLAN Tagging IEEE 802.1q;

15.4.1.27 Implementar, localmente ou via software de gerência, o protocolo NTP ou SNTP no modo cliente para a sincronização de horário;

15.4.1.28 Possuir cliente DHCP para a configuração automática dos seus parâmetros IP;

15.4.1.29 Permitir alimentação elétrica no padrão IEEE 802.3at Plus (PoE+), utilizando a porta do switch PoE+ onde estiver conectado;

15.4.1.30 Quando alimentado pela interface de rede via PoE+, não deve sofrer nenhuma perda de funcionalidade e operar no seu desempenho máximo;

15.4.1.31 Não possuir restrição de licenças para a quantidade de dispositivos conectados simultaneamente;

15.4.1.32 Implementar os padrões de segurança WPA2 Personal/Enterprise, WPA3 Personal, WPA3 Enterprise, OWE e Advanced Encryption Standard (AES);

15.4.1.33 Permitir habilitar e desabilitar a divulgação de cada SSID de forma independente;

15.4.1.34 Implementar Wireless Isolation para evitar que um dispositivo conectado a um SSID acesse os dados de outros dispositivos conectados no mesmo SSID;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.4.1.35 Implementar filtros baseados em protocolos e em endereços MAC;

15.4.1.36 Implementar o reuso de frequências (BSS coloring);

15.4.1.37 Implementar Target Wake Time para os clientes 802.11ax compatíveis;

15.4.1.38 Deve implementar OFDMA;

15.4.1.39 Deve suportar as funcionalidades de RADIUS Accounting, SNMP, Wireless Multimedia (WMM), Spanning Tree Protocol (STP), Bridge para LAN, Bridge para VLAN, Airtime Fairness, detecção de interferência, Fast roaming (802.11r), Band Steering, Autenticação via login social, Syslog e LLDP-MED;

15.4.1.40 Deve ser capaz de detectar Rogue SSID, Evil Twin SSID, BSSID Impersonate SSID, SSID Impersonate, Advanced Impersonate SSID e Adhoc SSID;

15.4.1.41 Disponibilizar sistema de hotspot vouchers baseado em tempo e volume de dados;

15.4.1.42 Deverá possuir acesso restrito por usuário e senha, com capacidade de criação de diferentes perfis de acesso onde seja possível determinar as funcionalidades atribuídas a cada perfil, existindo, no mínimo, um perfil com permissões de criação de usuários visitantes e um perfil com permissão para efetuar qualquer alteração;

15.4.1.43 Possuir listagem de clientes Wireless, indicando SSID, endereço IP e endereço MAC;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.4.1.44 Listagem de APs e o status de cada Ponto de Acesso de forma individual, exibindo informações sobre o canal, grupo e endereço MAC;

15.4.1.45 Autenticação por Portal Web, onde conectados à rede são redirecionados para um Portal Web onde deverão se autenticar e então receber as políticas de acesso;

15.5 Wi-Fi Externo deve possuir as seguintes características;

15.5.1 próprio para uso externo com resistência contra intempéries

15.5.1.1 Access Point Sem Fio Wi-Fi 6E, gerenciado por Plataforma de Gerência em Nuvem, para uso interno, sem antenas aparentes, que opere simultaneamente nas faixas de frequência de 2.4GHz, 5GHz e 6GHz, padrões 802.11b/g/n/a/ac/ax;

15.5.1.2 Deve possuir, no mínimo, 1 porta ethernet 100M/1000M/2.5G Base-T em conector RJ45 com suporte a alimentação PoE compatível com o padrão 802.3at e com reconhecimento automático de crossover MDI/MDIX;

15.5.1.3 Suporte a velocidades de no mínimo 4800 Mbps em 6GHz, 2400 Mbps em 5GHz e 1150 Mbps em 2.4GHz;

15.5.1.4 Cada rádio deverá possuir, no mínimo, 4 antenas internas omnidirecionais, com ganho de, no mínimo, 5.4 dBi at 2.4 GHz, 6.4 dBi at 5 GHz, 7.2 dBi at 6GHz.

15.5.1.5 Suporte a operação 4x4:4 MIMO;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.5.1.6 Suportar a utilização de canais de 20, 40, 80 e 160 MHz;

15.5.1.7 Suportar, no mínimo, 16 (dezesseis) SSIDs por rádio, com capacidade de configuração de VLAN e políticas de acesso independentes para cada SSID;

15.5.1.8 Possuir LED para a indicação do status de funcionamento do equipamento;

15.5.1.9 O equipamento deverá ser novo, sem uso anterior;

15.5.1.10 Deverá ser fornecido com a mais recente versão de hardware disponível na data da aquisição;

15.5.1.11 Deverá vir acompanhado de todos os acessórios para sua operacionalização, como cabos, softwares e manuais. Os manuais poderão ser disponibilizados no site do fabricante em língua portuguesa (Brasil) ou inglesa;

15.5.1.12 Deverá possuir mecanismo de segurança física no padrão Kensington lock hard point ou similar;

15.5.1.13 A estrutura física do equipamento deverá permitir fixação em teto e em parede;

15.5.1.14 Deverá conter todas as ferragens necessárias para a sua fixação em teto e em parede;

15.5.1.15 Deve suportar DFS;

15.5.1.16 Suportar temperatura em modo de operação entre 0° to 40° C;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.5.1.17 Características Gerais:

15.5.1.18 Deverá ser gerenciado de forma centralizada pelo Software de Gerência do mesmo fabricante do Access Point Sem Fio, para a configuração dos seus parâmetros

Wi-Fi, QoS, políticas de acesso, políticas de segurança, monitoração do espectro de rádio frequência e demais funcionalidades, com conexão lógica via roteamento da camada de rede do modelo OSI, através de rede privada e pública;

15.5.1.19 Deve permitir ser gerenciado através de interface GUI local, através de um browser;

15.5.1.20 Deverá ser auto configurável através do Software de Gerência sem a necessidade de intervenção técnica para a sua configuração inicial (Zero Touch);

15.5.1.21 Deverá atualizar a sua versão de firmware através do Software de Gerência;

15.5.1.22 Deverá carregar e salvar as suas configurações através do Software de Gerência;

15.5.1.23 Caso a comunicação entre o Access Point (AP) e o Software de Gerência seja interrompida, o AP deve continuar operando, permitindo que os dispositivos e

usuários já autenticados e associados à rede sem fio continuem acessíveis e que novos clientes possam obter acesso;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.5.1.24 Todo o tráfego de/para os dispositivos cliente deve ser encaminhado localmente e em hipótese alguma ser direcionado para o Software de Gerência em Nuvem;

15.5.1.25 Todo o tráfego de configuração, monitoria, gerência e estatísticas entre o Access Point e o Software de Gerência deverá ocorrer com a utilização de criptografia;

15.5.1.26 Suportar a pilha de protocolos TCP/IP;

15.5.1.27 Suportar os protocolos IPv4 e IPv6 simultaneamente;

15.5.1.28 Implementar VLAN Tagging IEEE 802.1q;

15.5.1.29 Implementar, localmente ou via software de gerência, o protocolo NTP ou SNTP no modo cliente para a sincronização de horário;

15.5.1.30 Possuir cliente DHCP para a configuração automática dos seus parâmetros IP;

15.5.1.31 Permitir alimentação elétrica no padrão IEEE 802.3at Plus (PoE+), utilizando a porta do switch PoE+ onde estiver conectado;

15.5.1.32 Quando alimentado pela interface de rede via PoE+, não deve sofrer nenhuma perda de funcionalidade e operar no seu desempenho máximo;

15.5.1.33 Não possuir restrição de licenças para a quantidade de dispositivos conectados simultaneamente;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.5.1.34 Implementar os padrões de segurança WPA2 Personal/Enterprise, WPA3 Personal, WPA3 Enterprise, OWE e Advanced Encryption Standard (AES);

15.5.1.35 Permitir habilitar e desabilitar a divulgação de cada SSID de forma independente;

15.5.1.36 Implementar Wireless Isolation para evitar que um dispositivo conectado a um SSID acesse os dados de outros dispositivos conectados no mesmo SSID;

15.5.1.37 Implementar filtros baseados em protocolos e em endereços MAC;

15.5.1.38 Implementar o reuso de frequências (BSS coloring);

15.5.1.39 Implementar Target Wake Time para os clientes 802.11ax compatíveis;

15.5.1.40 Deve implementar OFDMA;

15.5.1.41 Deve suportar as funcionalidades de RADIUS Accounting, SNMP, Wireless Multimedia (WMM), Spanning Tree Protocol (STP), Bridge para LAN, Bridge para VLAN, Airtime Fairness, detecção de interferência, Fast roaming (802.11r), Band Steering, Autenticação via login social, Syslog e LLDP-MED;

15.5.1.42 Deve ser capaz de detectar Rogue SSID, Evil Twin SSID, BSSID Impersonate SSID, SSID Impersonate, Advanced Impersonate SSID e Adhoc SSID;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.5.1.43 Disponibilizar sistema de hotspot vouchers baseado em tempo e volume de dados;

15.5.1.44 Deverá possuir acesso restrito por usuário e senha, com capacidade de criação de diferentes perfis de acesso onde seja possível determinar as funcionalidades atribuídas a cada perfil, existindo, no mínimo, um perfil com permissões de criação de usuários visitantes e um perfil com permissão para efetuar qualquer alteração;

15.5.1.45 Possuir listagem de clientes Wireless, indicando SSID, endereço IP e endereço MAC;

15.5.1.46 Listagem de APs e o status de cada Ponto de Acesso de forma individual, exibindo informações sobre o canal, grupo e endereço MAC;

15.5.1.47 Autenticação por Portal Web, onde conectados à rede são redirecionados para um Portal Web onde deverão se autenticar e então receber as políticas de acesso;

15.6. Caminhão zero quilômetro com chassi modular com longarinas simples, com drop e de perfil "U" constante na plataforma de carga, movido a diesel, com 170 cv de potência, três eixos do tipo 6x2, sistema de freio a AR, com freio a tambor nas rodas dianteiras e traseiras com ABS + EBD + ATC + HSA + ESC (controle de estabilidade eletrônica), com comprimento total de 9 metros e 12 centímetros, com ar-condicionado, trio-elétrico, banco do motorista com suspensão pneumática e revestimento em tecido ou couro, luzes de posição e lanternas traseiras em LED, suspensão traseira com eixo motriz e auxiliar (tag-balancim) pneumático com suspensor eletropneumático para eixo auxiliar, com molas semi elípticas, assimétricas e trapezoidais, suspensão dianteira com molas parabólicas, amortecedores hidráulicos telescópicos de dupla ação e barra



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

estabilizadora, capacidade de peso bruto total (PBT) – homologado de 13.000 quilos, cor branca.

15.7. Caminhão tipo cavalo mecânico zero quilômetro, com chassi escada com longarina de perfil "U" constante e superfície plana, do tipo 4x2, movido a diesel, com 370 cv de potência, com câmbio de 12 marchas para frente e 2 para ré, com distância entre eixos de 3 metros e 50 centímetros, 2 tanques de combustíveis de 310 litros cada, com Peso Bruto Total Combinado (PBTC) – de 44.800 quilos, freio de serviço a AR, tambor nas rodas dianteiras e traseiras com EBS + ATC + HSA + ESC, com suspensão dianteira eixo rígido, molas parabólicas com amortecedores hidráulicos telescópicos de dupla ação e barra estabilizadora trio elétrico, suspensão traseira pneumática air link com 2 bolsões de ar, válvula niveladora, barra Panhard, com ar condicionado, trio elétrico, cor branca

15.8 - Semirreboque carga seca, zero quilômetro com 2 eixos, 2 posições de pino rei, suspensão pneumática, suspensor do 1º eixo, válvula de nivelamento doca, 2 pares de pé mecânico acionados por manivela sendo 1 dianteiro e 1 traseiro, com 8 pinos lock para travar container, rampas hidráulicas fechada em chapa xadrez de aço, com comprimento total de 13 metros e 50 centímetros, com largura total de 2.6 metros, cor cinza.

15.9 - Gerador de Energia Cabinado a Diesel 4t, 7 KVA, Trifásico 220V Partida Elétrica, Painel Trifásico 220 volts, Possuir alternador síncrono, trifásico 220 V, 2 polos, com 7.5 kVA de potência máxima, excitatriz rotativa por escovas, possuir regulador eletrônico automático de tensão (AVR), possuir tanque de combustível com 13 litros , deve possuir sensor de nível de óleo que impede seu funcionamento caso o nível de óleo esteja abaixo do recomendado, possuir medidor digital que demonstra os parâmetros de Tensão (V); Frequência (Hz) e Tempo de Funcionamento (H).



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.10 - Gerador de energia de 10 KVA com motor a Diesel de 19,4 HP de potência máxima, refrigerado a água através de radiador, possuir partida elétrica, possuir alternador síncrono, trifásico 220 v, 2 polos, com 10 kVA de potência máxima, excitatriz rotativa por escovas, dotado de regulador eletrônico automático de tensão (AVR), possuir dispositivos de proteção contra alta temperatura da água e baixo nível de óleo para o conjunto, possuir carenagem silenciada, construída em chapas de aço, com tratamento interno acústico, que proporcionam baixos níveis de emissões sonoras possuir portas laterais para o acesso para realização das manutenções periódicas, possuir painel ats, possuir tanque de combustível de 25 litros, possuir 1 tomada de 220volts, possuir Painel ATS Trifásico com cabo de conexão, apto para detectar a interrupção ou a falta de energia elétrica e envia sinal de acionamento ou desligamento do grupo gerador que assume ou cessa, então a alimentação da carga requerida.

15.11 - Gerador de energia de 12 KVA com motor a Diesel de 19,4 HP de potência máxima, refrigerado a água através de radiador, possuir partida elétrica, possuir alternador síncrono, trifásico 220 v, 2 pólos, com 12 kVA de potência máxima, excitatriz rotativa por escovas, dotado de regulador eletrônico automático de tensão (AVR), possuir dispositivos de proteção contra alta temperatura da água e baixo nível de óleo para o conjunto, possuir carenagem silenciada, construída em chapas de aço, com tratamento interno acústico, que proporcionam baixos níveis de emissões sonoras possuir portas laterais para o acesso para realização das manutenções periódicas, possuir painel ats, possuir tanque de combustível de 25 litros, possuir 1 tomada de 220volts, possuir Painel ATS Trifásico com cabo de conexão, apto para detectar a interrupção ou a falta de energia elétrica e envia sinal de acionamento ou desligamento do grupo gerador que assume ou cessa, então a alimentação da carga requerida.

15.12 - Nobreak com Potência nominal de pico 1500 VA / 1050 W, Tensão nominal de entrada 120 / 220 V~, Frequência 60 Hz, Disjuntor 16 A, Tensão nominal de saída* 120 V~, possuir 6 tomadas de 10 A, possuir Forma de onda no modo Bateria Senoidal.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15.13 – Cama de solteiro do tipo box com colchão em molas ensacadas, medindo 188 cm comprimento x 88 cm de largura tanto da cama como do colchão, com capacidade para até 120 kg, conforto firme, densidade da espuma D33, revestimento em poliéster, possuir proteção antiácaro, antialérgico, antifungo e antimoho, cor branco.

15.14 – Extintor de incêndio do tipo pó químico, classe ABC, de 6 quilos.

15.15 – Extintor de incêndio do tipo CO2, de 6 quilos

16. DA MANUTENÇÃO E SUPORTE TÉCNICO PARA AS SOLUÇÕES MÓVEIS DE FISCALIZAÇÃO DOS TIPOS A, B, C, D, E e F:

16.4. Toda e qualquer manutenção preventiva será sem custos para o DETRAN durante todo o período contratado.

16.5. Toda e qualquer manutenção corretiva será sem custos para o DETRAN, exceto quando a manutenção seja em decorrência de mau uso, abuso, negligência e ou furto causados por servidores do DETRAN e seus prepostos.

16.6. Caberá único e exclusivamente a CONTRATADA realizar as revisões e manutenções preventivas baseadas por tempo/hora e ou quilometragem de equipamentos e veículos, cabendo ao DETRAN informar para a CONTRATADA os valores de quilometragem dos veículos alugados para cada tipo de solução móvel de fiscalização conduzidos pelos agentes de trânsito dos tipos caminhão/chassi, caminhão/cavalo mecânico de acordo com a programação descrita nos manuais dos fabricantes dos veículos.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

16.7. A CONTRATADA deverá realizar a manutenção com limpeza dos aparelhos de ar-condicionado, grupos geradores, sistema de purificação de água, câmeras de videomonitoramento e bebedouros a cada 30 dias, independentemente do tempo de hora de uso, salvo para os geradores que devem ter suas manutenções para troca de óleo lubrificante de acordo com o manual técnico do fabricante.

16.8. A CONTRATADA deverá realizar a inspeção da carga e prazo de validade dos extintores de incêndio do tipo CO2 e PÓ classe ABC realizando a troca da unidade por outra unidade carregada e dentro da validade quando necessário.

16.9. A CONTRATADA deverá fornecer 14 (quatorze) garrações de água mineral, mensalmente, para cada solução de telecomunicação móvel de fiscalização alugada dos tipos A e B e 10 (dez) garrações para cada solução móvel de fiscalização dos tipos D, E e F, sem custos para o DETRAN, além do valor mensal da locação, devendo estes garrações serem entregues onde uma solução dos tipos A e B estejam operando e na sede do DETRAN para as soluções D, E e F pela CONTRATADA ou empresa contratada pela mesma para realizar as entregas durante os dias da semana de segunda a sexta das 10:00 até as 14:00.

16.10. A CONTRATADA deverá realizar a substituição dos veículos do tipo caminhão/chassi e caminhão/cavalo mecânico utilizados nas soluções D, E e F quando estes atingirem 200.000 quilômetros rodados ou 5 (cinco) anos a partir da entrega dos mesmos.

16.9. A CONTRATADA deverá realizar a manutenção periódica a cada 12 meses para a programação visual das soluções móveis de fiscalização com relação a sua aparência a fim de se evitar a deterioração da programação visual, devendo manter a mesma nas mesmas condições durante a fase de entrega e aceite do DETRAN.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

16.10. A CONTRATADA deverá fornecer mensalmente 1 (um) cartucho de impressão (toner) para cada impressora laser instalada em uma solução de telecomunicação móvel de fiscalização com capacidade de impressão de até 1.000 páginas com até 5% de cobertura sem custos para o DETRAN.

**17. LOCALIDADES PARA INSTALAÇÃO DAS SOLUÇÕES MÓVEIS
DE FISCALIZAÇÃO MODELOS A, B e C**

17.4. As localidades são previstas em condições que já operamos ou vamos operar por questões estratégicas, contudo poderá ter um incremento de localidades devido a dinâmica operacional e as particularidades do Sistema de Segurança Pública. Nesse diapasão e ainda por ser registro de preço será dimensionado o que já consumido e que poderá ser consumido, uma vez que por se tratar de serviço continuado somente será requerido a instalação o que for consumido.

17.5. LOCALIDADES PREVISTAS – MODELO A, B E C

ITEM	RODOVIA	LOCAL
1	Rodovia PA 252	Abaetetuba
2	Rodovia PA 140	Santo Antônio do Tauá
3	Rodovia PA 257	Parauapebas
4	Rodovia PA 457	Santarém
5	Rodovia PA 287	Redenção
6	Rodovia PA 452	Alça Viária – Marituba
7	Rodovia PA 150	Goianésia do Pará
8	Rodovia PA 458	Bragança
9	Rodovia PA 136	Castanhal
10	Rodovia BR – 316, Km 17	Benfica
11	Rodovia PA 252	Acará
12	Rodovia PA 151	Barcarena
13	Rodovia PA 151	Igarapé Miri
14	Rodovia PA 150	Marabá
15	Rodovia PA 257	Eldorado dos Carajás



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

16	Rodovia PA 279	Xinguara
17	Rodovia PA 287	Conceição do Araguaia
18	Rodovia PA 263	Tucuruí
19	Rodovia PA 124	Santa Luzia do Pará
20	Rodovia PA 150	Morada Nova
21	Rodovia PA 150	Tailândia

17.6. LOCALIDADES PREVISTAS – MODELO D e E.

ITEM	LOCAL	ABRANGÊNCIA
1	Belém	Belém, Ananindeua, Salinópolis
2	Marabá	Marabá, Parauapebas e Santarém

18- QUANTIDADE ESTIMADA.

A quantidade **estimada** de itens/serviços foi dimensionada com base nas **localidades em operação** e na **possibilidade de uso**.

O pagamento, entretanto, será efetuado **exclusivamente** pelos quantitativos **efetivamente consumidos** e/ou requisitados.

MODELO	QUANTIDADE
A	04 unds
B	11 unds
C	15 unds
D	04 unds
E	04 unds
F	04 unds



**GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ**

19. SERVIÇOS GERENCIADOS DE CIBERSEGURANÇA E OBSERVABILIDADE DA REDE

19.1 O presente documento tem por objeto a especificação de serviços contínuos de segurança cibernética e observabilidade para a infraestrutura da rede de telecomunicações da CONTRATADA, figurando como parte integrante do Termo de Referência cujo objeto principal é a contratação de serviços de Links de comunicação dedicados, para assegurar a rede de telecomunicações da contratada, contemplando as seguintes áreas:

- **ÁREA 1** - Serviços Gerenciados de Segurança da Informação - SOC (Security Operations Center), em regime 24x7x365;
- **ÁREA 2** - Serviço de Resposta a Incidentes de Segurança - CSIRT (Computer Security Incident Response Team), em regime 24x7x365, integrado ao SOC;
- **ÁREA 3** - Serviço de Gestão dos Riscos Cibernéticos de Terceiros - TPRM (Third-Party Risk Management), por meio de plataforma especializada;
- **ÁREA 4** - Serviços de Monitoramento e Observabilidade (NOC);
- **ÁREA 5** - Gerenciamento de Vulnerabilidades (GV) da Infraestrutura Fornecida;
- **ÁREA 6** - Serviço de Consultoria e Suporte em Cibersegurança.

19.2. As seis áreas compõem solução única e integrada, sob responsabilidade de uma única CONTRATADA, em razão da necessidade de convergência da alarmística, da observabilidade e da resposta a incidentes em um mesmo ecossistema tecnológico, reduzindo o tempo de detecção (MTTD) e de resposta (MTTR), e evitando a fragmentação de responsabilidades em incidentes de segurança.

19.2.1 DEFINIÇÕES E SIGLAS



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Termo	Definição
CONTRATANTE	Organização responsável pelo presente TR e beneficiária dos serviços.
CONTRATADA / PROPONENTE	Empresa prestadora dos serviços objeto deste TR / empresa participante do certame.
SOC	Security Operations Center - Centro de Operações de Segurança.
CSIRT	Computer Security Incident Response Team - Time de Resposta a Incidentes de Segurança.
TPRM	Third-Party Risk Management - Gestão dos Riscos Cibernéticos de Terceiros.
NOC	Núcleo de Operações de Rede / Monitoramento e Observabilidade.
SIEM	Security Information and Event Management - plataforma de coleta, normalização, correlação e análise de eventos de segurança.
SOAR	Security Orchestration, Automation and Response - plataforma de orquestração,



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Termo	Definição
	automação e resposta.
Threat Intelligence	Inteligência de ameaças: coleta, análise e disseminação de informações sobre ameaças cibernéticas.
Honeypot	Servidor projetado para simular vulnerabilidades, atrair atacantes e registrar suas técnicas, táticas e ferramentas.
IOC	Indicator of Compromise - Indicador de Comprometimento (ex.: IP, hash, domínio, URL maliciosos).
EASM	External Attack Surface Management - gestão da superfície externa de ataque.
Plataforma de Bloqueio Automatizado	Plataforma de distribuição de listas dinâmicas de bloqueio (threat feeds de resposta), integrada aos firewalls da CONTRATANTE, para bloqueio automático de origens maliciosas.
Playbook	Fluxo de resposta automatizado ou semiautomatizado executado pela plataforma SOAR.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Termo	Definição
ITSM	IT Service Management - plataforma/porta de gestão de chamados, incidentes, mudanças e problemas.
GMUD	Gestão de Mudanças - processo e documentação de mudanças em ambiente produtivo.
MTTD/MTTR	Mean Time to Detect / Mean Time to Respond - tempo médio de detecção / de resposta.
Ponta A	Localidade concentradora (sede/datacenter) da rede da CONTRATANTE.
Ponta B	Localidades remotas (unidades regionais, postos e soluções móveis) da rede da CONTRATANTE.
P1, P2, P3, P4	Níveis de prioridade de incidentes e solicitações: Crítico, Alto, Médio e Baixo, respectivamente.
Código aberto (open source)	Software cujo código-fonte é disponibilizado sob licença aprovada pela OSI (Open Source Initiative), passível de



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Termo	Definição
	auditoria e customização.
LGPD	Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018.

19.3. REQUISITOS GERAIS E TRANSVERSAIS (OBRIGATÓRIOS PARA TODAS AS ÁREAS)

19.3.1. Tecnologia de código aberto (open source)

19.3.1.1. As plataformas tecnológicas centrais empregadas na prestação dos serviços - SIEM, SOAR, plataforma de dashboards, honeypots e componentes de coleta (agentes, coletores e encaminhadores de logs) - deverão ser baseadas em software de código aberto (open source), totalmente customizáveis, sem qualquer limitação de licenciamento proprietário por volume de eventos (EPS), por gigabyte ingerido, por quantidade de ativos ou por número de usuários.

19.3.1.2. A exigência de código aberto fundamenta-se na independência tecnológica (ausência de vendor lock-in), na auditabilidade do código executado sobre os dados da CONTRATANTE, na perenidade da solução ao término do contrato e na economicidade, eliminando custos de licenciamento que não agregam capacidade operacional.

19.3.1.3. A CONTRATADA deverá comprovar, na Prova de Conceito, a licença de código aberto de cada componente central ofertado (ex.: GPL, AGPL, Apache 2.0, MIT, BSD ou equivalente aprovada pela OSI), bem como a sua capacidade técnica de customizar tais componentes (criação de regras, parsers, pipelines, conectores e visualizações próprias).

19.3.1.4. A plataforma de Gestão dos Riscos de Terceiros (ÁREA 3) e a Plataforma de Bloqueio Automatizado deverão ser de desenvolvimento próprio da CONTRATADA ou baseadas em código aberto, vedada a oferta por meio de mera revenda de licenças de software proprietário de terceiros, de modo a garantir capacidade de evolução funcional sob demanda da CONTRATANTE, sem custos adicionais de licenciamento, e o pleno atendimento ao item 19.3.2.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

19.3.2. Soberania e residência de dados em território nacional

19.3.2.1. Toda a infraestrutura de processamento e armazenamento das plataformas empregadas nos serviços (SIEM, SOAR, dashboards, honeypots, plataforma TPRM, plataforma de bloqueio automatizado e portal ITSM) deverá estar hospedada em datacenters localizados em território brasileiro, em nuvem nacional ou infraestrutura própria da CONTRATADA no Brasil.

19.3.2.2. É vedado o armazenamento, espelhamento, processamento ou trânsito de logs, eventos, alertas, evidências e demais dados da CONTRATANTE para fora do território nacional, em conformidade com a LGPD e com os requisitos de soberania de dados aplicáveis a infraestruturas críticas de telecomunicações.

19.3.2.3. A comprovação dar-se-á mediante declaração formal do provedor de datacenter/nuvem e demonstração técnica na Prova de Conceito (resolução de endereços, geolocalização de IP, latência e documentação contratual).

19.3.2.4. Os sensores honeypot deverão estar igualmente hospedados em território brasileiro, conforme item 19.4.3.4.

19.3.3. Idioma

19.3.3.1. Todas as interfaces das plataformas voltadas à CONTRATANTE, dashboards, relatórios, documentação técnica e o atendimento (telefônico, escrito e presencial) deverão ser prestados em português do Brasil, salvo acordo prévio e formal da CONTRATANTE.

19.3.4. Operação própria, em regime 24x7x365

19.3.4.1. Os serviços de SOC e CSIRT deverão ser prestados por meio de Centro de Operações de Segurança próprio da CONTRATADA, localizado no Brasil, em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano.

19.3.5. Portal ITSM

19.3.5.1. A CONTRATADA deverá prover portal ITSM baseado na web, disponível 24x7 por meio do qual a CONTRATANTE poderá abrir, acompanhar, escalar e encerrar solicitações de serviço, incidentes, mudanças e problemas, com trilha completa de auditoria, anexos de evidências e relatórios de níveis de serviço.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

19.3.6. Comunicação segura

19.3.6.1. Por razões de segurança, as notificações automáticas (e-mail e mensageria) deverão conter apenas as informações mínimas necessárias (número de referência do ticket e breve descrição não sensível). Os detalhes completos do incidente deverão estar disponíveis exclusivamente por meio do Portal ITSM e dos canais seguros estabelecidos.

19.3.6.2. Anexos (diagramas, imagens, PDFs, artefatos) deverão trafegar exclusivamente pelo Portal, nunca por e-mail.

19.3.7. Relatórios mensais

19.3.7.1. A CONTRATADA fornecerá relatórios mensais sobre a prestação dos serviços, em arquivo eletrônico (PDF) e disponíveis no Portal, com informações analíticas e sintéticas, incluindo: requisições e incidentes abertos e fechados no período; data/hora de abertura, início de atendimento e fechamento; responsável pela abertura e pelo atendimento; descrição do problema e da solução; indicadores de SLA; estatísticas de detecção, bloqueios automatizados realizados e ameaças identificadas.

19.3.8. Garantia dos serviços

19.3.8.1. Todo resultado entregue terá garantia de correções e ajustes pelo prazo de 90 (noventa) dias seguintes à sua conclusão, sem ônus para a CONTRATANTE, mesmo que a conclusão tenha ocorrido nos últimos 90 (noventa) dias de vigência contratual.

19.3.9. Confidencialidade, LGPD e reversibilidade

19.3.9.1. A CONTRATADA firmará termo de confidencialidade (NDA) abrangendo todos os profissionais alocados, e atuará como operadora de dados pessoais nos termos da LGPD, mediante instruções da CONTRATANTE (controladora).

19.3.9.2. Ao término do contrato, a CONTRATADA deverá exportar e entregar à CONTRATANTE a integralidade dos logs, eventos, dashboards, regras, playbooks e bases de conhecimento, em formatos abertos (ex.: JSON, CSV, Sigma/YARA quando aplicável), e realizar o expurgo seguro e comprovado dos dados remanescentes.

19.3.9.3. Extinta a vigência do contrato, a CONTRATADA terá 5 (cinco) dias úteis para



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

atendimento das solicitações de reversibilidade.

19.3.10. Transição e implantação

19.3.10.1. A CONTRATADA deverá apresentar plano de transição contemplando: reunião de kickoff em até 5 (cinco) dias úteis da assinatura; inventário e onboarding dos itens de configuração; integração das fontes de log; ativação das integrações com firewall; implantação dos honeypots; configuração dos dashboards e da plataforma TPRM; e entrada em plena operação em até 45 (quarenta e cinco) dias corridos.

19.3.10.2. A CONTRATADA levantará, em tempo de transição, a lista de dispositivos a serem monitorados, a topologia da rede e a configuração SNMP dos equipamentos, quando aplicável.

19.4. ÁREA 1 - SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO (SOC)

19.4.1. Escopo operacional

19.4.1.1. A CONTRATADA deverá prestar Serviços Gerenciados de Segurança da Informação englobando a administração, a manutenção proativa e a operação permanente das ferramentas de segurança, em regime 24x7x365, incluindo:

- a) Serviços de administração, operação e atendimento a requisições, para sustentar e operar todas as soluções de segurança do ambiente, bem como outras ferramentas disponibilizadas pela CONTRATADA;
- b) Gestão e resposta a incidentes em primeiro nível (N1), com triagem, classificação e encaminhamento conforme processo de gestão de incidentes;
- c) Monitoramento e visibilidade contínua e ininterrupta de ataques cibernéticos direcionados à CONTRATANTE, por meio de correlacionamento de logs, análise de pacotes de rede e/ou identificação de comportamento anômalo de aplicações, serviços e infraestrutura;
- d) Atividade de inteligência de ameaças proativa (Threat Hunting), para descoberta, mitigação e tratamento antecipado de ameaças potencialmente danosas;
- e) Realização permanente de ações proativas de análise de lacunas (gap analysis) voltadas a manter o parque computacional estável, seguro, disponível e íntegro.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

19.4.2. Arquitetura da solução

19.4.2.1. As ferramentas deverão ser sustentadas em nuvem nacional (modalidade SaaS) ou infraestrutura da CONTRATADA no Brasil, de maneira a causar impacto mínimo no ambiente monitorado, admitindo-se a instalação de agentes de coleta, integrações por API ou repasse de syslog, observado integralmente o item 19.3.2 (residência de dados no Brasil).

19.4.2.2. A solução deverá suportar coleta de registros de eventos em tempo real por agentes instalados em dispositivos e sistemas, importação de logs por APIs e recebimento via syslog (UDP/TCP/TLS), com armazenamento e normalização centralizados para análise e correlação eficientes.

19.4.2.3. A solução deverá implementar controle de acesso baseado em papéis (RBAC), segregação por cliente/ambiente (multitenancy) e criptografia dos dados em trânsito e em repouso.

19.4.2.4. A retenção mínima dos eventos deverá ser de 90 (noventa) dias em acesso imediato (online) e 12 (doze) meses em arquivamento recuperável.

19.4.3. Tecnologias obrigatórias do ecossistema SOC

19.4.3.1. SIEM (Security Information and Event Management): plataforma centralizada, de código aberto e totalmente customizável, responsável pela coleta, análise, normalização, armazenamento e correlação eficiente de registros de eventos em tempo real, incluindo:

- a) Criação ilimitada de regras de correlação, parsers, pipelines de processamento e extratores de campos customizados;
- b) Mapeamento das detecções na matriz MITRE ATT&CK;
- c) Integração com plataformas de Threat Intelligence por meio dos protocolos STIX/TAXII;
- d) Busca estruturada de eventos com linguagem de consulta, agregações e alertas em tempo quase-real;
- e) API documentada para integração e automação.

19.4.3.2. SOAR (Security Orchestration, Automation and Response): plataforma intimamente relacionada ao SIEM, projetada para agir sobre eventos levantados pelo SIEM de forma automatizada, coordenando as atividades de resposta a incidentes, com recursos avançados de automação e fluxo de trabalho (workflows/playbooks).



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

19.4.3.3. Inteligência de Ameaças (Threat Intelligence): processo e plataforma para coleta, agregação, normalização e análise contextualizada de dados de múltiplas fontes (feeds públicos e privados, compartilhamento entre organizações, análise de malware, fóruns e comunidades especializadas), fornecendo alertas e Indicadores de Comprometimento (IOCs) acionáveis, com correlação automática contra os eventos do SIEM.

19.4.3.4. Honeypots: implementação de servidores projetados para simular serviços e vulnerabilidades conhecidas, atraindo potenciais atacantes para registro e estudo de suas técnicas, táticas e ferramentas, com os seguintes requisitos mínimos:

- a) No mínimo 3 (três) sensores honeypot ativos, hospedados em território brasileiro, simulando serviços de rede usuais (ex.: SSH, RDP, HTTP/HTTPS, FTP, Telnet, SMB e bancos de dados);
- b) Capacidade de identificar e armazenar, sempre que disponível: endereço IP e porta de origem potencialmente maliciosa; domínio reverso associado; geolocalização do IP; payload da requisição; login e senha utilizados em tentativas de autenticação; e exemplares dos malwares obtidos;
- c) Encaminhamento automático e contínuo de todos os registros e IOCs coletados para o SIEM (item 19.4.4.4).
- d) Devem ser implantados em uma rede DMZ.

19.4.3.5. Plataforma de dashboards: o ecossistema deverá incluir plataforma completa de dashboards, integrada ao SIEM, que permita a visualização das informações de forma clara e rápida, customizável e com possibilidade de adequação à identidade visual da CONTRATANTE, conforme requisitos do item 19.4.4.6.

19.4.4. Requisitos obrigatórios de integração e automação

Os requisitos a seguir constituem o núcleo de automação exigido para a operação do SOC e serão integralmente verificados na Prova de Conceito (ANEXO VII), de forma prática e com critério eliminatório.

19.4.4.1. Integração SIEM / SOAR

- a. A plataforma SOAR deverá possuir integração nativa e bidirecional com o SIEM, permitindo que alertas gerados pelo SIEM disparem automaticamente a criação de casos e a execução de playbooks, sem intervenção humana;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- b. Os playbooks deverão contemplar, no mínimo: enriquecimento automático de indicadores (reputação de IP, geolocalização, WHOIS, consulta a bases de Threat Intelligence); abertura e atualização automática de tickets no Portal ITSM; acionamento das notificações multicanal (item 19.4.4.2); e acionamento da Plataforma de Bloqueio Automatizado (item 19.4.4.3);
- c. Deverá ser disponibilizada biblioteca inicial de playbooks cobrindo, no mínimo, os cenários: força bruta (SSH/RDP/aplicações), varredura de portas, detecção de malware, comunicação com IOC conhecido e exfiltração de dados;
- d. A criação, alteração e evolução de playbooks durante a vigência contratual não poderá implicar custo adicional à CONTRATANTE.

19.4.4.2. Integração SIEM / SOAR - Notificações multicanal

- a. O ecossistema SIEM/SOAR deverá dispor de motor de notificações capaz de notificar a CONTRATANTE sobre qualquer evento ou alerta, de acordo com matriz de comunicação configurável por severidade, por tipo de evento e por destinatário;
- b. Deverão ser suportados, no mínimo, os seguintes canais de notificação: ligação telefônica automatizada (chamada de voz), WhatsApp, Telegram, Microsoft Teams, Slack, Discord e e-mail;
- c. Deverá ser possível acionar múltiplos canais simultaneamente para um mesmo evento, bem como definir canais distintos por severidade (ex.: P1 = ligação telefônica + WhatsApp; P3 = e-mail);
- d. As notificações deverão ser emitidas em até 5 (cinco) minutos após a geração do alerta na plataforma;
- e. Para incidentes P1, o fluxo deverá suportar confirmação de recebimento (acknowledge) e escalonamento automático para o próximo contato da lista de escalonamento em caso de ausência de confirmação no prazo configurado.

19.4.4.3. Integração SIEM / SOAR - Plataforma de Bloqueio Automatizado

- a. A CONTRATADA deverá disponibilizar plataforma de bloqueio automatizado baseada em listas dinâmicas de ameaças (threat feeds de resposta), de desenvolvimento próprio ou de código aberto (item 19.3.1.4), que se integre aos firewalls da



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

CONTRATANTE;

- b. A partir do momento em que um IP atacante seja constatado como malicioso - por correlação no SIEM, por captura em honeypot ou por inteligência de ameaças o endereço deverá ser automaticamente incluído na lista de bloqueio e o bloqueio efetivado no firewall da CONTRATANTE, sem intervenção humana;
- c. O tempo máximo entre a constatação de maliciosidade e a efetivação do bloqueio no firewall deverá ser de 5 (cinco) minutos;
- d. A integração deverá suportar, no mínimo, firewalls pfSense e Fortinet (FortiGate), além de qualquer fabricante que consuma listas dinâmicas externas via HTTP(S) (ex.: External Dynamic Lists/Threat Feeds) ou API;
- e. A plataforma deverá implementar: lista de exceções (whitelist) com precedência garantida sobre os bloqueios; políticas de expiração e remoção controlada de bloqueios; painel de bloqueios ativos; e trilha de auditoria completa de cada inclusão e remoção (origem da detecção, evidência, data/hora e regra aplicada);
- f. O histórico de bloqueios deverá ser pesquisável e exportável, e os indicadores de bloqueio deverão ser apresentados nos dashboards e nos relatórios mensais.

19.4.4.4. Integração SIEM / Honeypot / Bloqueio

- a. Todo IOC coletado pelos honeypots deverá ser automaticamente ingerido e processado pelo SIEM;
- b. Constatada a maliciosidade, o IOC deverá ser automaticamente propagado à Plataforma de Bloqueio Automatizado e bloqueado nos firewalls da CONTRATANTE, configurando cadeia completa e auditável: honeypot → SIEM → plataforma de bloqueio → firewall;
- c. A cadeia completa deverá ser demonstrada na Prova de Conceito com medição de tempo de ponta a ponta.

19.4.4.5. Inteligência Artificial nos dashboards do SIEM

- a. Os dashboards do SIEM deverão incorporar recursos de Inteligência Artificial que facilitem a análise rápida tanto pela equipe técnica da CONTRATADA quanto pela CONTRATANTE, contemplando no mínimo: sumarização automática de eventos e incidentes em linguagem natural (português do Brasil); apoio à investigação e triagem (explicação de alertas, contexto e recomendações de próximo passo); e destaque



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

automático de anomalias e tendências;

- b. Os recursos de IA deverão estar disponíveis no mesmo ecossistema de dashboards, sem custo adicional de licenciamento.

19.4.4.6. Integração SIEM / Dashboards

- a. O SIEM deverá estar integrado a plataforma completa de dashboards, permitindo a visualização das informações de forma clara e rápida, em tempo quase-real;
- b. Deverão ser disponibilizados, no mínimo, painéis de: visão executiva (postura de segurança e KPIs); eventos e alertas por severidade, origem e destino; ataques por geolocalização; top ofensores e top ativos atacados; tendências históricas; indicadores de SLA; e bloqueios automatizados realizados;
- c. Os dashboards deverão ser customizáveis, com criação de novos painéis sob demanda da CONTRATANTE sem custo adicional, e com perfis de acesso distintos (executivo e técnico);
- d. A plataforma deverá permitir adequação à identidade visual da CONTRATANTE (logotipo e cores institucionais).

19.4.4.7. Integração Honeypot / Dashboards

- a. Os honeypots deverão estar integrados à mesma plataforma de dashboards, com painéis dedicados contendo, no mínimo: volume de interações por sensor; origens (IP, geolocalização); serviços/portas atacados; credenciais mais tentadas; payloads capturados; e malwares coletados;
- b. Os IOCs oriundos dos honeypots deverão ser visualizáveis em conjunto com os eventos do SIEM, compondo visão unificada de ameaças.

19.4.5. Casos de uso mínimos de detecção

19.4.5.1. A solução deverá entrar em operação com, no mínimo, os seguintes casos de uso de detecção ativos e mapeados em MITRE ATT&CK: força bruta e password spraying (SSH, RDP, VPN, aplicações web e diretório); varreduras de rede e enumeração; execução de malware; criação e elevação anômala de privilégios; acessos fora de horário e de geolocalizações atípicas; comunicação com IOCs conhecidos; ataques a aplicações web (OWASP Top 10); e anomalias em serviços críticos da rede indicados pela CONTRATANTE.

19.4.5.2. Novos casos de uso deverão ser desenvolvidos continuamente, sem custo adicional,



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

a partir das ameaças observadas e das necessidades da CONTRATANTE.

19.4.6. Métrica de valoração e cobrança do SOC

19.4.6.1. A cobrança dos Serviços Gerenciados de Segurança da Informação (SOC) será realizada na modalidade de pagamento por link ativado (relação 1:1), calculada mensalmente com base na criticidade e localização das pontas da rede, conforme categorias:

Categoria	Descrição da localidade	Tipo de ponta	Métrica de cobrança
TIPO 1	Localidade-sede / datacenter principal da CONTRATANTE	Ponta A	1 Unidade de SOC por equipamento / mês
TIPO 2	Unidades regionais de maior porte (Classe A)	Ponta B	1 Unidade de SOC por link / mês
TIPO 3	Demais unidades, postos avançados, postos de fiscalização e soluções móveis itinerantes	Ponta B	1 Unidade de SOC por link / mês

19.4.6.2. Nota de medição: o faturamento mensal do SOC corresponderá ao número exato de links ativos e efetivamente monitorados no período (1 unidade de SOC para 1 link ativado); no caso da localidade-sede (Ponta A), 1 (uma) unidade de SOC corresponderá ao equipamento/dispositivo monitorado.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

19.5. ÁREA 2 - SERVIÇO DE RESPOSTA A INCIDENTES DE SEGURANÇA (CSIRT)

19.5.1. Requisitos de negócio

- a. O serviço deverá ser totalmente gerenciado, em regime 24x7x365, incluindo integridade, disponibilidade e gerenciamento completo de mudanças, com acordos de nível de serviço (SLA) estendidos, incluindo configuração e ajuste de dispositivos;
- b. O Serviço de Resposta a Incidentes (CSIRT) deverá ser prestado por CSIRT próprio da CONTRATADA e integrar-se ao SOC entregue pela CONTRATADA (ÁREA 1), no regime 24x7x365, reagindo a incidentes de cibersegurança em tempo hábil, de modo a evitar danos aos serviços prestados, aos dados e às aplicações;
- c. A CONTRATANTE, quando julgar necessário, poderá solicitar atuação local da CONTRATADA em suas dependências ou nas dependências de seus clientes, correndo todos os custos de deslocamento por conta da CONTRATADA, sem qualquer ônus para a CONTRATANTE;
- d. O serviço deverá seguir as melhores práticas da indústria (ISO/IEC 27001, ISO/IEC 27035, NIST SP 800-61 e ITIL) para os processos de gerenciamento de mudanças, eventos, incidentes e problemas;
- e. A CONTRATADA deverá estar apta, com conhecimento e ferramentas, para contenção e recuperação das principais ameaças do mercado;
- f. A CONTRATANTE poderá solicitar a revisão de resultados entregues em desacordo com o escopo, normas ou legislação, ficando a CONTRATADA obrigada a refazer o serviço sem ônus;
- g. Durante todo o período de execução, a CONTRATADA é obrigada a manter, em base histórica, os dados sobre a execução de serviços em garantia.

19.5.2. Matriz de serviços

19.5.2.1. A CONTRATADA deverá fornecer o conjunto central de módulos e elementos de serviço a seguir:



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Grupo	Módulos e elementos de serviço
Elementos principais	Operação 24x7; Centro de Operações de Segurança próprio; Portal Web (ITSM); suporte ao idioma português do Brasil; gerenciamento de dispositivos; comunicações; gestão de escalonamento.
Saúde e disponibilidade	Monitoramento de saúde e disponibilidade; melhoria e recomendação; implementação de mudanças de saúde e disponibilidade.
Gerenciamento de incidentes	Geração, diagnóstico, resolução e relatórios de incidentes.
Gestão de capacidade	Monitoramento e relatórios de capacidade; recomendação de melhoria; planejamento de capacidade; implementação de mudança de capacidade.
Ativos e configuração	Rastreamento e relatórios de ativos; controle de itens de configuração e atualizações; relatório de status do item de configuração.
Solicitações e mudanças	Cumprimento e gerenciamento de solicitações de serviço; gestão de



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Grupo	Módulos e elementos de serviço
	mudanças (normal, padrão e emergência).
Gerenciamento de problemas	Identificação e registro de problemas; relatórios de problemas; identificação e implementação de soluções.

19.5.3. Elementos principais do serviço

19.5.3.1. Gestão de acessos: a CONTRATANTE fornecerá à CONTRATADA acesso privilegiado aos itens de configuração dentro do escopo. A CONTRATADA deverá criar conta de administrador de contingência (Break Glass) para a CONTRATANTE, armazenando as credenciais com segurança; a cada uso da conta, a senha deverá ser redefinida.

19.5.3.2. Monitoração: os itens de configuração deverão ser monitorados por múltiplos protocolos, incluindo SNMP v2/v3, SSH v2, HTTPS e ICMP. O acesso de engenharia à linha de comando deverá ser protegido via SSH v2, por meio de ferramenta de gestão de acessos críticos com jump-server confiável, sendo a VPN opção de contingência.

19.5.3.3. Escalonamento: a CONTRATADA deverá fornecer processo de escalonamento com definição de responsabilidades. A CONTRATANTE fornecerá lista de escalonamento para incidentes graves, a ser percorrida automaticamente até o atendimento. Casos escalonados somente poderão ser rebaixados com aprovação da CONTRATANTE.

19.5.3.4. Backups de itens de configuração: a CONTRATADA deverá manter backup das configurações no escopo (sistema operacional e configuração; regras; assinaturas; arquivos de configuração), realizar backup prévio e posterior a toda mudança, e gerar eventos periódicos de testes de restauração com relatório à gestão da CONTRATANTE.

19.5.4. Gestão de incidentes

19.5.4.1. Os incidentes poderão ser gerados pelo monitoramento do SOC (ÁREA 1), pela abertura de caso no Portal ITSM ou por chamada telefônica ao CSIRT. Em chamadas



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

telefônicas, o CSIRT criará o caso em nome da CONTRATANTE com o impacto e a urgência pertinentes.

19.5.4.2. As prioridades deverão ser calculadas com base na matriz de Impacto x Urgência, conforme tabela:

IMPACTO \ URGÊNCIA	1. Trabalho bloqueado	2. Trabalho degradado	3. Trabalho não afetado
Toda a organização	Crítico (P1)	Crítico (P1)	Alto (P2)
Vários departamentos	Crítico (P1)	Alto (P2)	Médio (P3)
Departamento único	Alto (P2)	Médio (P3)	Baixo (P4)
Individual	Médio (P3)	Baixo (P4)	Baixo (P4)

19.5.4.3. O CSIRT realizará a triagem do incidente para avaliar a prioridade; os incidentes serão atribuídos ao engenheiro apropriado para investigação, análise e plano de correção; a CONTRATANTE será notificada das atualizações e do plano de restauração por meio do Portal e dos canais de notificação multicanal (item 19.4.4.2).

19.5.4.4. A CONTRATADA trabalhará para resolver os incidentes e movê-los a estado resolvido no Portal, permitindo à CONTRATANTE confirmar a resolução.

19.5.5. Gestão de mudanças (GMUD)

19.5.5.1. Serão adotados 3 (três) tipos de solicitação de mudança: Normal (exige aprovação mútua prévia e documentada de ambas as partes); Padrão (pré-aprovada, criada via Portal); e de Emergência (implementação imediata para resolução de incidente ou aplicação de patch de segurança).

19.5.5.2. A implementação de qualquer mudança exigirá: backup da configuração atual; cópia



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

acessível de software/firmware aplicável; plano de reversão (rollback) documentado; número de ticket para auditoria; implementação e teste; backup da nova configuração; e atualização do ticket com o resultado. Toda mudança deverá estar integralmente documentada no Portal.

19.5.5.3. A CONTRATADA realizará análise de impacto de mudança (pré e/ou pós-implementação), assegurando que pré-requisitos são atendidos, backups existem, a alteração é consistente com as melhores práticas de segurança e pode ser implementada no prazo solicitado.

19.5.5.4. A CONTRATANTE poderá cancelar uma solicitação até 2 (duas) horas antes de mudança programada comprometida com configuração de dispositivo.

19.5.6. Gerenciamento de problemas

19.5.6.1. A CONTRATADA seguirá as melhores práticas ITIL para identificação e registro de problemas, derivados, entre outros, de incidentes repetidos de mesma natureza ou similaridade e de problemas compostos por múltiplos incidentes. Identificado e registrado um problema, plano sugerido ou opções de resolução deverão ser registrados no ticket, com implementação acordada entre as partes.

19.5.7. Escopo da operação do serviço

19.5.7.1. A CONTRATADA deverá prover, dentro dos serviços de CSIRT, no mínimo, as seguintes atividades:

Nº	Atividade	Nº	Atividade
1	Aceitação de bilhete de incidente de segurança	15	Medidas ad hoc e contenção
2	Análise de incidentes de segurança da	16	Restauração de sistemas



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Nº	Atividade	Nº	Atividade
	informação		
3	Triagem de incidentes (priorização/categorização)	17	Suporte de outras entidades de segurança
4	Coleta de informações	18	Coordenação de incidentes de segurança
5	Coordenação de análise detalhada	19	Comunicação interna
6	Análise da causa raiz de incidentes	20	Distribuição de notificação interna
7	Correlação incidente cruzado	21	Distribuição interna de info relevante
8	Análise de artefatos e evidências forenses	22	Coordenação de atividades
9	Análise de mídia ou superfície	23	Relatórios internos



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Nº	Atividade	Nº	Atividade
10	Engenharia reversa	24	Apoio à gestão de crises
11	Análise dinâmica / em tempo de execução	25	Distribuição de informações aos constituintes
12	Análise comparativa	26	Relatório de status de segurança da informação
13	Mitigação e recuperação	27	Comunicação de decisões estratégicas
14	Plano de resposta estabelecido		

19.5.8. Integração com o ecossistema do SOC

19.5.8.1 Os incidentes originados de alertas do SIEM deverão ser transferidos ao CSIRT com o contexto completo (eventos, enriquecimentos, ações automáticas executadas), compondo linha do tempo única entre SOC e CSIRT;

19.5.8.2 Os IOCs identificados durante a resposta a incidentes deverão realimentar automaticamente a plataforma de Threat Intelligence e a Plataforma de Bloqueio Automatizado (item 19.4.4.3), imunizando o ambiente contra reincidência;

19.5.8.3 A CONTRATADA deverá realizar comunicação e coordenação com outros CSIRTS e



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

órgãos competentes, tais como CERT.br, CTIR Gov e NIC.br, quando aplicável.

19.5.9. Métrica de valoração e cobrança do CSIRT

19.5.9.1. O serviço de CSIRT terá modelo misto de precificação sob demanda, composto por Franquia Recorrente (banco de horas): contratação de carga de horas /dia durante o período contratual de 24 (vinte e quatro) meses, funcionando como banco de horas global da CONTRATANTE.

19.5.9.2. Os acionamentos técnicos (mitigação, forense, resposta a incidentes) serão mensurados em horas técnicas e deduzidos do banco global. Consumida a totalidade da franquia, o excedente será pago por Hora Adicional Sob Demanda, mediante autorização prévia da CONTRATANTE.

19.6. ÁREA 3 - GESTÃO DOS RISCOS CIBERNÉTICOS DE TERCEIROS (TPRM)

19.6.1. Disposições gerais

19.6.1.1 O serviço será prestado por meio de plataforma especializada de TPRM disponibilizada pela CONTRATADA, em modalidade SaaS, hospedada integralmente em território brasileiro (item 19.3.2), de desenvolvimento próprio da CONTRATADA ou baseada em código aberto (item 19.3.1.4);

19.6.1.2 A plataforma não deverá requerer a instalação de qualquer software ou hardware no ambiente computacional da CONTRATANTE ou de seus terceiros;

Interface e documentação em português do Brasil;

19.6.1.3 Evoluções funcionais solicitadas pela CONTRATANTE deverão ser avaliadas e, quando acordadas, implementadas sem custo adicional de licenciamento.

19.6.2. Requisitos funcionais da plataforma

19.6.2.1 Disponibilizar interface simples e amigável para onboarding de serviços de nuvem e de superfície externa de ataque;

19.6.2.2 Disponibilizar interface para criação de questionários de autoavaliação personalizáveis, programáveis para envio regular a qualquer grupo de terceiros;

19.6.2.3 Suportar questionários com diferentes tipos de resposta: parágrafo, escolha única, múltipla escolha e upload de arquivos;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

19.6.2.4 Permitir inclusão de anexos como evidências nas respostas e centralizar todas as evidências de avaliação em repositório único acessível;

19.6.2.5 Permitir filtrar e visualizar questionários por status (pendente, concluído, aguardando revisão etc.) e por tempo de resposta, auxiliando na priorização e no monitoramento em tempo real;

19.6.2.6 Suportar envio programado de questionários em intervalos recorrentes (mensal, trimestral e anual) e envio sob demanda para grupos específicos;

19.6.2.7 Permitir gestão de questionários ativos e inativos, com alternância conforme necessidade;

19.6.2.8 Disponibilizar status das avaliações com base na data de vencimento, identificando avaliações pontuais e intempestivas;

19.6.2.9 Permitir criação de perguntas obrigatórias ou opcionais, com controle de envio de respostas obrigatórias antes da conclusão;

19.6.2.10 Permitir comunicação entre a organização emissora e o destinatário, com comentários nas avaliações e em perguntas individuais;

19.6.2.11 Disponibilizar painel de controle interativo para visualização das avaliações, incluindo o número de questionários em cada status;

19.6.2.12 Disponibilizar histograma de duração das avaliações, oferecendo insights sobre a eficiência do processo;

19.6.2.13 Garantir segurança do gerenciamento de usuários por convites por e-mail com tempo de expiração e autenticação segura;

19.6.2.14 Disponibilizar interface de administração com, no mínimo, 2 (dois) perfis de acesso: administrador e operador;

19.6.2.15 Disponibilizar mecanismos de compartilhamento de alertas e riscos entre organizações, com controles de acesso e mascaramento de dados apropriados;

Possibilitar a organização da gestão de riscos por ambiente, por equipes e por organização.

19.6.3. Escopo de análise

19.6.3.1. A plataforma deverá suportar, de forma nativa e não intrusiva, testes de segurança por meio de acesso de leitura restrito a metadados de API, contemplando no mínimo:

19.6.3.1.1 Provedores de nuvem: Microsoft Azure; Amazon Web Services (AWS);



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Google Cloud Platform (GCP); Huawei Cloud; e Oracle Cloud Infrastructure (OCI);

19.6.3.1.2 Ferramentas de colaboração e produtividade SaaS: Google Workspace, Microsoft 365, Slack, GitHub, BitBucket, Jira, GitLab e Zendesk;

19.6.3.1.3 Superfície externa de ataque (EASM) de organizações, especificadas a partir de lista de domínios DNS com serviços publicados na Internet.

19.6.3.2. Não deverá haver limitação quanto à quantidade de serviços ou itens de configuração testados.

19.6.3.3. Deverá permitir a análise de ambientes de parceiros e terceiros da CONTRATANTE, abrangendo, no mínimo, infraestrutura de nuvem pública, superfície externa de ataque e ferramentas SaaS de produtividade.

19.6.3.4. Deverá permitir o agendamento de testes com cronogramas distintos por ambiente (incluindo opções diária e semanal) e a execução de testes sob demanda para rápida confirmação da solução de problemas.

19.6.4. Segurança e privacidade

19.6.4.1 Executar todos os testes com permissão de acesso somente leitura às APIs dos provedores testados, limitada a parâmetros de configuração e metadados;

19.6.4.2 Não acessar ou ler dados de negócio ou de aplicações não públicas dos ambientes monitorados; não possuir permissão de alteração nos ambientes monitorados;

19.6.4.3 Suportar duplo fator de autenticação (senha e TOTP) e autenticação OAuth com identidades do Google;

19.6.4.4 Criptografar os dados coletados em trânsito e armazenados;

19.6.4.5 Implementar mascaramento de dados sensíveis da empresa terceira na visualização por outra organização, ocultando: usuários e seus dados pessoais; recursos de nuvem; endereços IP; e demais detalhes não públicos do ambiente do terceiro.

19.6.5. Gestão de riscos de terceiros

19.6.5.1 Realizar o gerenciamento de riscos e vulnerabilidades de ambientes de terceiros sem permissão de visualização de dados sensíveis ou pessoais;

19.6.5.2 Implementar métrica de pontualidade que calcule o tempo médio de resposta de terceiros para a resolução de vulnerabilidades, com base em dados estatísticos e histórico de



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

respostas;

19.6.5.3 Disponibilizar a métrica de pontualidade para cada alerta e vulnerabilidade, indicando se as respostas ocorreram em período adequado;

Possibilitar a criação automática de alertas e vulnerabilidades a partir de testes automatizados;

19.6.5.4 Disponibilizar relatório de desempenho de pontualidade por organização terceira, com tempo médio de resolução, frequência de respostas pontuais e dados históricos;

19.6.5.5 Não permitir o encerramento manual de alertas ou vulnerabilidades previamente identificadas: o fechamento somente ocorrerá após verificação automatizada da efetiva correção (ciclo completo de gerenciamento de vulnerabilidades).

19.6.6. Classificação, frameworks e conformidade

19.6.6.1 Filtrar riscos e vulnerabilidades por severidade (crítica, alta, média, baixa, informativa), por estado (fechado, em tratamento, falso positivo, controle mitigatório e risco aceito), por data de criação e por ambiente;

19.6.6.2 Classificar alertas, no mínimo, por disciplinas: compliance, resposta a incidente, auditoria, backup, confidencialidade, integridade, disponibilidade, monitoramento e hardening;

19.6.6.3 Identificar potenciais violações de conformidade com frameworks reconhecidos: NIST, CIS Controls, MITRE ATT&CK, PCI DSS e CCM;

19.6.6.4 Identificar potenciais violações de leis e regulamentações aplicáveis: LGPD e GDPR.

19.6.7. Acurácia e periodicidade

19.6.7.1 Realizar verificações diárias, por padrão, para falhas de configuração e exposição indevida de dados;

19.6.7.2 Permitir configuração da periodicidade das verificações em serviços de nuvem com intervalos de, no mínimo, 6h, 12h, 24h ou 7 dias;

19.6.7.3 Permitir configuração da periodicidade das verificações de superfície externa com intervalos de, no mínimo, 24h ou 7 dias;

19.6.7.4 Verificar a existência de problemas de segurança em todos os ativos associados aos serviços monitorados, não por amostragem, e sem necessidade de cadastro prévio dos ativos.

19.6.8. Verificações e testes mínimos

19.6.8.1. A plataforma deverá realizar testes automatizados contínuos verificando, no mínimo:



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

- 19.6.8.1.1 Exposição de objetos de armazenamento de dados (buckets S3, Blob Storage, RDS, Elasticsearch, Kibana, contêineres);
- 9.6.8.1.2 Concessões de privilégio excessivas e autenticação/autorização insegura ou sem MFA;
- 9.6.8.1.3 Publicação indevida ou acidental de serviços (FTP, Telnet, SMB, NetBIOS, RDP, RPC, CIFS expostos);
- 9.6.8.1.4 Uso de tecnologias ou serviços desatualizados ou inseguros;
- 9.6.8.1.5 Ausência de criptografia ou adoção de criptografia insegura (imagens, armazenamentos, volumes e protocolos de tráfego);
- 9.6.8.1.6 Parâmetros de backup e continuidade;
- 9.6.8.1.7 Ausência de trilha de auditoria e/ou monitoramento;
- 9.6.8.1.8 Aspectos adicionais de configuração do Control Plane, como gerenciamento de controle de acesso (IAM);
- 9.6.8.1.9 Quantidades e tipos de dados expostos em áreas de armazenamento;
- 9.6.8.1.10 Lista de portas e serviços expostos;
- 9.6.8.1.11 Enriquecimento e contexto adicional em alertas e vulnerabilidades, para facilitar a análise de criticidade e triagem.

19.6.9. Governança

- 19.6.9.1 Fornecer mecanismos para descrição dos riscos associados aos alertas identificados;
- 19.6.9.2 Fornecer mecanismos de descrição de recomendações e melhores práticas para solução dos alertas;
- 19.6.9.3 Possibilitar a segregação de acesso por organizações, parceiros, ambientes e equipes.

19.6.10. Integração com a plataforma de dashboards

- 19.6.10.1 A plataforma de TPRM deverá estar integrada à mesma plataforma de dashboards do ecossistema SOC (item 19.4.4.6), compondo visão unificada de riscos: SOC + honeypots + terceiros;
- 19.6.10.2 Deverão ser disponibilizados painéis de TPRM contendo, no mínimo: postura de risco por terceiro; evolução histórica; riscos por severidade, disciplina e framework; pontualidade de resolução; e ranking de terceiros;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

19.6.10.3 Os painéis deverão ser acessíveis aos perfis executivo e técnico da CONTRATANTE, em português do Brasil.

19.6.11. Demais itens obrigatórios

19.6.11.1 Disponibilizar API REST e ferramenta de linha de comando (CLI) documentadas para automação de atividades, sem custo adicional;

19.6.11.2 Disponibilizar SDK em linguagem amplamente utilizada para interação automatizada com a API REST, sem custo adicional;

19.6.11.3 Disponibilizar interface web pública de monitoração de uptime e performance das interfaces da plataforma (status page);

19.6.11.4 Notificar por e-mail ou webhooks problemas relevantes encontrados, atualização de status de vulnerabilidades e outros eventos relevantes;

19.6.11.5 Disponibilizar visualização de dados históricos sobre a porcentagem de riscos e vulnerabilidades tratados por cada terceiro, isolada ou agregada, ao longo do tempo;

19.6.11.6 Gerar trilha de auditoria das ações dos usuários com retenção mínima de 1 (um) ano e exportação em lote com datas de início e fim definidas;

19.6.11.7 Exportar vulnerabilidades e riscos em formato CSV e JSON, inclusive em lotes;

19.6.11.8 Manter histórico de alteração das vulnerabilidades e riscos, permitindo acompanhar mudanças de estado, recorrências e demais alterações;

19.6.11.9 Permitir compartilhamento de riscos e vulnerabilidades individuais por permalinks utilizáveis por organizações primeiras ou terceiras, sem violar o requisito de mascaramento de dados.

19.6.12. Métrica de valoração e cobrança do TPRM

19.6.12.1. A cobrança será realizada por Unidade de Riscos de Terceiros, sendo que 1 (uma) unidade contempla o monitoramento de até 10 (dez) registros de CNPJ de organizações terceiras, faturada mensalmente conforme quantidade contratada e efetivamente provisionada.

19.7. ÁREA 4 - SERVIÇOS DE MONITORAMENTO E OBSERVABILIDADE (NOC)

19.7.1. Dos requisitos de qualificação técnica da equipe



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

19.7.1.1. Para a execução dos serviços de monitoramento, observabilidade, gestão de eventos, disponibilidade, desempenho e capacidade dos ambientes de Tecnologia da Informação, a CONTRATADA deverá disponibilizar profissionais devidamente qualificados, com experiência comprovada compatível com as atividades desempenhadas, observando os seguintes perfis:

19.7.2. Head de Monitoramento e Observabilidade

19.7.2.1. Profissional responsável pela gestão estratégica da operação, governança dos serviços, definição de indicadores de desempenho, acompanhamento de níveis de serviço (SLA), gestão de equipes e relacionamento executivo com a CONTRATANTE.

19.7.2.2. Requisitos mínimos:

19.7.2.2.1 Experiência comprovada em gestão de operações de monitoramento e observabilidade de ambientes corporativos;

19.7.2.2.2 Conhecimento em governança de TI, gestão de serviços e continuidade operacional;

19.7.2.2.3 Capacidade de conduzir processos de melhoria contínua e evolução tecnológica;

19.7.2.2.4 Experiência na definição e acompanhamento de indicadores operacionais, disponibilidade e capacidade dos ambientes monitorados;

19.7.2.2.5 Vivência na gestão de equipes multidisciplinares e atendimento a ambientes críticos.

19.7.3. Coordenador de Monitoramento e Observabilidade

19.7.3.1. Profissional responsável pela coordenação técnica e operacional da equipe, acompanhamento dos eventos gerados pelos sistemas monitorados, gestão de escalonamentos, garantia da qualidade dos serviços prestados e cumprimento dos procedimentos operacionais.

19.7.3.2. Requisitos mínimos:

19.7.3.2.1 Experiência comprovada na coordenação de operações de monitoramento e observabilidade;

19.7.3.2.2 Conhecimento em gestão de incidentes, eventos, problemas e mudanças;

19.7.3.2.3 Capacidade de análise crítica de indicadores operacionais e definição de planos de ação;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

19.7.3.2.4 Experiência na elaboração de relatórios gerenciais e operacionais;

19.7.3.2.5 Atuação na condução de equipes técnicas e no acompanhamento de acordos de nível de serviço.

19.7.4. Analista de Monitoramento e Observabilidade

19.7.4.1. Profissional responsável pela operação diária dos serviços de monitoramento, acompanhamento de eventos, identificação de anomalias, análise inicial de incidentes e acionamento dos responsáveis conforme fluxos de escalonamento definidos.

19.7.4.2. Requisitos mínimos:

19.7.4.2.1 Experiência em monitoramento de infraestrutura, serviços, aplicações e recursos tecnológicos;

19.7.4.2.2 Conhecimento em análise de disponibilidade, desempenho, capacidade e continuidade operacional;

19.7.4.2.3 Capacidade de identificar, registrar, classificar e escalonar incidentes e eventos;

19.7.4.2.4 Experiência na elaboração de registros operacionais e documentação técnica;

19.7.4.2.5 Conhecimento em redes, sistemas operacionais, serviços corporativos e boas práticas de operação de TI.

19.7.5. Analista Sênior de Monitoramento e Observabilidade

19.7.5.1. Profissional responsável pela análise avançada dos ambientes monitorados, tratamento de incidentes críticos, apoio técnico especializado à operação e proposição de melhorias contínuas dos processos de monitoramento.

19.7.5.2. Requisitos mínimos:

19.7.5.2.1 Experiência comprovada em ambientes críticos de TI;

19.7.5.2.2 Conhecimento avançado em análise de desempenho, disponibilidade, capacidade e correlação de eventos;

19.7.5.2.3 Capacidade de atuação em incidentes de alta complexidade;

19.7.5.2.4 Experiência na criação e revisão de indicadores, procedimentos operacionais e fluxos de escalonamento;

19.7.5.2.5 Atuação como referência técnica para a equipe operacional.

19.7.6. Comprovação da Qualificação Técnica



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

19.7.6.1. A CONTRATADA deverá apresentar, quando solicitado pela CONTRATANTE, documentação comprobatória da experiência profissional da equipe alocada, incluindo currículos, certificados de capacitação, declarações de experiência profissional ou outros documentos equivalentes que demonstrem a aptidão dos profissionais para execução dos serviços contratados.

19.7.7. Métrica de Valoração e Cobrança do NOC do Circuito.

A cobrança dos serviços de monitoração de infraestrutura de conectividade (NOC) será indexada ao Volume de Sensores Ativos por Localidade da Rede Fornecida. Cada localidade de link ativado para o DETRAN-PA enquadrar-se-á mensalmente em uma das seguintes faixas comerciais:

- Faixa 1: De 0 a 50 sensores ativos por localidade contratada.
- Faixa 2: De 51 a 100 sensores ativos por localidade contratada.
- Faixa 3: De 101 a 150 sensores ativos por localidade contratada.
- Faixa 4: De 01 a 25 sensores ativos por equipamento monitorado.
- Bloco Adicional: Bloco fixo de +50 sensores ativos por localidade (utilizado de forma modular quando uma ponta ultrapassar o limite de 50 sensores).

Para fins de precificação de NOC para o DETRAN SEDE (Data Center e Site de Contingência) considerar 25 sensores por cada equipamento.

19.8. ÁREA 5 - GERENCIAMENTO DE VULNERABILIDADES DA INFRAESTRUTURA FORNECIDA (GV)

19.8.1. Este Serviço compreende a execução continuada de rotinas de análise de segurança cibernética e higienização tecnológica aplicadas exclusivamente sobre os ativos físicos e lógicos que compõem a infraestrutura da rede de telecomunicações alocada pela CONTRATADA, devendo implementar rotinas de varredura proativa e busca por ameaças



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

(Threat Hunting) internas ao canal de telecomunicações contratado.

19.8.1.1 Análise de Vulnerabilidade Híbrida: Suporte e rastreamento técnico de segurança em ativos on-premises e em nuvem pertencentes à infraestrutura técnica da rede fornecida, fazendo uso de coletores e ferramentas de Scan locais.

19.8.2. Métrica de Valoração e Cobrança do GV:

19.8.2.1 A cobrança deste Serviço possui natureza linear e contínua, estruturada sob a métrica de mensalidade fixa por equipamento/dispositivo monitorado (Relação 1:1). O volume faturado acompanhará rigorosamente a distribuição e os quantitativos de circuitos ativos definidos para o serviço de SOC.

19.9. ÁREA 6 - SERVIÇO DE CONSULTORIA E SUPORTE EM CIBERSEGURANÇA

19.9.1. Serviço de Consultoria e Suporte em Cibersegurança para apoio a diversos serviços e implementações, correções e aplicações de patches nos equipamentos instalados nas pontas A e B, apoio nas instalações, etc.

19.9.2. Métrica de Valoração e Cobrança: Este serviço deve ser cobrado por hora técnica contratada.

19.10. QUALIFICAÇÃO TÉCNICA

19.10.1. Qualificação da empresa

19.10.1.1 Atestado(s) de Capacidade Técnica, emitido(s) por pessoa jurídica de direito público ou privado, comprovando a prestação de serviços de SOC 24x7 com SIEM de código aberto por período mínimo de 6 (seis) meses ininterruptos;

19.10.1.2 Atestado(s) comprovando a prestação de serviços de resposta a incidentes de segurança (CSIRT);

19.10.1.3 Atestado(s) comprovando a prestação de serviço de gestão de riscos cibernéticos de terceiros (TPRM) contemplando, no mínimo, 50 (cinquenta) organizações monitoradas;

19.10.1.4 Declaração formal de que opera Centro de Operações de Segurança próprio em território brasileiro, com indicação do endereço, passível de visita técnica pela CONTRATANTE;

19.10.1.5 Comprovação de que as plataformas ofertadas atendem aos itens 19.3.1. (código



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

aberto / desenvolvimento próprio) e 19.3.2. (hospedagem no Brasil);

19.10.1.6 A licitante deverá apresentar, no mínimo, 01 (um) Atestado de Capacidade Técnica emitido por pessoa jurídica de direito público ou privado, comprovando a execução satisfatória de serviços de monitoramento e observabilidade de ambientes de Tecnologia da Informação, contemplando ambiente com quantitativo igual ou superior a 500 (quinhentos) ativos monitorados, compatível em características, complexidade e volume com o objeto da presente contratação.

19.10.2. Qualificação e certificações da equipe técnica

19.10.2.1. Para a execução dos serviços, a CONTRATADA deverá comprovar que a equipe alocada possui as seguintes certificações técnicas vigentes, conforme o escopo de atuação de cada profissional:

Perfil profissional	Certificações exigidas (mínimo)
Engenheiro e ou Coordenador de SOC	Pelo menos uma: CISSP, GSEC, SABSA, CEH, CISM, CRISC, CGEIT ou ISO/IEC 27001 (Auditor/Implementador).
Analista de Segurança de Perímetro (Firewall e VPNs)	ISFS (Information Security Foundation); desejável certificação do fabricante do firewall utilizado pela CONTRATANTE (ex.: Fortinet NSE).
Analista I - CSIRT	Linux LPIC-1 ou ISFS.
Analista II - CSIRT	Linux LPIC-1, ISFS ou CEH.
Analista III - CSIRT	CompTIA Security+ ou CEH.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Perfil profissional	Certificações exigidas (mínimo)
Analista Forense Digital	Pelo menos uma: ACE, ACFEI, CCFT, CEH, CHFI, EnCE ou certificação de nível GIAC.
Analista de Governança de TI e Riscos (TPRM)	Pelo menos uma: CRISC, CISM, CGEIT, ITIL Foundation v3 (ou superior), CompTIA Security+, CEH, COBIT 5, COBIT 2019 ou ISO/IEC 27001.
Analistas de Assessment (Níveis I, II e III)	ISFS, Auditor Interno/Externo ISO 27001 ou CEH.
Head de Monitoramento e Observabilidade (NOC)	Certificação ITIL Foundation V3 ou superior; Zabbix Certified Specialist (ZCS); Zabbix Certified Professional (ZCP); Zabbix Certified Expert (ZCE).
Coordenador de Monitoramento (NOC)	Certificação Zabbix Certified Specialist (ZCS); Zabbix Certified Professional (ZCP).
Analista Sênior de Monitoramento (NOC)	Certificação ITIL Foundation V3 ou superior; Zabbix Certified Specialist (ZCS); Zabbix Certified Professional (ZCP); Zabbix Certified Expert (ZCE).
Analista de Monitoramento e	Certificação Zabbix Certified Specialist



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Perfil profissional	Certificações exigidas (mínimo)
Observabilidade (NOC)	(ZCS).

19.10.2.2. As comprovações dar-se-ão por meio de certificados válidos e vínculo formal dos profissionais com a PROPONENTE (contrato de trabalho, contrato de prestação de serviços ou declaração de contratação futura vinculada à assinatura do contrato).

19.11. NÍVEIS DE SERVIÇO (SLA)

19.11.1. Matriz de acordos de nível de serviço

19.11.1.1. Todos os serviços seguirão as metas abaixo. O descumprimento sujeitará a CONTRATADA a penalidades sobre a taxa de serviço mensal, respeitado o limite acumulado de 5% (cinco por cento) do valor total do contrato ao longo da vigência.

Categoria	Descrição do indicador	Prioridade	SLA requerido	Penalidade	Horário
Solicitação de Serviço (Atribuição)	Tempo para atribuir o ticket de solicitação após recebimento no Service Desk	P1 e P2 / P3 e P4	15 minutos / 4 horas	1% da taxa de serviço mensal	24x7
Solicitação Resolvida	Tempo máximo	P1/P2 e P3/P4	2/5/10 dias corridos	1% da taxa de serviço	24x7



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Categoria	Descrição do indicador	Prioridade	SLA requerido	Penalidade	Horário
	total para resolução definitiva da solicitação de serviço			mensal	
Incident Management Response	Tempo limite para atribuição e primeiro atendimento ao ticket de incidente de segurança	P1 e P2 / P3 e P4	30 minutos / 60 minutos	1% da taxa de serviço mensal	24x7
Incident Management Resolve	Tempo limite para resolução completa e remediação do incidente	P1/P2/P3 e P4	8/16/48 horas	N/A	24x7
Emergency Change	Atribuição de ticket de mudança de	N/A	60 minutos	N/A	24x7



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Categoria	Descrição do indicador	Prioridade	SLA requerido	Penalidade	Horário
Response	emergência				
Change Response	Atribuição de ticket de mudança padrão ou normal	N/A	60 minutos	N/A	24x7
Change Implementation Complete	Conclusão das alterações programadas dentro da janela de mudança acordada	N/A	95% de conformidade	N/A	24x7
Resolve Notification	Notificação de resolução do ticket após restauração do serviço	N/A	30 minutos	N/A	24x7



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Categoria	Descrição do indicador	Prioridade	SLA requerido	Penalidade	Horário
Notificação multicanal de alertas	Tempo entre a geração do alerta na plataforma e a emissão das notificações (item 19.4.4.2)	Todas	5 minutos	1% da taxa de serviço mensal	24x7
Bloqueio automatizado	Tempo entre a constatação de maliciosidade e a efetivação do bloqueio no firewall (item 19.4.4.3)	Todas	5 minutos	1% da taxa de serviço mensal	24x7
Elaboração de documento	Elaboração de documento	N/A	2 dias corridos	N/A	8x5



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Categoria	Descrição do indicador	Prioridade	SLA requerido	Penalidade	Horário
de GMUD	de mudanças envolvendo os ativos de segurança gerenciados				
Planejamento e implantação	Análise e planejamento de effort para adição de novas funcionalidades de ferramentas	N/A	7 dias corridos	N/A	8x5
Análise de potenciais ameaças	Execução de rotinas de Threat Hunting sob demanda de usuários ou do time de segurança	N/A	1 dia corrido	N/A	8x5

19.11.2. Severidade de chamados e metas de atendimento



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Indicador	BAIXA	MÉDIA	ALTA	URGENTE
Descrição	Problema técnico com pouco ou baixo impacto na utilização do serviço	Problema técnico que impeça a utilização parcial de uma funcionalidade	Problema técnico que impeça completamente a utilização de uma funcionalidade	Problema técnico que impeça a utilização do serviço em sua totalidade
Início do atendimento	Até 24 horas corridas	Até 12 horas corridas	Até 4 horas corridas	Até 2 horas corridas
Meta de chamados no prazo	85%	90%	92%	90%
Multa por descumprimento	0,5% do valor mensal	1% do valor mensal	1,5% do valor mensal	2% do valor mensal

19.11.2.1. Medição: Meta = quantidade de registros atendidos no prazo / total de registros do período. O limite de penalidade acumulada é de 5% do valor total do contrato ao longo da vigência.

19.11.2.2. Em caso de falhas de software (bugs) cuja correção dependa de nova versão da comunidade/mantenedor, a CONTRATADA deverá prover solução de contingência em até 90 (noventa) dias úteis da abertura do chamado; a contingência não conclui o chamado, mas suspende a contagem do prazo de resolução.

19.11.3. Disponibilidade das plataformas



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

19.11.3.1 As plataformas SIEM, SOAR, dashboards e TPRM deverão apresentar disponibilidade mensal mínima de 99,5% (noventa e nove vírgula cinco por cento), aferida por monitoramento próprio e auditável pela CONTRATANTE;

19.11.3.2 A plataforma TPRM deverá disponibilizar página pública de status e uptime (item 19.6.11);

19.11.3.3 Indisponibilidades programadas deverão ser comunicadas com antecedência mínima de 48 (quarenta e oito) horas e realizadas em janelas acordadas.

19.12. GOVERNANÇA DO CONTRATO, RELATÓRIOS E REUNIÕES

19.12.1 Reunião mensal de governança operacional, com apresentação do relatório mensal (item 19.3.7), indicadores de SLA, incidentes relevantes, bloqueios realizados, postura de riscos de terceiros e plano de melhoria contínua;

19.12.2 Relatório executivo trimestral consolidado, com visão de tendências, evolução da postura de segurança e recomendações estratégicas;

19.12.3 Designação, pela CONTRATADA, de gestor de contas técnico como ponto focal, e de coordenador de SOC responsável pela operação;

19.12.4 A CONTRATANTE fornecerá 2 (dois) contatos de segurança designados e 1 (um) contato de Service Desk para interação com os serviços.

19.13. DA PROVA DE CONCEITO (POC)

19.13.1. A PROPONENTE mais bem classificada será convocada a realizar Prova de Conceito da solução ofertada, conforme roteiro detalhado no ANEXO VII - PROVA DE CONCEITO, parte integrante deste TR.

19.13.2. A Prova de Conceito possui caráter eliminatório: será exigida a comprovação prática de 100% (cem por cento) dos requisitos do roteiro obrigatório, abrangendo as áreas (SOC, CSIRT, TPRM e NOC), incluindo as integrações e automações do item 19.4.4.

19.13.3. A PROPONENTE deverá iniciar a Prova de Conceito em até 10 (dez) dias úteis da convocação e concluí-la em até 5 (cinco) dias úteis do início, sob pena de desclassificação.

19.13.4. A reprovação na Prova de Conceito implicará desclassificação e convocação da próxima classificada, sujeita às mesmas exigências.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

ANEXO II DO TERMO DE EFERÊNCIA
CONDIÇÕES GERAIS

1. O DETRAN/PA será o gestor dos serviços contratados, sendo responsável pela sua administração e gerência.
2. Os municípios / localidades onde poderão ser instalados os circuitos encontram-se relacionados no **Anexo IV**.
3. São de responsabilidade da CONTRATADA a disponibilização de recursos de conectividade (roteadores, terminais, equipamentos correlatos) e os serviços de configurações necessários à prestação dos serviços, bem como a manutenção e atualização tecnológica de tais recursos.
4. O prazo do contrato será de **24 (meses)**, podendo ser prorrogado para perfazer no máximo 10 (DEZ) anos, conforme Lei Federal nº 14.133/2021.
5. Todos os serviços serão operacionalizados com os preços fixos contratados pelo período de 12 meses a partir da assinatura do contrato.
6. Relação de serviços complementares:
 - a) Havendo extravio e/ou dano no equipamento causado pela CONTRATANTE, será concretizada a cobrança em conta/fatura.
 - b) Mudança de endereço de circuito local e interurbano deverá ser igual ao valor de instalação do circuito contratado.
7. Qualquer serviço complementar não previsto no item anterior não poderá ser cobrado pela CONTRATADA, exceto com a anuência da CONTRATANTE.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

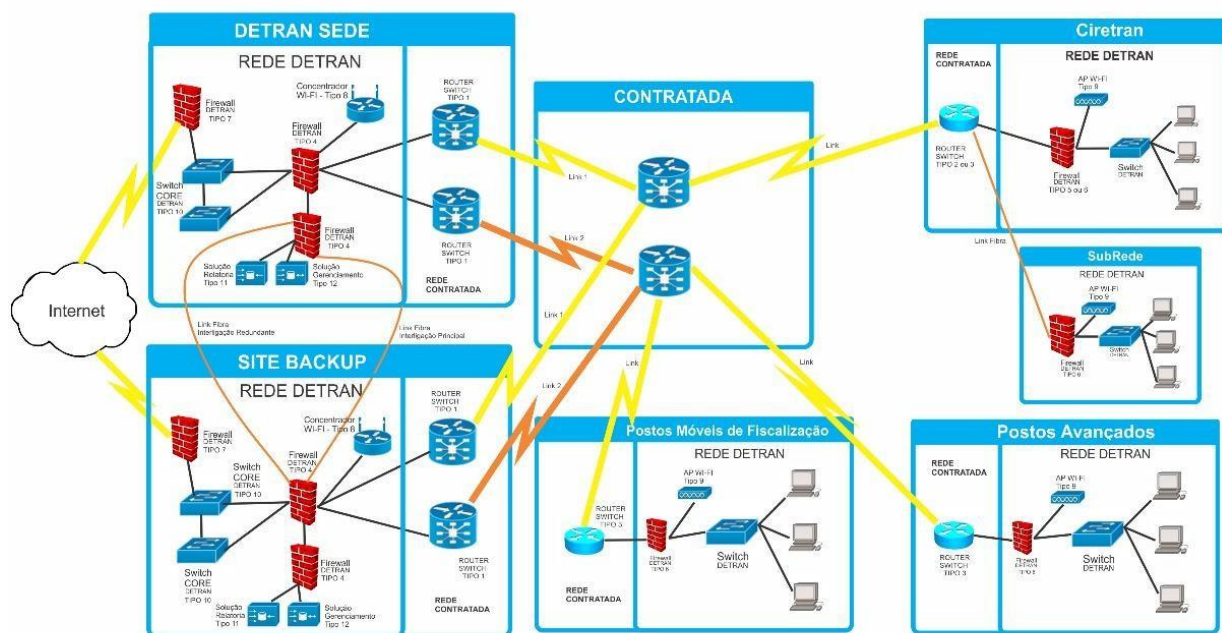
8. Os serviços devem ser prestados conforme coluna “Prazo de Ativação do Circuito (dias corridos)” da planilha 1 do ANEXO IV DO TERMO DE REFERÊNCIA, a contar do recebimento da abertura da Ordem de Serviço (OS), emitida pela Diretoria de Tecnologia e Informática, podendo ser prorrogada, excepcionada, por até igual período, desde que justificado previamente pelo contratado e autorizado pela Contratante. .
9. Será considerado **VENCEDOR** o licitante que apresentar o **menor VALOR GLOBAL para o custo total de todos os serviços contidos neste edital (incluindo todos os impostos), conforme a Tabela 11 do Anexo VI.**
10. Todas as especificações técnicas contidas neste edital e seus anexos são mínimas.
11. Todos os equipamentos fornecidos pela contratada e instalados nas dependências da sede do DETRAN e CIRETRANS deverão ser novos, de primeiro uso e devidamente homologados pela ANATEL (quando se aplicar).
12. **Não será permitido** a instalação de equipamentos WI-FI no DETRAN SEDE, CIRETRANS, POSTOS AVANÇADOS E POSTOS DE FISCALIZAÇÃO FIXO OU MÓVEL, sem a anuência da DTI Diretoria de Tecnologia e Informática.
13. Todos os serviços deverão iniciados através de Ordem de Serviço emitida e acompanhada pela DTI.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

ANEXO III - TOPOLOGIA

TOPOLOGIA DETRAN





GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

ANEXO IV DO TERMO DE REFERÊNCIA

SOLUÇÃO DE TELECOMUNICAÇÃO - CARACTERÍSTICAS DOS CIRCUITOS

PLANILHA 1

SOLUÇÃO DE TELECOMUNICAÇÃO - CARACTERÍSTICAS DOS CIRCUITOS- DETRAN/PA

Regional	Município	Velocidade do Link (MBPS)	Nível de Criticidade	Contingência/ Velocidade do link	Prazo de Ativação do Circuito (dias corridos)	Tempo de Máximo de Reparo (Horas)	Tipos de Equipamentos a serem instalados (Item 7.2)
Grupo 1							
ABAETETUBA	Abaetetuba	20	4	Sim / 5mbps	30	8	2,5,9 e 13
	Barcarena	10	4	Sim 5mbps	30	8	3,6,9 e 13
	Cametá	10	3	Não	30	12	3,6,9 e 13
	Igarapé Mirim	10	3	Não	30	12	3,6,9 e 13
	Tailândia	10	3	Não	30	8	3,6,9 e 13
Grupo 2							
ALTAMIRA	Altamira	20	4	Sim / 5mbps	30	8	2,5,9 e 13
	Uruará	10	3	Não	30	24	3,6,9 e 13
	Medicilândia	10	2	Não	90	24	3,6,9 e 13
Grupo 3							
BELEM	Belém - Internet	1gb	5	Sim / 1gb	30	2	1,4,7,8,9,10,11,12



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

	Posto shopping metrópole	50	4	Sim / 10 Mbps	30	4	3,6,9 e 13
	Posto Shopping Pátio Belém	40					3,6,9 e 13
	Posto shopping boulevard	40	4	Sim / 10 Mbps	30	2	2,5,9 e 13
	Posto shopping parque	60	4	Sim / 10 Mbps	30	2	2,5,9 e 13
	Ananindeua	60	4	Sim / 20 Mbps	30	4	2,5,9 e 13
	Posto Estação Cidadania São Brás	20	3	Sim / 10 Mbps	30	4	3,6,9 e 13
	Icoaraci	10	3	Não	30	4	3,6,9 e 13
	Marituba	10	3	Não	30	4	3,6,9 e 13
	Parque de Retenção	10	3	Sim / 5 Mbps	30	4	3,6,9 e 13
	Site Contigência 1	10gb	5	sim / 10gb	90	1	1,4,7,8,9,10,11,12
	SERPRO - BELÉM	1gb	5	sim / 1gb	90	1	2
	Soure	15	3	Não	30	48	3,6,9 e 13
Grupo 4							
BREVES	Breves	10	3	Sim / 5mbps	90	48	3,6,9 e 13
Grupo 5							
CAPANEMA	Capanema	20	4	Sim / 5mbps	30	8	2,5,9 e 13
	Bragança	10	4	Não	30	8	3,6,9 e 13
	Capitão Poço	10	3	Não	30	8	3,6,9 e 13
	Salinópolis	15	3	Sim / 5mbps	30	8	3,6,9 e 13



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Grupo 6							
CASTANHAL	Castanhal	30	4	Sim / 10 Mbps	30	6	2,5,9 e 13
	São Miguel do Guamá	10	3	Não	30	8	3,6,9 e 13
	Tomé Açu	10	3	Não	30	8	3,6,9 e 13
	Igarapé Açu	10	3	Não	30	8	3,6,9 e 13
	Vigia	10	3	Não	30	8	3,6,9 e 13
	Santa Isabel do Pará	10	3	Sim / 5mbps	30	6	3,6,9 e 13
Grupo 7							
ITAITUBA	Itaituba	30	4	Sim / 5mbps	30	24	2,5,9 e 13
	Novo Progresso	10	3	Sim / 5mbps	90	36	3,6,9 e 13
	Rurópolis	10	3	Sim / 5mps	90	36	3,6,9 e 13
Grupo 8							
MARABA	Marabá	40	4	Sim / 20mbps	30	8	2,5,9 e 13
	Jacundá	10	3	Não	30	8	3,6,9 e 13
	São Geraldo do Araguaia	10	3	Não	90	12	3,6,9 e 13
	Itupiranga	10	3	Não	30	8	3,6,9 e 13
Grupo 9							
PARAGOMINAS	Paragominas	20	4	Sim / 5mbps	30	8	2,5,9 e 13
	Mãe do Rio	10	3	Não	30	8	3,6,9 e 13
	Dom Eliseu	15	3	Sim / 5mbps	30	8	3,6,9 e 13
	Rondon do Pará	10	3	Não	30	8	3,6,9 e 13
Grupo 10							
PARAUPEBAS	Parauapebas	40	4	Sim / 5mbps	30	8	2,5,9 e 13
	Curionópolis	10	3	Não	30	8	3,6,9 e 13



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

	Eldorado dos Carajás	10	3	Não	30		3,6,9 e 13
	Canaã dos Carajás	15	3	Não	30	12	3,6,9 e 13
Grupo 11							
REDENÇÃO	Redenção	40	4	Sim / 5mbps	90	6	2,5,9 e 13
	Santana do Araguaia	10	3	Sim / 5mbps	90	12	3,6,9 e 13
	Conceição do Araguaia	10	3	Sim / 5mbps	90	12	3,6,9 e 13
	Xinguara	20	3	Sim / 5mbps	90	12	2,5,9 e 13
	Tucumã	10	3	Não	90	12	3,6,9 e 13
	Ourilândia	5	3	Não			3,6,9 e 13
	São Félix do Xingú	10	3	Não	90	16	3,6,9 e 13
Grupo 12			1				
SANTARÉM	Santarém	40	4	Sim / 20 mbps	30	6	2,5,9 e 13
	Alenquer	10	3	Não	90	24	3,6,9 e 13
	Monte Alegre	10	3	Não	60	24	3,6,9 e 13
	Óbidos	10	3	Não	60	24	3,6,9 e 13
	Oriximiná	10	3	Não	30	24	3,6,9 e 13
	Monte Dourado	10	3	Sim / 5mbps	30	18	3,6,9 e 13
Grupo 13							
TUCURUI	Tucuruí	20	4	Sim / 5mbps	30	8	2,5,9 e 13
	Novo Repartimento	10	3	Sim / 5 mps	30	18	3,6,9 e 13



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

ANEXO V DO TERMO DE REFERÊNCIA
PLANILHAS DE PREÇOS DE REFERÊNCIA

PLANILHAS DE PREÇOS PARA SOLUÇÃO DE TELECOMUNICAÇÃO DE LINK DE INTRANET (PLANILHAS 1, 2 e 3)

PLANILHA 1

SOLUÇÃO DE TELECOMUNICAÇÃO DE LINK TERRESTRE DE INTRANET

ITEM	Link dedicado terrestre de intranet para Ananindeua, Belém, Benevides, Icoaraci e Marituba	Valor mensal (A) R\$	Valor do Upgrade em (100%) da velocidade deverá ser 60% do valor mensal (A) R\$
1	10 Mbps		
2	20 Mbps		
3	30 Mbps		
4	40 Mbps		
5	50 Mbps		
6	60 Mbps		
7	80 Mbps		
8	100 Mbps		
9	200 Mbps		
10	300 Mbps		



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

PLANILHA 2

SOLUÇÃO DE TELECOMUNICAÇÃO DE LINK TERRESTRE DE INTRANET PARA O INTERIOR DO ESTADO

Item	Link dedicado terrestre de intranet	Valor mensal (A)	Valor do upgrade em (100%) da velocidade deverá ser 60% do valor mensal (A)	Valor do link de Sub rede deverá ser 30% do valor (A)
		R\$	R\$	R\$
1	5 Mbps			
2	10 Mbps			
3	15 Mbps			
4	20 Mbps			
5	30 Mbps			
6	40 Mbps			
7	50 Mbps			
8	70 Mbps			
9	80 Mbps			



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

PLANILHA 3

**SOLUÇÃO DE TELECOMUNICAÇÃO DE LINK DE INTRANET DO TIPO (SATÉLITE) PARA O INTERIOR DO ESTADO
CONTIGÊNCIA**

Item	Link via satélite	Valor mensal (A) (R\$)	Valor do Upgrade em (100%) da velocidade deverá ser 60% do valor mensal (A) (R\$)	Valor do link de Sub rede deverá ser 30% do valor (A) (R\$)
1	5 MBPS			



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Planilha de Preços de LINK DE INTERNET

PLANILHA 4

PREÇOS PARA SOLUÇÃO DE TELECOMUNICAÇÃO DE LINK DEDICADO DE INTERNET

Item	Link dedicado de internet	Valor mensal (A) (R\$)	Valor do Upgrade em (100%) da velocidade deverá ser 60% do valor mensal (A) (R\$)
1	400 Mbps		
2	600 Mbps		
3	800Mbps		
4	1GB		
5	2GB		
6	4GB		



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

PLANILHA 5		
EQUIPAMENTO		
Item	Descrição	Valor unitário mensal de locação R\$
1	Tipo 1 - Solução de Conectividade ROTEADOR / SWITCH - (Ponta "A" – DETRAN/SEDE)	
2	Tipo 2 - Solução de Conectividade ROTEADOR / SWITCH - (Ponta "B" – CIRETRAN A)	
3	Tipo 3 - Solução de Conectividade ROTEADOR / SWITCH - (Ponta "B" – CIRETRANS B e POSTOS/SUB REDE).	
4	Tipo 4 - Solução NGFW - (Ponta "A" – DETRAN/SEDE)	
5	Tipo 5 - Solução NGFW - (Ponta "B" – CIRETRAN A)	
6	Tipo 6 - Solução NGFW - (Ponta "B" – CIRETRAN B, POSTOS/SUB REDE)	
7	Tipo 7 - Solução NGFW - (Ponta "A" – DETRAN/SEDE - INTERNET)	
8	Tipo 8 - Solução WI-FI CONCENTRADOR - (Ponta "A" – DETRAN/SEDE)	
9	Tipo 9 - Solução WI-FI ACESSO - (Ponta A e Ponta B – DETRAN/SEDE e CIRETRANS/POSTOS/SUB-REDE)	
10	TIPO 10 - Switch Core/Distribuição L3 10 Ponta A - DETRAN SEDE)	
11	Tipo 11 - Solução de Relatoria (1 unidade) (Ponta A - DETRAN SEDE)	
12	Tipo 12 - Solução de Gerência Centralizada (1 unidade) Ponta A DETRAN SEDE)	
13	Tipo 13 Sistema ininterrupto de energia elétrica (Nobreak):	



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

PLANILHAS DE PREÇOS SOLUÇÃO PORTÁTIL PARA ACESSO VIA SATÉLITE
(PLANILHAS 6 E 7)

PLANILHA 6

SOLUÇÃO DE TELECOMUNICAÇÃO PORTÁTIL E VEICULAR PARA ACESSO VIA SATÉLITE E FRANQUIA MENSAL

Item	Kit portátil de Link via satélite	Valor unitário mensal (R\$)
1	Tipo 01 - kit portátil de acesso via satélite	
2	Tipo 02 - kit veicular de acesso via satélite	



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

PLANILHA 7

PLANILHA DE VALORES DE REFERÊNCIA DE CONSUMO DA SOLUÇÃO DE TELECOMUNICAÇÃO PORTÁTIL E VEÍCULAR PARA ACESSO VIA SATÉLITE

Item	Link via satélite	Unidade	Valor unitário R\$
1	Valor da disponibilidade mensal do sinal via satélite dos Kits do Tipo e 1 e Tipo 2.	1	



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

PLANILHAS DE PREÇOS DE REFERÊNCIA PARA SOLUÇÃO DE TELECOMUNICAÇÃO MÓVEL DE FISCALIZAÇÃO
DETRAN/PA

PLANILHAS 8, 9 e 10

PLANILHA 8

ITEM	DESCRIÇÃO	QDT	Valor unitário mensal de locação R\$
1	Solução de telecomunicação móvel de fiscalização contendo todos os equipamentos, mobiliários, veículos e demais componentes descritos no item 14.2.5.1. MODELO A do ANEXO I	1	R\$
2	Solução de telecomunicação móvel de fiscalização contendo todos os equipamentos, mobiliários, veículos e demais componentes descritos no item 14.2.5.2. MODELO B	1	R\$
3	Solução de telecomunicação móvel de fiscalização contendo todos os equipamentos, mobiliários e demais componentes descritos no item 14.2.5.3. MODELO C	1	R\$
4	Solução de telecomunicação móvel de fiscalização contendo todos os equipamentos, mobiliários, veículos e demais componentes descritos no item 14.2.5.4. MODELO D	1	R\$



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

5	Solução de telecomunicação móvel de fiscalização contendo todos os equipamentos, mobiliários, veículos e demais componentes descritos no item 14.2.5.5. MODELO E	1	R\$
6	Solução de telecomunicação móvel de fiscalização contendo todos os equipamentos, mobiliários, veículos e demais componentes descritos no item 14.2.5.6. MODELO F	1	R\$



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

PLANILHA 9
TAXA DE INSTALAÇÃO PARA SOLUÇÃO DE TELECOMUNICAÇÃO MÓVEL DE FISCALIZAÇÃO – DETRAN/PA

COMPOSIÇÃO DE PREÇOS DE REFERÊNCIAS PARA IMPLEMENTAÇÃO INFRAESTRUTRA PARA SOLUÇÃO DE
TELECOMUNICAÇÃO MÓVEL DE FISCALIZAÇÃO – DETRAN/PA

Item	Descrição	QT	Valor único (R\$)
1	Taxa de instalação solução de telecomunicação móvel de fiscalização do tipo A e B	1	
2	Taxa de instalação solução de telecomunicação móvel de fiscalização do tipo C	1	



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

PLANILHA 10
VALORES DOS ITENS DEDICADOS PARA COMPOSIÇÃO E FORMAÇÃO DAS SOLUÇÕES DE TELECOMUNICAÇÕES MÓVEIS DE FISCALIZAÇÃO MODELOS A, B, C, D, E e F DESCRITOS NO ITEM 15.3. DO ANEXO I

Item	Descrição	1	Valor de locação mensal R\$
	MODELO A	1	
	MODELO B	1	
	MODELO C	1	
	MODELO D	1	
	MODELO E	1	
	MODELO F	1	



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

PLANILHA 11
SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO PARA A REDE DE TELECOMUNICAÇÕES

COMPOSIÇÃO DE PREÇOS DE REFERÊNCIAS PARA IMPLEMENTAÇÃO DE SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO PARA A REDE DE TELECOMUNICAÇÕES

Item	Descrição	UNID	QUANT	VALOR ÚNICO (R\$)
1	SERVIÇOS DE SOC (Security Operations Center)			
1.1	SOC - TIPO 1 - Ponta A (Detran SEDE) - Por Equipamento	Equipamento Monitorado / Mês	1	
1.2	SOC - TIPO 2 - Ponta B (Ciretrans A)	Link / Mês	1	
1.3	SOC - TIPO 3 - Ponta B (Ciretrans B, Postos, etc.)	Link / Mês	1	
2	SERVIÇOS DE NOC (Network Operations Center)			
2.1	NOC - Faixa 1 (De 0 a 50 sensores monitorados por localidade)	Link / Mês	1	
2.2	NOC - Faixa 2 (De 51 a 100 sensores monitorados por localidade)	Link / Mês	1	



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

2.3	NOC - Faixa 3 (De 101 a 150 sensores monitorados por localidade)	Link / Mês	1	
2.4	NOC - Faixa 4: (De 01 a 25 sensores por equipamento monitorado)	Equipamento Monitorado / Mês	1	
2.5	NOC - Bloco Adicional (Expansão de +50 sensores)	UNIDADE	1	
3	SERVIÇOS DE CSIRT (Resposta a Incidentes da Rede)			
3.1	CSIRT - Franquia Recorrente (Banco de Horas)	Hora Técnica	1	
3.2	CSIRT - Hora Adicional Excedente (Sob Demanda)	Hora Técnica	1	
4	GERENCIAMENTO DE VULNERABILIDADES (GV)			
4.1	GV - TIPO 1 - Por Equipamento	Equipamento / Mês	1	
5	GESTÃO DE RISCOS DE TERCEIROS DA OPERADORA			
5.1	TPRM - Auditoria de Risco Cibernético de Operadoras	CNPJ / Mês	1	



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

6	SERVIÇOS DE CONSULTORIA E SUPORTE EM CIBERSEGURANÇA			
6.1	Franquia Recorrente (Banco de Horas)	Hora Técnica	1	
6.2	Hora Adicional Excedente (Sob Demanda)	Hora Técnica	1	



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

ANEXO VI DO TERMO DE REFERÊNCIA

MODELO DE PROPOSTA

TABELAS 1, 2, 3, 4, 5, 6, 7, 8, 9 e 10 DE VALORES MENSAIS

TABELA 1 SOLUÇÃO DE TELECOMUNICAÇÃO INTRANET – DETRAN/PA									
Município	Velocidade do Link de intranet (Mbps)	Valor do Link de intranet Mensal (Planilhas 1 e 2) (A)	Tipos de Equipamentos (Planilha 5)	Qtd. dos Equipamentos (B)	Valor Unitário do Equipamento (Planilha 5) R\$ (C)	Total mensal por tipo de Equipamento (R\$) (D) = (B) x (C)	Total da SOMA de todos os equipamentos da Localidade (Valor mensal) (R\$)	Total Mensal (R\$) (E) = (A+D)	Total 24 meses (R\$) (F) = (E * 24)
Abaetetuba	20		2	1					
			5	2					
			9	2					
			13	1					
Barcarena	10		3	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

			6	1					
			9	2					
			13	1					
Cametá	10		3	1					
			6	1					
			9	1					
			13	1					
Tailândia	10		3	1					
			6	1					
			9	1					
			13	1					
Altamira	20		2	1					
			5	2					
			9	2					
			13	1					
Uruará	10		3	1					
			6	1					
			9	1					
			13	1					
Medicilândia	10		3	1					
			6	1					
			9	1					
			13	1					
Shopping pátio Belém	40		3	1					
			6	1					
			9	2					
			13	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Shopping Boulevard	40		3	1					
			6	1					
			9	2					
			13	1					
Shopping metrópole	50		3	1					
			6	1					
			9	2					
			13	1					
Posto shopping parque	60		3	1					
			6	1					
			9	2					
			13	1					
Ananindeua	60		2	61					
			5	2					
			9	2					
			13	1					
Posto Estação Cidadania São Brás	20		3	1					
			6	1					
			9	1					
			13	1					
Icoaraci	10		3	1					
			6	1					
			9	1					
			13	1					
Marituba	10		3	1					
			6	1					
			9	2					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

			13	1					
Parque de Retenção - Belém	10		3	1					
			6	1					
			9	1					
			13	1					
Soure	10		3	1					
			6	1					
			9	1					
			13	1					
Breves	10		3	1					
			6	1					
			9	1					
			13	1					
Capanema	20		3	1					
			5	2					
			9	4					
			13	1					
Bragança	10		3	1					
			6	1					
			9	3					
			13	1					
Capitão Poço	10		3	1					
			6	1					
			9	1					
			13	1					
Salinópolis	15		3	1					
			6	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

			9	2					
			13	1					
Castanhal	30		2	1					
			5	2					
			9	4					
			13	1					
São Miguel do Guamá	10		3	1					
			6	1					
			9	1					
			13	1					
Tomé Açu	10		3	1					
			6	1					
			9	1					
			13	1					
Igarapé Açu	10		3	1					
			6	1					
			9	1					
			13	1					
Vigia	10		3	1					
			6	1					
			9	1					
			13	1					
Santa Isabel do Pará	10		3	1					
			6	1					
			9	1					
			13	1					
Itaituba	30		2	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

			5	2					
			9	3					
			13	1					
Novo Progresso	10		3	1					
			6	1					
			9	1					
			13	1					
Marabá	40		2	1					
			5	2					
			9	4					
			13	1					
Jacundá	10		3	1					
			6	1					
			9	2					
			13	1					
São Geraldo do Araguaia	10		3	1					
			6	1					
			9	1					
			13	1					
Itupiranga	10		3	1					
			6	1					
			9	1					
			13	1					
Paragominas	20		2	1					
			5	2					
			9	4					
			13	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Mãe do Rio	10		3	1					
			6	1					
			9	1					
			13	1					
Dom Eliseu	15		3	1					
			6	1					
			9	1					
			13	1					
Rondon do Pará	10		3	1					
			6	1					
			9	1					
			13	1					
Parauapebas	40		2	1					
			5	2					
			9	4					
			13	1					
Curionópolis	10		3	1					
			6	1					
			9	1					
			13	1					
Eldorado dos Carajás	10		3	1					
			6	1					
			9	1					
			13	1					
Canaã dos Carajás	15		3	1					
			6	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

			9	2					
			13	1					
Redenção	40		2	1					
			5	2					
			9	4					
			13	1					
Santana do Araguaia	10		3	1					
			6	1					
			9	1					
			13	1					
Conceição do Araguaia	10		3	1					
			6	1					
			9	1					
			13	1					
Xinguara	20		2	1					
			5	2					
			9	3					
			13	1					
Tucumã	10		3	1					
			6	1					
			9	1					
			12	1					
Ourilândia	10		3	1					
			6	1					
			9	1					
			13	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

São Félix do Xingu	10		3	1					
			6	1					
			9	1					
			13	1					
Santarém	40		22	1					
			5	2					
			9	6					
			13	1					
Alenquer	10		3	1					
			6	1					
			9	1					
			13	1					
Monte Alegre	10		3	1					
			6	1					
			9	1					
			13	1					
Óbidos	10		3	1					
			6	1					
			9	1					
			13	1					
Oriximiná	10		3	1					
			6	1					
			9	1					
			13	1					
Monte Dourado	10		3	1					
			6	1					
			9	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

TABELA 2
SOLUÇÃO DE TELECOMUNICAÇÃO – SUB REDES DETRAN/PA – SOB DEMANDA

Município	SUB REDE, conforme Anexo I, item 5, subitem 5.7.	Preço de referência Planilha 2(Anexo V)	Tipo de Equipame nto (Planilha 5)	Qtd. de Equipament os (H)	Valor Unitário do Equipament o (Planilha 5) (R\$) (I)	Total mensal por tipo de Equipament os (R\$) (J = H*I)	Total da SOMA de todos os equipament os da Localidade (R\$)	Total Mensal (R\$) (K = G+J)	Total 24 meses (R\$) (L = K * 24)
Abaetetuba	20		2	1					
			5	2					
			9	2					
			13	1					
Barcarena	10		3	1					
			6	1					
			9	2					
			13	1					
Cametá	10		3	1					
			6	1					
			9	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

			13	1					
Tailândia	10		3	1					
			6	1					
			9	1					
			13	1					
Altamira	20		2	1					
			5	2					
			9	2					
			13	1					
Uruará	10		3	1					
			6	1					
			9	1					
			13	1					
Medicilândia	10		3	1					
			6	1					
			9	1					
			13	1					
Shopping pátio Belém	40		3	1					
			6	1					
			9	2					
			13	1					
Shopping Boulevard	40		3	1					
			6	1					
			9	2					
			13	1					
Shopping metrópole	50		3	1					
			6	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

			9	2					
			13	1					
Posto shopping Grão Pará- Belém	60		3	1					
			6	1					
			9	2					
			13	1					
Ananindeua	60		2	1					
			5	1					
			9	2					
			13	1					
Saci Guamá	20		3	1					
			6	1					
			9	1					
			13	1					
Icoaraci	10		3	1					
			6	1					
			9	1					
			13	1					
Marituba	10		3	1					
			6	1					
			9	2					
			13	1					
Parque de Retenção - Belém	10		3	1					
			6	1					
			9	1					
			13	1					
Soure	10		3	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

			6	1					
			9	1					
			13	1					
Breves	10		3	1					
			6	1					
			9	1					
			13	1					
Capanema	20		2	1					
			5	2					
			9	4					
			13	1					
Bragança	10		3	1					
			6	1					
			9	3					
			13	1					
Capitão Poço	10		3	1					
			6	1					
			9	1					
			13	1					
Salinópolis	15		3	1					
			6	1					
			9	2					
			13	1					
Castanhal	30		2	1					
			5	2					
			9	4					
			13	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

São Miguel do Guamá	10		3	1					
			6	1					
			9	1					
			13	1					
Tomé Açu	10		3	1					
			6	1					
			9	1					
			13	1					
Igarapé Açu	10		3	1					
			6	1					
			9	1					
			13	1					
Vigia	10		3	1					
			6	1					
			9	1					
			13	1					
Santa Isabel do Pará	10		3	1					
			6	1					
			9	1					
			13	1					
Itaituba	30		2	1					
			5	2					
			9	3					
			13	1					
Novo Progresso	10		3	1					
			6	1					
			9	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

			13	1					
Marabá	40		2	1					
			5	2					
			9	4					
			13	1					
Jacundá	10		3	1					
			6	1					
			9	2					
			13	1					
São Geraldo do Araguaia	10		3	1					
			6	1					
			9	1					
			13	1					
Itupiranga	10		3	1					
			6	1					
			9	1					
			13	1					
Paragominas	20		2	1					
			5	2					
			9	4					
			13	1					
Mãe do Rio	10		3	1					
			6	1					
			9	1					
			13	1					
Dom Eliseu	15		3	1					
			6	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

			9	1					
			13	1					
Rondon do Pará	10		3	1					
			6	1					
			9	1					
			13	1					
Parauapebas	40		2	1					
			5	2					
			9	4					
			13	1					
Curionópolis	10		3	1					
			6	1					
			9	1					
			13	1					
Eldorado dos Carajás	10		3	1					
			6	1					
			9	1					
			13	1					
Canaã dos Carajás	15		3	1					
			6	1					
			9	2					
			13	1					
Redenção	40		2	1					
			5	2					
			9	4					
			13	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Santana do Araguaia	10		3	1					
			6	1					
			9	1					
			13	1					
Conceição do Araguaia	10		3	1					
			6	1					
			9	1					
			13	1					
Xinguara	20		2	1					
			5	2					
			9	3					
			13	1					
Tucumã	10		3	1					
			6	1					
			9	1					
			12	1					
Ourilândia	10		3	1					
			6	1					
			9	1					
			13	1					
São Félix do Xingu	10		3	1					
			6	1					
			9	1					
			13	1					
Santarém	40		22	1					
			5	2					
			9	6					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

			13	1					
Alenquer	10		3	1					
			6	1					
			9	1					
			13	1					
Monte Alegre	10		3	1					
			6	1					
			9	1					
			13	1					
Óbidos	10		3	1					
			6	1					
			9	1					
			13	1					
Oriximiná	10		3	1					
			6	1					
			9	1					
			13	1					
Monte Dourado	10		3	1					
			6	1					
			9	1					
			13	1					
Tucuruí	20		2	1					
			5	2					
			9	3					
			13	1					
Igarapé Miri	10		3	1					
			6	1					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

TABELA 3
SOLUÇÃO DE TELECOMUNICAÇÃO
UPGRADE EM 100% DE LINK DE INTRANET /INTERNET A PARTIR DO 13º MÊS – SOB DEMANDA

Município	Upgrade em 100% de Link de intranet /internet a partir do 13º mês. Velocidade do Link de intranet/internet (Mbps)	Valor de 60% da coluna (A) da Tabela 1 do Anexo VI. Valor mensal (R\$) (M)	Valor de 12 meses (R\$) (N = M *12)
Abaetetuba	20		
Barcarena	10		
Cametá	10		
Tailândia	10		
Altamira	20		
Uruará	10		
Medicilândia	10		
Belém – Internet	1GB		
Posto Shopping Pátio Belém	40		
Posto Shopping Boulevard	40		
Posto Shopping Metrôpole	50		
Posto shopping Parque- Belém	60		
Ananindeua	60		
Posto Estação cidadania São Braz	10		
Icoaraci	10		



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Marituba	10		
Parque de Retenção - Belém	10		
Soure	10		
Breves	10		
Capanema	20		
Bragança	10		
Capitão Poço	10		
Salinópolis	15		
Castanhal	30		
São Miguel do Guamá	10		
Tomé Açu	10		
Igarapé Açu	10		
Vigia	10		
Santa Isabel do Pará	10		
Itaituba	30		
Novo Progresso	10		
Marabá	40		
Jacundá	10		
São Geraldo do Araguaia	10		
Itupiranga	10		
Paragominas	20		
Mãe do Rio	10		
Dom Eliseu	15		
Rondon do Pará	10		
Parauapebas	40		
Curionópolis	10		
Eldorado dos Carajás	10		



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Canaã dos Carajás	15		
Redenção	40		
Santana do Araguaia	10		
Conceição do Araguaia	10		
Xinguara	20		
Tucumã	10		
Ourilândia	10		
São Félix do Xingú	10		
Santarém	40		
Alenquer	10		
Monte Alegre	10		
Óbidos	10		
Oriximiná	10		
Monte Dourado	10		
Tucuruí	20		
Igarapé Miri	10		
Rurópolis	10		
Novo Repartimento	10		
		VALOR TOTAL	



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

TABELA 4

SOLUÇÃO DE TELECOMUNICAÇÃO – LINK DE INTERNET, BACKBONE DO SITE CONTINGENTE e SERPRO – DETRAN/PA - SEDE

Município	Velocidade do Link de internet (Mbps)	Valor do Link de internet Mensal (O)	Tipo de Equipamento (Planilha 5)	Qtd. Equipamento (Planilha 5) (P)	Valor Unitário por equipamento (Planilha 5) (R\$) (Q)	Total mensal por tipo de equipamento (Planilha 5) (R\$) (R = P*Q)	Total da SOMA de todos os equipamentos da Localidade (R\$)	Total Mensal (R\$) (S = O+R)	Total 24 meses (R\$) (T = S * 24)
Belém – Internet - SEDE	1GB		1	2					
			4	2					
			7	2					
			8	1					
			9	30					
			10	20					
			11	1					
			12	1					
Belém Site Contigência	10GB		1	2					
			4	2					
			7	2					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

TABELA 5

SOLUÇÃO DE TELECOMUNICAÇÃO PORTÁTIL PARA ACESSO VIA SATÉLITE

COMPOSIÇÃO DE PREÇO DE SOLUÇÃO DE TELECOMUNICAÇÃO PORTÁTIL E VEICULAR PARA ACESSO VIA SATÉLITE

Item	Kit portátil e veicular de Link via satélite	QTD	Valor unitário (Planilha 6) (R\$)	Valor total mensal (R\$)	Valor total 24 meses (R\$)
1	Tipo 01 - kit Portátil de acesso via satélite	20			
2	Tipo 02 - kit Veicular de acesso via satélite	30			
VALOR TOTAL (Item 1, 2 e 3)					R\$



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

TABELA 6

TABELA DE VALORES DE CONSUMO DA SOLUÇÃO DE TELECOMUNICAÇÃO PORTÁTIL E VEICULAR DE ACESSO VIA SATÉLITE

Item	Descrição de regra de cobrança de consumo dos Kits do Tipo e 1 e Tipo 2	QTD	Valor unitário (R\$) (Planilha 7)	Valor Mensal (R\$)	Valor Total 24 meses (R\$)
1	Valor da disponibilidade de sinal dos Kits do Tipo e 1 e Tipo 2.	50			
		VALOR TOTAL R\$			



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

TABELA 7
SOLUÇÃO DE TELECOMUNICAÇÃO MÓVEL DE FISCALIZAÇÃO DETRAN/PA

COMPOSIÇÃO DE PREÇOS PARA SOLUÇÃO DE TELECOMUNICAÇÃO MÓVEL DE FISCALIZAÇÃO

Item	Descrição	QT	Valor Unitário mensal (R\$) (Planilha 8)	Valor Total mensal (R\$)	Valor Total 24 meses (R\$)
1	Locação de solução de telecomunicação móvel de fiscalização tipo A	04			
2	Locação de solução de telecomunicação móvel de fiscalização tipo B	11			
3	Locação de solução de telecomunicação móvel de fiscalização tipo C	15			
4	Locação de solução de telecomunicação móvel de fiscalização tipo D	04			
5	Locação de solução de telecomunicação móvel de fiscalização tipo E	04			
6	Locação de solução de telecomunicação móvel de fiscalização tipo F	04			



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

TABELAS DE VALORES DE SERVIÇOS DE PARCELA ÚNICA

TABELA 8 COMPOSIÇÃO DE PREÇOS DE INSTALAÇÃO E CONFIGURAÇÃO - DETRAN/PA (Parcela Única)				
COMPOSIÇÃO DE PREÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DE TODOS OS EQUIPAMENTOS NOS MUNICÍPIOS				
Regional	Municípios	Valor de Instalação do Link e Infraestrutura (CC) R\$	Valor configuração e instalação dos equipamentos de rede de comunicação (DD) R\$	Valor Total (EE=CC+DD) R\$
ABAETETUBA	Abaetetuba			
	Barcarena			
	Cametá			
	Tailândia			
	Igarapé Miri			
ALTAMIRA	Altamira			
	Uruará			
	Medicilândia			



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

BELÉM	Belém - Internet			
	Posto Shopping Pátio Belém			
	Posto Shopping Boulevard			
	Posto Shopping Metrópole			
	Posto shopping Parque			
	Ananindeua			
	Posto Estação Cidadania São Braz			
	Icoaraci			
	Marituba			
	Parque de Retenção			
	SERPRO/BELEM			
	Site de Contingência			
	Soure			
BREVES	Breves			
CAPANEMA	Capanema			
	Bragança			
	Capitão Poço			



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

	Salinópolis			
CASTANHAL	Castanhal			
	Igarapé Açu			
	São Miguel do Guamá			
	Tomé Açu			
	Vigia			
	Santa Isabel do Pará			
ITAITUBA	Itaituba			
	Novo Progresso			
	Rurópolis			
MARABÁ	Marabá			
	Jacundá			
	São Geraldo do Araguaia			
	Itupiranga			
PARAGOMINAS	Paragominas			
	Mãe do Rio			
	Dom Eliseu			
	Rondon do Pará			
PARAUPEBAS	Parauapebas			



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

	Curionópolis			
	Eldorado dos Carajás			
	Canaã dos Carajás			
REDENÇÃO	Redenção			
	Santana do Araguaia			
	Conceição do Araguaia			
	Xinguara			
	Tucumã			
	Ourilândia			
	São Félix do Xingu			
SANTARÉM	Santarém			
	Alenquer			
	Monte Alegre			
	Óbidos			
	Oriximiná			
	Monte Dourado			
TUCURUÍ	Tucuruí			
	Novo Repartimento			
VALOR TOTAL				



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

TABELA 9
COMPOSIÇÃO DE PREÇOS DE INSTALAÇÃO E CONFIGURAÇÃO - DETRAN/PA

**COMPOSIÇÃO DE PREÇOS PARA INSTALAÇÃO DA BASE DE INFRAESTRUTURA PARA SOLUÇÃO DE TELECOMUNICAÇÃO
MÓVEL DE FISCALIZAÇÃO**

Item	Descrição	QTD	Valor Unitário (R\$) Parcela única (Planilha 9)	Valor Total (R\$) Parcela única
1	Serviço de infraestrutura para solução de telecomunicação móvel de fiscalização tipo A e B	15		
2	Serviço de infraestrutura para solução de telecomunicação móvel de fiscalização tipo C	15		
			VALOR TOTAL	



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

TABELA 10

COMPOSIÇÃO DE PREÇOS PARA SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO PARA A REDE DE TELECOMUNICAÇÕES NAS CIRETRANS, POSTOS AVANÇADOS E POSTOS DE FISCALIZAÇÃO

Município	Quant. Equipamentos Monitorados (A)	Faixa de Serviço NOC (B) PLANILHA 11 DO ANEXO V	Tipo de Serviço SOC (C) PLANILHA 11 DO ANEXO V	Valor do GV (D) PLANILHA 11 do ANEXO V	Soma dos Valores dos Serviços (A*D + (B+C)) PLANILHA 11 do ANEXO V (VALOR MENSAL)	VALOR PARA 24 MESES
Abaetetuba	6	2	2			
Barcarena	6	2	2			
Cametá	4	1	3			
Tailândia	4	1	3			
Altamira	6	2	2			
Uruará	4	1	3			
Medicilândia	4	1	3			
Shopping Pátio Belém	5	1	3			
Shopping Boulevard	5	1	3			
Posto Parque Shopping	5	1	3			
Ananindeua	6	2	2			
Posto Estação Cidadania São Brás	4	1	3			



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Icoaraci	4	1	3			
Marituba	5	1	3			
Parque de Retenção Belém	4	1	3			
Soure	4	1	3			
Breves	4	1	3			
Capanema	8	2	2			
Bragança	6	2	2			
Capitão Poço	4	1	3			
Salinópolis	5	2	2			
Castanhal	8	2	2			
São Miguel do Guamá	4	1	3			
Tomé Açú	4	1	3			
Igarapé Açú	4	1	3			
Vigia	4	1	3			
Santa Isabel do Pará	4	1	3			
Itaituba	4	1	3			
Novo Progresso	4	1	3			
Marabá	8	2	2			
Jacundá	5	1	3			
São Geraldo do Araguaia	4	1	3			
Itupiranga	4	1	3			
Paragominas	8	2	2			



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Mãe do Rio	4	1	3			
Dom Eliseu	4	1	3			
Rondon do Pará	4	1	3			
Parauapebas	8	2	2			
Curionópolis	4	1	3			
Eldorado dos Carajás	4	1	3			
Canaã dos Carajás	4	1	3			
Redenção	8	2	2			
Santana do Araguaia	4	1	3			
Conceição do Araguaia	4	1	3			
Xinguara	7	2	2			
Tucumã	4	1	3			
Ourilândia	4	1	3			
São Félix do Xingú	4	1	3			
Santarém	10	2	2			
Alenquer	4	1	3			
Monte Alegre	4	1	3			
Óbidos	4	1	3			
Oriximiná	4	1	3			
Monte Dourado	4	1	3			
Tucuruí	7	2	2			
Igarapé Miri	4	1	3			



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Novo Repartimento	4	1	3			
Rurópolis	4	1	3			
Link SERPRO	2	3	1			
VALOR TOTAL						

TABELA 11

COMPOSIÇÃO DE PREÇOS PARA SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO PARA A REDE DE TELECOMUNICAÇÕES PRÉDIO SEDE



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Município	Quant. Equipamentos Monitorados (A)	Faixa de Serviço NOC (B) PLANILHA 11 DO ANEXO V	Tipo de Serviço SOC (C) PLANILHA 11 DO ANEXO V	Valor do GV (D) PLANILHA 11 do ANEXO V	Soma dos Valores dos Serviços ((A*B)+(A*C) + (A*D)) PLANILHA 11 do ANEXO V (VALOR MENSAL)	VALOR PARA 24 MESES
Data Center/SEDE-Belém	59	4	1			
Data Center Contingência	29	4	1			
VALOR TOTAL						

TABELA 12

COMPOSIÇÃO DE PREÇOS DE REFERÊNCIAS PARA IMPLEMENTAÇÃO DE SERVIÇOS DE GESTÃO EM SEGURANÇA DA INFORMAÇÃO PARA A REDE DE TELECOMUNICAÇÕES



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Item	Descrição	UNID	QUANT	Soma do valor dos serviços (PLANILHA 10 do anexo V)	VALOR TOTAL 24 MESES (R\$)
1	SERVIÇOS DE CSIRT (Resposta a Incidentes da Rede)				
1.1	CSIRT - Franquia Recorrente (Banco de Horas)	Hora Técnica	17.520		
2	SERVIÇOS DE CONSULTORIA E SUPORTE.				
2.1	Franquia Recorrente (Banco de Horas)	Hora Técnica	17.520		
3	GESTÃO DE RISCOS DE TERCEIROS DA OPERADORA				
3.1	TPRM - Auditoria de Risco Cibernético de Operadoras	CNPJ / Mês	10		
VALOR TOTAL					



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

VALOR GLOBAL PARA LANCE
SOMATÓRIO DAS TABELAS 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 e 12

TABELA	DESCRIÇÃO	VALOR TOTAL DE CADA TABELA PELO PERÍODO DE 24 MESES (R\$)
1	SOLUÇÃO DE TELECOMUNICAÇÃO INTRANET – DETRAN/PA	
2	SOLUÇÃO DE TELECOMUNICAÇÃO – SUB REDES DETRAN/PA – SOB DEMANDA	
3	SOLUÇÃO DE TELECOMUNICAÇÃO UPGRADE EM 100% DE LINK DE INTRANET /INTERNET A PARTIR DO 13º MÊS – SOB DEMANDA	
4	SOLUÇÃO DE TELECOMUNICAÇÃO – LINK DE INTERNET, BACKBONE DO SITE CONTINGENTE e SERPRO – DETRAN/PA - SEDE	
5	SOLUÇÃO DE TELECOMUNICAÇÃO PORTÁTIL PARA ACESSO VIA SATÉLITE	



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

6	TABELA DE VALORES DE CONSUMO DA SOLUÇÃO DE TELECOMUNICAÇÃO PORTÁTIL E VEICULAR DE ACESSO VIA SATÉLITE	
7	SOLUÇÃO DE TELECOMUNICAÇÃO MÓVEL DE FISCALIZAÇÃO DETRAN/PA	
8	COMPOSIÇÃO DE PREÇOS DE INSTALAÇÃO E CONFIGURAÇÃO - DETRAN/PA (Parcela Única)	
9	COMPOSIÇÃO DE PREÇOS PARA INSTALAÇÃO DA BASE DE INFRAESTRUTURA PARA SOLUÇÃO DE TELECOMUNICAÇÃO MÓVEL DE FISCALIZAÇÃO	
10	COMPOSIÇÃO DE PREÇOS PARA SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO PARA A REDE DE TELECOMUNICAÇÕES NAS CIRETRANS, POSTOS AVANÇADOS E POSTOS DE FISCALIZAÇÃO	
11	COMPOSIÇÃO DE PREÇOS PARA SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO PARA A REDE DE TELECOMUNICAÇÕES PRÉDIO SEDE	
12	COMPOSIÇÃO DE PREÇOS DE REFERÊNCIAS PARA IMPLEMENTAÇÃO DE SERVIÇOS DE GESTÃO EM SEGURANÇA DA INFORMAÇÃO PARA A REDE DE TELECOMUNICAÇÕES	
VALOR GLOBAL PARA LANCE		



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

ANEXO VII DO TERMO DE REFERÊNCIA
PROVA DE CONCEITO

1. Este anexo visa apresentar as regras para execução das provas de conceitos com o objetivo de assegurar que a empresa licitante possui a capacidade técnica e operacional para o pronto atendimento dos objetos descritos no ANEXO I, sendo esta etapa do processo licitatório mandatória e desclassificatória para a licitante classificada e convocada através do sistema comprasnet que deixar de cumprir na sua totalidade todas as provas de conceito descritas abaixo, assim como, é mandatório a obtenção de 100% (cem por cento) de êxito em cada uma das provas, sob pena de desclassificação.

1.1 A licitante deverá realizar todas as provas de conceitos descritas nos itens abaixo com 100% de eficiência para cada uma das provas, sob pena de desclassificação pela não execução ou pela não assertividade de 100% quanto seus objetivos, não cabendo qualquer responsabilidade financeira por parte do DETRAN com os eventuais custos para implementação e realização das provas de conceito, tanto para a licitante que conseguir êxito total em todas as provas como para a licitante que por ventura venha a fracassar.

1.1.1 Todos os equipamentos incluindo soluções, veículos automotores, pessoal técnico e motoristas que vão conduzir as provas de conceito deverão ser obrigatoriamente de propriedade da licitante assim como os funcionários, sob pena de desclassificação do certame licitatório.

1.2 Prova de conceito dedicada para o item **6.3. do ANEXO I que trata da QUALIDADE E DISPONIBILIDADE DO SERVIÇO PARA A REDE DE COMUNICAÇÃO DIGITAL PRIVATIVA E INDEPENDENTE.**

1.2.1. Latência: O tempo de resposta, medido através de pacotes ICMP de 32 bytes deverá ser inferior a 400 ms (quatrocentos milissegundos) para 90% dos pacotes no caso de enlaces que usem comunicação via satélite, e inferior a 90 ms (noventa milissegundos) para 90% dos pacotes no caso de enlaces terrestres para as



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

localidades fora da região metropolitana de Belém é de 5ms (cinco milissegundos) para as localidades que compõem a região metropolitana de Belém com os municípios de Ananindeua, Icoaraci, Benevides e Marituba, onde a medição será realizada entre um sítio remoto e o sítio central da rede, com a rede sem tráfego. A quantidade mínima de testes ICMP realizados, para efeito do cálculo dos 90% dos pacotes, será de 1000 testes.

1.2.2. A licitante deverá realizar prova de conceito em 4 (quatro) sites do DETRAN, em tempo real, na mesma data, em conjunto com equipe de técnicos do DETRAN que estarão na sede do DETRAN acompanhando as provas em conjunto com a equipe técnica da licitante nas dependências remotas e sede do DETRAN.

1.2.2.1. A licitante deverá providenciar a conectividade entre os sites remotos do DETRAN situados nas localidades, conforme descrito abaixo, com a sede do DETRAN, através de um circuito terrestre de fibra ótica, cabendo ao DETRAN liberar o acesso da equipe técnica da licitante o acesso nas suas dependências para que a licitante possa ativar seus circuitos para a realização dos testes descritos no item 1.2, devendo este teste obter 100% de êxito para os parâmetros descritos do item 1.2. Tanto no circuito situado na região metropolitana de Belém como os sites situados fora da região metropolitana de Belém.

1.2.2.2. A licitante deverá manter durante a realização da prova de conceito 1(um) técnico do seu quadro de funcionários em cada um dos sites, onde os parâmetros descritos no item 1.2 deverão ser realizados no mínimo 3 (três) vezes para cada um dos sites em conjunto com 1(um) técnico da licitante e equipe técnica do DETRAN, devendo cada um dos testes ter seu resultado com 100% de êxito alcançado, devendo os mesmos serem salvos em mídia digital e anexado junto ao processo licitatório a fim de comprovação da prova realizada e com êxito de 100%;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.2.2.2.1 Os testes com circuitos com enlaces de comunicação via satélite deverão ser realizados em ambos os sites remotos, fora da região metropolitana de Belém seguindo os mesmos padrões e quantidade de testes descritos no item 1.2. e 1.2.1 para os circuitos terrestres observando a latência específica para cada um dos tipos de circuitos descritos no item 6.3.1. do ANEXO I.

1.2.2.2.2 Os testes com os 2 (dois) circuitos com enlaces entre o DETRAN SEDE e o SITE DE CONTINGÊNCIA de comunicação com velocidade de 10 Gb deverão ser realizados na região metropolitana de Belém, conforme o item 8.6.1 do Anexo 1, seguindo os mesmos padrões e quantidade de testes descritos no item 1.2. e 1.2.1 para estes circuitos terrestres observando a latência específica descrita no item 6.3.1. do ANEXO I.

1.2.2.2.3 Deverão ser apresentado o software de monitoramento e auditoria previstos no item 6.2.2 e 6.2.3 do Anexo 1, com a demonstração de requisitos nesta prova de conceito;

1.2.1.3. Endereço das localidades para prova de conceito dos itens 6.3. e 6.3.1. do ANEXO I.

- **Site 1** localizado na região metropolitana de Belém (Parque Shopping Belém);
- **Site 2** localizado fora da região metropolitana de Belém (Posto de fiscalização alça viária) situado no Km 14, Rodovia PA 483.
- **Site 3** localizado fora da região metropolitana de Belém (Ciretran de São Félix do Xingu) situada na rua Independência, 955, bairro Alecrim.
- **Site 4 – Site de Contingência** localizado na região metropolitana de Belém (DETRAN SEDE), situado na Av Augusto Montenegro Km3

1.2.1.4. A Licitante classificada em primeiro lugar deverá realizar a prova de conceito em até 10 (dez) dias úteis, contados a partir da sua convocação publicada no sistema comprasnet, devendo as provas de conceito serem realizadas entre os horários das 11:00 até as 14:00.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.3. Prova de conceito para o item 14 e 14.1.3. A CONTRATADA deverá possuir estrutura própria para o transporte das soluções de fiscalização móveis para os modelos A,B e C composta por caminhão do tipo cavalo mecânico do tipo 6x2, equipado com equipamento próprio para içamento das soluções móveis de fiscalização do tipo munck, devendo a lança do munk ter no mínimo 15 metros de comprimento, com capacidade mínima de carga de 10 toneladas nesta configuração com capacidade para poder embarcar e desembarcar as unidades em qualquer localidade designada pelo DETRAN

sempre que for solicitado. Semirreboque do tipo carga seca, própria para o transporte de contêiner de até 12 metros de comprimento, equipada com 08 travas de segurança em sua estrutura para fixar container de 6 metros ou 12 metros, devendo os equipamentos serem de propriedade da contratada assim como o motorista ser funcionário da mesma, não sendo possível a subcontratação dos mesmos tendo em vista que a CONTRATADA deverá manter o serviço disponível para atendimento do DETRAN de forma continuada para o pronto atendimento dentro do prazo de 12 horas úteis, a partir da solicitação feita pelo DETRAN para efetuar a movimentação de uma solução de fiscalização móvel de um ponto A para um ponto B dentro do território do estado do Pará.

1.3.1. A licitante deverá realizar esta prova de conceito na sede do DETRAN, cabendo a mesma realizar o desembarque e embarque de uma estrutura do tipo container com 12 (doze) metros de comprimento utilizando para o seu transporte um equipamento rodoviário do tipo semirreboque próprio para o transporte de container com travas de segurança, próprias para container, em sua estrutura, puxada por um veículo do tipo caminhão (cavalo mecânico) equipado com sistema de içamento (munck) capaz de retirar o container do semirreboque e coloca-lo sobre o solo com uma distância mínima de 5 (cinco) metros do semirreboque, devendo a manobra de desembarque (retirar um container de cima do semirreboque, colocar no solo, depois embarcar o mesmo no semirreboque e prendê-lo nas travas de segurança) ser executada pelo conjunto, cavalo mecânico e semi reboque, não podendo sob hipótese alguma utilizar outro equipamento para realizar a manobra que não seja esta configuração, devendo a operação ficar a cargo de um funcionário da licitante, incluindo o próprio motorista.

1.3.1.1. Todos os equipamentos dedicados para realização da prova de



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

conceito devem ser obrigatoriamente da licitante, devendo a licitante apresentar os documentos de registro junto ao sistema RENAVAN (CRLV), assim como o motorista do cavalo mecânico também deve ser funcionário da licitante devidamente registrado e com habilitação válida, categoria E

1.3.1.2. A Licitante classificada em primeiro lugar deverá realizar a prova de conceito em até 10 (dez) dias úteis, contados a partir da sua convocação publicada no sistema comprasnet, devendo a prova de conceito ser realizada entre os horários das 09:00 até as 11:00.

1.4. Prova de conceito dedicada para os item 13, 13.1 e 13.2 do ANEXO I

1.4.1. A Licitante deverá comprovar a capacidade técnica operacional para o item 13.1. **(Equipamento tipo 01- Portátil)** capaz de fornecer conexão do tipo banda larga, via satélite, utilizando antena do tipo fixa, própria para ser utilizada de forma estacionária (local fixo), capaz de enviar e receber dados, voz e imagem com as características descritas no item 13.1 do ANEXO I, devendo a prova de conceito ser realizada no mesmo site situado fora da área metropolitana de Belém (Posto de fiscalização do DETRAN alça viária) situado na Rodovia PA 483, Km 14, cabendo a licitante, garantir o acesso em tempo real pelos agentes da DTO a página do DETRAN na internet para realizar consultas sobre veículos e condutores, realizar acesso a base nacional de veículos (RENAVAN e RENACH) para consultas de veículos e condutores utilizando todos os itens que compõe a solução portátil do tipo 1.

1.4.1.1. A licitante deverá obter 100% de êxito para os parâmetros descritos no item 13.1. do ANEXO I e todos os acessos deverão ser registrados em mídia digital e anexada ao processo licitatório.

1.4.1.2. A Licitante classificada em primeiro lugar deverá realizar a prova de conceito em até 10 (dez) dias úteis, contados a partir da sua convocação publicada no sistema comprasnet, devendo a prova de conceito ser realizada entre os horários das 11:00 até as 14:00.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

14.2. A Licitante deverá comprovar a capacidade técnica operacional para o item 13.2 (**Equipamento tipo 02 – Veicular**) terminal móvel capaz de fornecer conexão do tipo banda larga via satélite, capaz de enviar e receber dados, voz e imagem, próprio para ser montado sobre o teto de veículos automotores com capacidade de funcionamento para a transmissão e recebimento de dados, mesmo com o veículo em movimento, com as características descritas no item 13.2 do ANEXO I.

14.3 A Licitante classificada em primeiro lugar deverá realizar a prova de conceito em até 10 (dez) dias úteis, contados a partir da sua convocação publicada no sistema comprasnet, devendo a prova de conceito ser realizada entre os horários das 11:00 até as 14:00 tendo como local para realizar a prova de conceito o posto de fiscalização do DETRAN na alça viária, onde os testes deverão ser conduzidos na rodovia PA 483, Km 14.

QUESTIONÁRIO DA POC

item	ELEMENTOS DE VISUALIZAÇÃO	SIM	NÃO
1	Os colaboradores (técnico(s), administrativo, gerente e/ou motorista(s)) que irão demonstrar a POC são contratados pela empresa, ou seja, possui vínculo empregatício de caráter não eventual.		
2	Veículo (s) é (são) registrados em nome da empresa licitante.		
3	A empresa para fins de latência, demonstrou o tempo de resposta, medido através de pacotes ICMP de 32 bytes deverá ser inferior a 400 ms (quatrocentos milissegundos) para 90% dos pacotes no caso de enlaces que usem comunicação via satélite, inferior a 90 ms (noventa milissegundos) para 90% dos pacotes no caso de enlaces terrestres para as localidades fora da região metropolitana de Belém e de 5ms (cinco milissegundos) para		



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

	as localidades que compõem a região metropolitana de Belém com os municípios de Ananindeua, Icoaraci, Benevides e Marituba, onde a medição será realizada entre um sítio remoto e o sítio central da rede, com a rede sem tráfego. A quantidade mínima de testes ICMP realizados, para efeito do cálculo dos 90% dos pacotes, será de 1000 testes.		
4	Demonstração de testes em circuitos com enlaces de comunicação via satélite em ambos os sites remotos, fora da região metropolitana de Belém seguindo os mesmos padrões do item 3 (latência específica).		
5	A empresa disponibilizou equipe e operacionalizou o acesso a 3 (três) sites (localidade) de forma simultânea, ou seja, na mesma hora e data no qual deverá ter a participação de técnicos da DTI - Diretoria de Tecnologia e Informática e empresa licitante para acompanhamento da execução que deverá atender em 100%.		
6	Site 1 (Localidade): localizado na região metropolitana de Belém (Parque Shopping Belém) estação cidadania		
7	Site 2 (Localidade): localizado fora da região metropolitana de Belém (Posto de fiscalização alça viária) situado no Km 14, Rodovia PA 483.		
8	Site 3 (Localidade): localizado fora da região metropolitana de Belém (Ciretran de São Félix do Xingu) situada na cidade de São Félix do Xingú.		
9	Site 4 – SITE DE CONTINGÊNCIA (Localidade): localizado na região metropolitana de Belém (Parque de retenção do Benguí) – TESTE DE ROTA A e B com velocidade de 10 GB e latência de 5 (cinco) milissegundos;		
10	A empresa possuir estrutura própria (apresentar CRLV do veículo atual e contrato de trabalho do condutor) para o transporte das soluções de fiscalização móveis para os modelos A, B e C composta por caminhão do tipo cavalo mecânico do tipo 6x2, equipado com equipamento próprio para içamento das soluções móveis de fiscalização do tipo munk, devendo a lança do munk ter no mínimo 15 metros de comprimento, com capacidade de carga mínima de 10 toneladas nesta configuração, com capacidade para poder embarcar e desembarcar as unidades.		
11	Semirreboque do tipo carga seca, própria para o transporte de contêiner de até 12 metros de comprimento, equipada com 08 travas de segurança em sua estrutura para fixar container de 6 metros ou 12 metros, (apresentar CRLV do semirreboque e contrato de trabalho do operador/condutor)		



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

12	A empresa licitante demonstrou o embarque e desembarque de uma estrutura do tipo container com 12 (doze) metros de comprimento utilizando para o seu transporte um equipamento rodoviário do tipo semirreboque próprio para o transporte de container com travas de segurança, próprias de contenier, em sua estrutura, puxada por um veículo do tipo caminhão (cavalo mecânico) 6x2, equipado com sistema de içamento (munck) capaz de retirar o container do semirreboque e coloca-lo sobre o solo com uma distância mínima de 5 (cinco) metros do semirreboque, devendo a manobra de desembarque (retirar um container de cima do semirreboque, colocar no solo, depois embarcar o mesmo no semirreboque e prendê-lo nas travas de segurança) ser executada pelo conjunto, cavalo mecânico e semi reboque, não podendo sob hipótese alguma utilizar outro equipamento para realizar a manobra que não seja esta configuração, devendo a operação ficar a cargo de um funcionário da licitante, incluindo o próprio motorista.		
13	A empresa licitante está com equipamento portátil – tipo 1, local: site 2 (Rodovia Alça Viária, PA 483, Km 14) – apresentou conexão do tipo banda larga, via satélite, utilizando antena do tipo fixa, própria para ser utilizada de forma estacionária (local fixo), capaz de enviar e receber dados, voz e imagem com as seguintes características mínimas aceitáveis para demonstrar: 12.1 - Peso do terminal não superior a 11 (onze) quilos, podendo ser transportado em maleta; 12.2 - Possuir interfaces ethernet, 12.3 - Alimentação do tipo AC; 12.4- Capacidade de download de 20 mbps; 12.5 - Capacidade de upload de 10 mbps; 12.6 - Capacidade de trabalhar com VPN; 12.7 – Capacidade de enviar e receber imagem de vídeo;		



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

	Streaming; Uma vez apresentados os itens acima elencados que compõe a solução portátil foi possível acessar à página do DETRAN na internet para realizar consultas sobre veículos e condutores, e ainda realizar acesso a base nacional de veículos (RENAVAN e RENACH) para consultas de veículos e condutores para fins de comprovação da efetivação e atendimento.		
14	A empresa licitante apresentou para o (Equipamento tipo 02 – Veicular) com terminal móvel com fornecimento de conexão do tipo banda larga via satélite, capaz de enviar e receber dados, voz e imagem, próprio para ser montado sobre o teto de veículos automotores com capacidade de funcionamento para a transmissão e recebimento de dados, mesmo com o veículo em movimento com as seguintes características mínimas a serem observadas: a) Peso do terminal para ser instalado dentro do veículo não superior a 11 (onze) quilos, conforme indicação do fabricante. b) Possuir antena externa, própria para ser fixada sobre o teto do veículo utilizando sistema de fixação magnética ou por parafusos. c) Possuir capacidade de alinhar a sua antena de forma automática em relação ao satélite, mesmo com o veículo em movimento, sem interferência humana. d) Possuir capacidade de manter de forma contínua a transmissão e recepção de dados com o veículo em movimento e em velocidade superior a 100 km por hora. e) Possuir interfaces do tipo , ethernet, f) Alimentação do tipo DC, podendo operar com 12 volts DC. h) Capacidade de download de 20 Mbps i) Capacidade de upload de 10 Mbps j) Capacidade de trabalhar com VPN.		



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

15	Demonstração dos itens do software de monitoramento e auditoria. • Os equipamentos dos enlaces deverão estar com protocolo habilitado SNMP, somente leitura e aferindo o consumo do link. • Demonstrar por comando Ping “verificar se há perdas de pacote” e sua latência conforme edital. • Demonstrar consumo de download e upload durante a apresentação da solução. • Deverá ser usada ferramenta para gerar os tráfegos de upload e download nos links entre DETRAN SEDE e SITE de CONTINGÊNCIA. Durante no mínimo 5 minutos de “stress” dos links comprovando os 10 gb nos dois links.		



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.5 PROVA DE CONCEITO (POC) PARA SERVIÇOS GERENCIADOS DE CIBERSEGURANÇA E OBSERVABILIDADE DA REDE

1.5.1. A Prova de Conceito (POC) destina-se à verificação da compatibilidade da plataforma tecnológica e dos serviços ofertados com as exigências funcionais da contratação, compreendendo a demonstração prática e operacional do pleno funcionamento dos requisitos especificados no TR, nas quatro áreas: SOC, CSIRT, Gestão dos Riscos de Terceiros (TPRM) e Observabilidade e Monitoramento Unificado.

1.5.2. A área de Observabilidade visa demonstrar as capacidades de uma plataforma integrada para monitoramento de infraestrutura, aplicações, serviços e componentes de negócio, proporcionando visibilidade operacional em tempo real, alarmística inteligente, análise de desempenho e apoio à tomada de decisão.

1.5.3. A PROPONENTE deverá comprovar o percentual de 100% (cem por cento) de atendimento dos requisitos descritos no Roteiro Obrigatório deste Anexo. A POC tem caráter eliminatório.

1.5.4. A CONTRATANTE designará comissão técnica que acompanhará a PROPONENTE CONVOCADA em todas as etapas, registrando os resultados em relatório.

1.5.5. A PROPONENTE CONVOCADA será responsável por prover todo o ambiente necessário (hardware, software, banco de dados, conectividade à Internet e demais recursos) à realização da POC, em quantidade e especificação suficientes para a execução de todos os passos.

1.5.6. A execução dos passos será de responsabilidade da PROPONENTE CONVOCADA, com acompanhamento e supervisão da comissão técnica da CONTRATANTE.

1.5.7. Além das atividades do Roteiro Obrigatório, poderá ser solicitada a demonstração de qualquer outra funcionalidade ou requisito especificado no TR.

1.5.8. As demais proponentes poderão acompanhar a POC em local determinado pela comissão técnica, vedada qualquer manifestação durante a realização; manifestações deverão ser anotadas e apresentadas ao final dos testes.

1.5.9. Cada proponente poderá enviar, no máximo, 1 (um) representante legal e 2 (dois) representantes técnicos para acompanhamento.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.5.10. Deverá ser possível à comissão técnica, durante todo o período da POC, o acesso sem impedimentos à estrutura da solução apresentada, para confirmação dos itens demonstrados, incluindo consoles administrativas, configurações e logs.

1.5.11. A PROPONENTE deverá fornecer contas de acesso à solução para a comissão técnica, com os papéis necessários à validação dos processos e funcionalidades (no mínimo: perfil administrador, perfil operador e perfil somente leitura/executivo).

1.6. LOCAIS, PRAZOS E REGRAS DE EXECUÇÃO

1.6.1. A POC será realizada em sessão aberta, nas dependências da do DETRAN-PA (endereço e horário a serem indicados na convocação), podendo parte dos recursos ser acessada remotamente a partir da infraestrutura da PROPONENTE, desde que visível e auditável pela comissão.

1.6.2. A PROPONENTE CONVOCADA terá prazo de até 10 (dez) dias úteis após a convocação para iniciar a POC, sob pena de desclassificação.

1.6.3. Após o início, a PROPONENTE CONVOCADA terá prazo de até 5 (cinco) dias úteis para concluí-la, sob pena de desclassificação.

1.6.4. Cronograma de referência (poderá ser ajustado pela comissão técnica).

1.6.5. A PROPONENTE poderá utilizar base de dados de demonstração (DEMO) para facilitar a verificação, ou base em ambiente de testes e/ou homologação da CONTRATANTE, desde que os dados utilizados permitam executar integralmente os roteiros.

1.6.6. A PROPONENTE poderá apresentar plano de testes próprio compatível com as funcionalidades do Roteiro Obrigatório, com o intuito de facilitar a verificação, sem prejuízo da execução integral dos cenários deste Anexo.

1.6.7. Todos os tempos medidos (notificação, bloqueio, resposta) serão cronometrados pela comissão técnica com base nos timestamps das próprias plataformas, que deverão estar sincronizadas via NTP.

1.7. INFRAESTRUTURA E PRÉ-REQUISITOS DA POC



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.7.1. A PROPONENTE deverá disponibilizar, no mínimo, o seguinte ambiente de demonstração:

- Instância completa do ecossistema SOC: SIEM, SOAR, plataforma de dashboards, plataforma de Threat Intelligence e plataforma de bloqueio automatizado, hospedados em datacenter no Brasil (produção ou homologação equivalente);
- No mínimo 1 (um) sensor honeypot ativo e acessível, hospedado no Brasil, com histórico mínimo de 7 (sete) dias de capturas reais;
- Laboratório de ataque/vítima: ao menos 1 (um) host atacante (ex.: distribuição de pentest), 1 (um) servidor Linux e 1 (um) host Windows como vítimas, gerando logs para o SIEM;
- Firewall de laboratório (físico ou virtual) de pelo menos um dos fabricantes exigidos (pfSense ou FortiGate), integrado à plataforma de bloqueio automatizado, com tráfego de teste passante;
- Plataforma TPRM com organização de demonstração contendo: 1 (uma) conta de nuvem pública (mínimo AWS, Azure ou GCP) com falhas de configuração proposital, 1 (um) domínio DNS público para EASM e 1 (uma) organização terceira fictícia para fluxo de questionários;
- Portal ITSM operacional;
- Arquitetura da solução de Observabilidade baseada em microsserviços, proporcionando escalabilidade, alta disponibilidade, resiliência operacional e independência entre componentes;
- Componentes de observabilidade configurados para: Coleta de métricas, Processamento de eventos, Armazenamento histórico, Camada de APIs e Visualização e análise de dados;
- Monitoramento ativo de ativos de infraestrutura, aplicações, serviços críticos, URLs, APIs, endpoints e validação de certificados digitais;
- Conectividade, projetor/telão e acesso de leitura da comissão a todas as consoles.

1.7.2. A comissão técnica poderá indicar valores, nomes, IPs e parâmetros a serem utilizados nos testes, no ato da execução, para afastar demonstrações pré-gravadas. É vedado o uso de vídeos, apresentações ou simulações não funcionais como substituto de demonstração ao vivo.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.8. ROTEIRO OBRIGATÓRIO - ÁREA 1: SOC

1.8.1. Arquitetura, código aberto e soberania de dados

Objetivo: Comprovar que as plataformas centrais são de código aberto, customizáveis, e que toda a infraestrutura está hospedada em território brasileiro (item 19.3.1 do TR).

Pré-requisitos: Acesso administrativo às consoles; documentação de licenças; declaração do provedor de datacenter.

Roteiro de execução:

1.8.1.1. Apresentar a console do SIEM e identificar o software, sua versão e a licença de código aberto correspondente (aprovada pela OSI), exibindo a documentação pública do projeto;

1.8.1.2. Repetir a identificação para SOAR, plataforma de dashboards e componentes de coleta (agentes/coletores);

1.8.1.3. Demonstrar capacidade de customização: criar, ao vivo, um extrator/parser de campo e uma regra simples definida pela comissão;

1.8.1.4. Comprovar a hospedagem no Brasil: resolução DNS e geolocalização dos IPs das plataformas, teste de latência a partir da rede local, e apresentação da declaração do datacenter/nuvem nacional;

1.8.1.5. Demonstrar que não há tráfego de logs para fora do território nacional (arquitetura de rede, destinos configurados nos coletores e regras de saída);

1.8.1.6. Exibir interfaces em português do Brasil;

1.8.1.7. Demonstrar RBAC e segregação por cliente/ambiente (multitenancy) nas plataformas.

Evidências obrigatórias: Telas das consoles com versões e licenças; resultado de geolocalização/latência; declaração do datacenter; captura da regra e do parser criados ao vivo.

Critério de aceite: Todos os componentes centrais comprovadamente open source e hospedados no Brasil, com customização demonstrada ao vivo. Resultado registrado como ATENDE / NÃO ATENDE.

1.8.2. Coleta, normalização e busca de eventos



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Objetivo: Comprovar a capacidade de coleta multiprotocolo, normalização e busca eficiente de eventos no SIEM (item 19.4.2.do TR).

Pré-requisitos: Hosts do laboratório (Linux, Windows e firewall) configurados como fontes de log.

Roteiro de execução:

1.8.2.1. Demonstrar ingestão simultânea por, no mínimo, 3 (três) métodos: agente instalado (Windows e/ou Linux), syslog (firewall) e API/integração;

1.8.2.2. Gerar eventos reais nos três ambientes (login, alteração de configuração, tráfego bloqueado) e exibi-los no SIEM em tempo quase-real;

1.8.2.3. Demonstrar a normalização: campos extraídos (IP origem/destino, usuário, ação, severidade) consistentes entre fontes distintas;

1.8.2.4. Executar buscas com a linguagem de consulta da plataforma, incluindo filtro por intervalo de tempo, agregação (contagem por IP de origem) e exportação do resultado;

1.8.2.5. Demonstrar o pipeline de processamento aplicando transformação/enriquecimento em evento definido pela comissão;

1.8.2.6. Exibir a configuração de retenção (90 dias online / 12 meses arquivado) e o mecanismo de housekeeping/expurgo.

Evidências obrigatórias: Telas de ingestão por cada método; consultas executadas e seus resultados; configuração de retenção.

Critério de aceite: Ingestão pelos três métodos funcionando, eventos normalizados e pesquisáveis em tempo quase-real. Resultado registrado como ATENDE / NÃO ATENDE.

1.8.3. Correlação, detecção e MITRE ATT&CK

Objetivo: Comprovar a detecção em tempo quase-real de ataques reais por regras de correlação mapeadas em MITRE ATT&CK (item 19.4.3. do TR).

Pré-requisitos: Host atacante do laboratório com ferramentas de teste; casos de uso activos no SIEM.

Roteiro de execução:



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.8.3.1. Executar, a partir do host atacante, ataque de força bruta SSH contra o servidor Linux do laboratório (ferramenta à escolha, ex.: hydra), e evidenciar a geração automática de alerta no SIEM com severidade e técnica MITRE ATT&CK associada (ex.: T1110);

1.8.3.2. Executar varredura de portas (ex.: nmap) contra a rede do laboratório e evidenciar o alerta correspondente;

1.8.3.3. Executar teste com arquivo EICAR no host Windows e evidenciar a detecção de malware refletida no SIEM;

1.8.3.4. Demonstrar detecção de comunicação com IOC conhecido: gerar tráfego para IP/domínio constante da base de Threat Intelligence e evidenciar o alerta de correlação;

1.8.3.5. Apresentar o catálogo de casos de uso ativos com o respectivo mapeamento MITRE ATT&CK;

1.8.3.6. Criar, ao vivo, uma regra de correlação solicitada pela comissão (ex.: N falhas de login seguidas de sucesso no mesmo usuário) e demonstrá-la funcionando.

Evidências obrigatórias: Alertas gerados com timestamps; mapeamento ATT&CK; regra criada ao vivo e seu disparo.

Critério de aceite: Todos os ataques simulados detectados automaticamente, com classificação correta e regra criada ao vivo funcional. Resultado registrado como ATENDE / NÃO ATENDE.

1.8.4. Integração SIEM / SOAR - automação e playbooks

Objetivo: Comprovar a integração nativa e bidirecional SIEM/SOAR com execução automática de playbooks (item 19.4.4.1 do TR).

Pré-requisitos: Cenário S3 executado (alertas disponíveis).

Roteiro de execução:

1.8.4.1. Demonstrar que o alerta de força bruta do cenário S3 disparou automaticamente um caso/playbook na plataforma SOAR, sem intervenção humana;

1.8.4.2. Exibir o playbook executado: enriquecimento automático do IP atacante (reputação, geolocalização, WHOIS, consulta a Threat Intelligence), com os resultados anexados ao caso;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.8.4.3. Evidenciar a abertura automática de ticket no Portal ITSM vinculado ao caso, com numeração e rastreabilidade;

1.8.4.4. Apresentar a biblioteca de playbooks exigida (força bruta, varredura, malware, phishing, IOC conhecido e exfiltração);

1.8.4.5. Modificar, ao vivo, um playbook (incluir etapa indicada pela comissão, ex.: nova consulta de enriquecimento ou nova ação de notificação) e reexecutá-lo com sucesso;

1.8.4.6. Demonstrar atualização bidirecional: action executada no SOAR refletida no alerta/caso do SIEM e vice-versa.

Evidências obrigatórias: Linha do tempo do caso no SOAR; ticket criado no ITSM; playbook alterado ao vivo; logs de execução.

Critério de aceite: Disparo automático comprovado, enriquecimento funcional, ticket automático e playbook editado ao vivo. Resultado registrado como ATENDE / NÃO ATENDE.

1.8.5. Notificações multicanal

Objetivo: Comprovar o motor de notificações multicanal integrado ao SIEM/SOAR, em todos os canais exigidos (item 19.4.4.2 do TR).

Pré-requisitos: Contas/destinos de teste para cada canal, com dispositivos visíveis à comissão.

Roteiro de execução:

1.8.5.1. Apresentar a matriz de comunicação configurável: canais por severidade, por tipo de evento e por destinatário;

1.8.5.2. Gerar evento de severidade alta (reutilizando o laboratório) e evidenciar o recebimento de notificação automática em CADA UM dos canais: ligação telefônica automatizada (chamada de voz recebida e atendida diante da comissão), WhatsApp, Telegram, Microsoft Teams, Slack, Discord e e-mail;

1.8.5.3. Cronometrar o tempo entre a geração do alerta e a emissão das notificações, que não poderá exceder 5 (cinco) minutos;

1.8.5.4. Demonstrar o acionamento simultâneo de múltiplos canais para o mesmo evento;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.8.5.5. Configurar, ao vivo, política distinta por severidade definida pela comissão (ex.: P1 = ligação + WhatsApp; P3 = somente e-mail) e demonstrar seu funcionamento;

Evidências obrigatórias: Registro audiovisual/fotográfico dos recebimentos em cada canal; timestamps das plataformas; configuração da matriz.

Critério de aceite: Notificação recebida nos 7 (sete) canais, dentro do tempo máximo, com matriz configurável e escalonamento por ausência de ACK funcionando. Resultado registrado como ATENDE / NÃO ATENDE.

1.8.6. Plataforma de bloqueio automatizado integrada ao firewall

Objetivo: Comprovar o bloqueio automático de IP malicioso no firewall da CONTRATANTE, sem intervenção humana (item 19.4.4.3 do TR).

Pré-requisitos: Firewall de laboratório (pfSense ou FortiGate) integrado à plataforma de bloqueio; host atacante com IP controlado.

Roteiro de execução:

1.8.6.1. Apresentar a arquitetura da plataforma de bloqueio: mecanismo de distribuição das listas dinâmicas (HTTP(S)/EDL/API), autenticação e integração configurada no firewall de laboratório;

1.8.6.2. Executar, a partir do host atacante, atividade maliciosa detectável (ex.: força bruta ou varredura agressiva) contra o ambiente monitorado;

1.8.6.3. Evidenciar a constatação automática de maliciosidade (correlação no SIEM) e a inclusão automática do IP atacante na lista de bloqueio, sem qualquer ação manual;

1.8.6.4. Evidenciar no firewall a efetivação do bloqueio: presença do IP na lista/objeto consumido e tráfego subsequente do atacante efetivamente negado (logs de deny);

1.8.6.5. Cronometrar o tempo entre a constatação de maliciosidade e a efetivação do bloqueio, que não poderá exceder 5 (cinco) minutos;

1.8.6.6. Demonstrar a lista de exceções (whitelist): incluir o IP do atacante na whitelist e comprovar que ele não volta a ser bloqueado, com precedência garantida;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.8.6.7. Demonstrar a política de expiração/remoção controlada de bloqueios e a remoção manual auditada;

1.8.6.8. Exibir o painel de bloqueios ativos e a trilha de auditoria completa do ciclo (origem da detecção, evidência, data/hora, regra aplicada, remoção);

1.8.6.9. Demonstrar suporte ao segundo fabricante exigido (pfSense e FortiGate), ao menos por configuração documentada e tela de integração, caso apenas um esteja fisicamente no laboratório.

Evidências obrigatórias: Logs do firewall (deny) antes/depois; lista dinâmica consumida; painel de bloqueios; trilha de auditoria; cronometragem.

Critério de aceite: Cadeia detecção → bloqueio 100% automática, dentro do tempo máximo, com whitelist, expiração e auditoria comprovadas. Resultado registrado como ATENDE / NÃO ATENDE.

1.8.7. Honeypot e cadeia completa honeypot → SIEM → bloqueio

Objetivo: Comprovar a operação dos honeypots no Brasil, a riqueza das capturas e o bloqueio automático de IOCs coletados (item 19.4.4.4 do TR).

Pré-requisitos: Sensor honeypot ativo com histórico ≥ 7 dias; cenário S6 operacional.

Roteiro de execução:

1.8.7.1. Apresentar a malha de honeypots: quantidade, provedores/regiões no Brasil e comprovação de hospedagem nacional (geolocalização dos IPs e documentação);

1.8.7.2. Exibir o histórico real de capturas dos últimos 7 (sete) dias, demonstrando os campos mínimos: IP e porta de origem, domínio reverso, geolocalização, payload da requisição, credenciais tentadas (login/senha) e amostras de malware coletadas;

1.8.7.3. Realizar, a partir do host atacante, interação ao vivo com o honeypot (ex.: tentativas de autenticação SSH com credenciais indicadas pela comissão) e evidenciar o registro completo da interação;

1.8.7.4. Evidenciar a ingestão automática e contínua dos eventos e IOCs do honeypot no SIEM;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.8.7.5. Evidenciar que o IP atacante, constatado malicioso a partir das interações com o honeypot, foi automaticamente propagado à plataforma de bloqueio e bloqueado no firewall do laboratório - cadeia completa honeypot → SIEM → plataforma de bloqueio → firewall - sem intervenção humana;

1.8.7.6. Cronometrar o tempo de ponta a ponta da cadeia, que não poderá exceder 5 (cinco) minutos;

1.8.7.7. Exibir a trilha de auditoria do bloqueio originado do honeypot, identificando a origem da detecção como honeypot.

Evidências obrigatórias: Histórico de capturas; registro da interação ao vivo; eventos no SIEM; bloqueio no firewall com auditoria; cronometragem.

Critério de aceite: Capturas com todos os campos mínimos e cadeia completa automatizada comprovada dentro do tempo máximo. Resultado registrado como ATENDE / NÃO ATENDE.

1.8.8. Dashboards integrados e Inteligência Artificial

Objetivo: Comprovar a plataforma de dashboards integrada ao SIEM e ao honeypot, com recursos de IA embarcados (itens 19.4.4.5 e 19.4.4.6 do TR).

Pré-requisitos: Cenários S2 a S7 executados (dados disponíveis).

Roteiro de execução:

1.8.8.1. Apresentar a plataforma de dashboards integrada ao SIEM, com painéis em tempo quase-real: visão executiva, eventos por severidade/origem/destino, ataques por geolocalização, top ofensores, top ativos atacados, tendências, SLA e bloqueios automatizados;

1.8.8.2. Demonstrar que os eventos dos cenários anteriores (ataques, bloqueios, honeypot) estão refletidos nos painéis;

1.8.8.3. Apresentar painel dedicado do honeypot na mesma plataforma: interações por sensor, origens, serviços atacados, credenciais mais tentadas e malwares coletados;

1.8.8.4. Demonstrar os recursos de IA dos dashboards: sumarização automática, em português do Brasil, dos eventos/incidentes de um período indicado pela comissão;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.8.8.5. Demonstrar apoio de IA à investigação: a partir de um alerta dos cenários anteriores, obter explicação do alerta, contexto e recomendação de próximos passos;

1.8.8.6. Demonstrar consulta em linguagem natural (português) sobre os dados de segurança e o destaque automático de anomalias/tendências;

1.8.8.7. Criar, ao vivo, um painel/visualização solicitado pela comissão e aplicar identidade visual customizada (logotipo/cores);

1.8.8.8. Demonstrar perfis de acesso distintos aos dashboards (executivo e técnico).

Evidências obrigatórias: Telas dos painéis com os dados da POC; respostas da IA; evidência de processamento nacional; painel criado ao vivo.

Critério de aceite: Dashboards unificados (SIEM + honeypot) funcionais, com IA operante em PT-BR, processada no Brasil, e customização ao vivo. Resultado registrado como ATENDE / NÃO ATENDE.

1.8.9. Threat Intelligence

Objetivo: Comprovar a plataforma de inteligência de ameaças e sua correlação automática com o ambiente monitorado (item 19.4.3.3 do TR).

Pré-requisitos: Plataforma de Threat Intelligence integrada ao SIEM.

Roteiro de execução:

1.8.9.1. Apresentar as fontes de inteligência configuradas (feeds públicos e privados) e o processo de agregação e normalização de IOCs;

1.8.9.2. Demonstrar a integração via STIX/TAXII com ingestão de coleção de IOCs;

1.8.9.3. Cadastrar, ao vivo, um IOC indicado pela comissão (IP do host atacante) e evidenciar a correlação retroativa e/ou em tempo real com os eventos do SIEM;

1.8.9.4. Evidenciar que IOCs de alta confiança alimentam automaticamente a plataforma de bloqueio (integração com o cenário S6);

1.8.9.5. Demonstrar consulta de contexto de um IOC (primeira/última atividade, campanhas/famílias associadas, fontes) durante uma investigação.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Evidências obrigatórias: Telas das fontes e IOCs; correlação gerada; bloqueio derivado de IOC; consulta de contexto.

Critério de aceite: Ingestão STIX/TAXII funcional, correlação automática comprovada e realimentação do bloqueio automatizado. Resultado registrado como ATENDE / NÃO ATENDE.

1.8.10. Relatórios, SLA e housekeeping

Objetivo: Comprovar a geração de relatórios operacionais e executivos e os controles de retenção (itens 19.11. do TR).

Pré-requisitos: Dados dos cenários anteriores disponíveis.

Roteiro de execução:

1.8.10.1. Gerar, ao vivo, relatório mensal-tipo contendo: requisições/incidentes abertos e fechados, timestamps completos, responsáveis, descrição de problema/solução, indicadores de SLA, detecções e bloqueios do período;

1.8.10.2. Exportar o relatório em PDF e demonstrar sua disponibilização no Portal ITSM;

1.8.10.3. Demonstrar painel de acompanhamento de SLA com os indicadores da Matriz (atribuição, resposta, resolução, notificação, bloqueio);

1.8.10.4. Demonstrar as rotinas de expurgo/housekeeping e a política de retenção configurada;

1.8.10.5. Demonstrar a exportação de eventos brutos em formato aberto (JSON/CSV) para fins de reversibilidade.

Evidências obrigatórias: Relatório gerado; telas de SLA; configuração de retenção; arquivo exportado.

Critério de aceite: Relatórios completos gerados ao vivo e controles de retenção/reversibilidade demonstrados. Resultado registrado como ATENDE / NÃO ATENDE.

1.9. ROTEIRO OBRIGATÓRIO - ÁREA 2: CSIRT

1.9.1. Portal ITSM, processos e matriz de priorização



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Objetivo: Comprovar o portal ITSM e os processos de gestão de incidentes, solicitações, mudanças e problemas (item 19.3.5.do TR).

Pré-requisitos: Portal ITSM operacional com perfis para a comissão.

Roteiro de execução:

1.9..1.1. Apresentar o Portal ITSM: abertura, acompanhamento, escalonamento e encerramento de chamados, com trilha de auditoria e anexos;

1.9..1.2. Abrir, ao vivo, solicitação de serviço e incidente com impacto/urgência definidos pela comissão, evidenciando o cálculo automático de prioridade pela matriz Impacto x Urgência (P1 a P4);

1.9..1.3. Demonstrar a validação e ajuste de impacto/urgência pela equipe CSIRT;

1.9..1.4. Simular abertura de incidente por telefone, com autenticação de identidade do solicitante e criação do caso pelo CSIRT em nome da CONTRATANTE;

1.9..1.5. Demonstrar os relatórios de solicitações/incidentes e os indicadores de SLA correspondentes;

1.9..1.6. Apresentar o catálogo de serviços e os fluxos de gerenciamento de problemas (identificação a partir de incidentes recorrentes).

Evidências obrigatórias: Tickets criados; matriz aplicada; registro da abertura telefônica; relatórios exibidos.

Critério de aceite: Portal funcional com priorização automática correta e processos formalizados demonstrados. Resultado registrado como ATENDE / NÃO ATENDE.

1.9..2. Resposta completa a incidente simulado (exercício prático)

Objetivo: Comprovar a capacidade operacional de resposta ponta a ponta a um incidente crítico, conforme escopo de operação (item 19.5. do TR), com medição de SLA.

Pré-requisitos: Laboratório da POC; equipe CSIRT da PROPONENTE em regime real de acionamento.

Roteiro de execução:



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.9..2.1. Deverá ser injetado um incidente simulado P1 no ambiente de laboratório (ex.: execução de artefato malicioso com persistência e comunicação de comando e controle em host Windows);

1.9..2.2. Evidenciar a detecção (SOC) e o acionamento do CSIRT, cronometrando o tempo de primeira resposta, que deverá respeitar o SLA de 30 (trinta) minutos para P1;

1.9..2.3. Executar e narrar as fases: aceitação do bilhete; triagem e priorização; coleta de informações; contenção (isolamento do host); erradicação; e restauração do sistema;

1.9..2.4. Demonstrar a análise de causa raiz e a correlação de incidente cruzado (verificação de outros hosts afetados);

1.9..2.5. Evidenciar a comunicação durante o incidente: atualizações no Portal, notificações multicanal e relatório de status;

1.9..2.6. Evidenciar a realimentação automática: IOCs do incidente incorporados ao Threat Intelligence e bloqueados pela plataforma de bloqueio (item 19.5.8.2 do TR);

1.9..2.7. Entregar, ao final, relatório pós-incidente contendo: linha do tempo completa, artefatos, causa raiz, ações executadas, lições aprendidas e recomendações.

Evidências obrigatórias: Linha do tempo do incidente; registros de contenção; relatório pós-incidente; cronometragem do SLA.

Critério de aceite: Incidente contido e documentado dentro dos SLAs, com todas as fases demonstradas ao vivo e realimentação automática comprovada. Resultado registrado como ATENDE / NÃO ATENDE.

1.9..3. Forense digital e cadeia de custódia

Objetivo: Comprovar a capacidade de análise forense com preservação de evidências (item 19.5.9 do TR).

Pré-requisitos: Host comprometido do cenário C2 (ou imagem fornecida pela comissão).

Roteiro de execução:

1.9..3.1. Realizar aquisição forense de memória do host comprometido, com ferramenta apropriada, gerando hash criptográfico da evidência;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.9..3.2. Realizar aquisição de imagem de disco (ou de partição/artefatos relevantes, a critério da comissão), igualmente com hash e registro;

1.9..3.3. Formalizar a cadeia de custódia: identificação da evidência, coletor, data/hora, hashes e armazenamento seguro;

1.9..3.4. Analisar os artefatos: processos, persistência, conexões de rede, artefatos de execução e linha do tempo do comprometimento;

1.9..3.5. Apresentar relatório forense preliminar com as conclusões e os IOCs extraídos.

Evidências obrigatórias: Hashes das evidências; formulário de cadeia de custódia; relatório forense preliminar.

Critério de aceite: Aquisições íntegras (hashes válidos), cadeia de custódia formalizada e análise conclusiva. Resultado registrado como ATENDE / NÃO ATENDE.

1.9..4. Escalonamento, comunicação segura e coordenação externa

Objetivo: Comprovar os fluxos de escalonamento e comunicação do CSIRT (item 19.5.3.3 do TR).

Pré-requisitos: Lista de escalonamento de teste definida pela comissão.

Roteiro de execução:

1.9..4.1. Configurar lista de escalonamento hierárquica fornecida pela comissão e demonstrar o acionamento sucessivo automático em incidente grave sem confirmação do primeiro contato (antigo C6.1);

1.9..4.2. Demonstrar que as notificações automáticas contêm apenas informações mínimas (ID do ticket e descrição não sensível), com detalhes completos restritos ao Portal (antigo C6.2);

1.9..4.3. Demonstrar o bloqueio do envio de anexos por e-mail e o tráfego de anexos exclusivamente pelo Portal (antigo C6.3);

1.9..4.4. Demonstrar a autenticação de identidade em contato telefônico (em ambos os sentidos) (antigo C6.4);



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.9.4.5. Apresentar o procedimento e os modelos de comunicação/coordenação com CSIRTs externos e órgãos competentes (ex.: CERT.br, CTIR Gov), incluindo critérios de acionamento (antigo C6.5);

1.9.4.6. Demonstrar a conta Break Glass: criação, guarda segura, uso emergencial e redefinição de senha após o uso (antigo C6.6).

Evidências obrigatórias: Registros do escalonamento; exemplos de notificações; procedimento documentado; evidência do ciclo Break Glass.

Critério de aceite: Escalonamento automático funcional, comunicação minimizada comprovada e procedimentos de coordenação externa formalizados. Resultado registrado como ATENDE / NÃO ATENDE.

1.9.5. Integração SOC ↔ CSIRT - linha do tempo única

Objetivo: Comprovar que incidentes fluem do SOC ao CSIRT com contexto completo e rastreabilidade única (item 19.5.8. do TR).

Pré-requisitos: Cenários S3-S6 e C2 executados.

Roteiro de execução:

1.9.5.1. A partir de um alerta gerado no SIEM, demonstrar a transferência do caso ao CSIRT com todo o contexto: eventos brutos, enriquecimentos, ações automáticas executadas (notificações e bloqueios) e histórico (antigo C8.1);

1.9.5.2. Exibir a linha do tempo única do incidente, abrangendo desde a detecção no SOC até o encerramento no CSIRT, sem perda de informação entre plataformas (antigo C8.2);

1.9.5.3. Demonstrar que as ações do CSIRT (contenções, mudanças, IOCs) retroalimentam o SOC (novas regras, IOCs em Threat Intelligence, bloqueios) (antigo C8.3);

1.9.5.4. Demonstrar a visão consolidada no dashboard executivo: status de incidentes SOC/CSIRT em painel único (antigo C8.4).

Evidências obrigatórias: Linha do tempo única exibida; evidência de retroalimentação; painel consolidado.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Critério de aceite: Rastreabilidade ponta a ponta sem ruptura entre SOC e CSIRT, com retroalimentação automática. Resultado registrado como ATENDE / NÃO ATENDE.

1.10. ROTEIRO OBRIGATÓRIO - ÁREA 3: GESTÃO DOS RISCOS DE TERCEIROS (TPRM)

1.10.1. Plataforma, soberania e controle de acesso

Objetivo: Comprovar os requisitos gerais da plataforma TPRM (item 19.6 do TR).

Pré-requisitos: Plataforma TPRM com organização de demonstração.

Roteiro de execução:

1.10.1.1. Apresentar a plataforma em interface web, comprovando: ausência de necessidade de instalação de software/hardware no ambiente do cliente ou de terceiros; interface e documentação em português do Brasil;

1.10.1.2. Comprovar a hospedagem integral em território brasileiro (geolocalização dos IPs, arquitetura e declaração do datacenter) e a condição de desenvolvimento próprio ou base em código aberto;

1.10.1.3. Demonstrar o gerenciamento de usuários por convites por e-mail com tempo de expiração;

1.10.1.4. Demonstrar autenticação com duplo fator (senha + TOTP) e autenticação OAuth com identidade Google;

1.10.1.5. Demonstrar os perfis de acesso administrador e operador, com diferenças efetivas de permissão;

1.10.1.6. Demonstrar a segregação por organizações, parceiros, ambientes e equipes.

Evidências obrigatórias: Telas da plataforma; geolocalização; fluxo de convite com expiração; login MFA/OAuth; matriz de perfis.

Critério de aceite: Plataforma SaaS nacional comprovada, com autenticação segura e segregação funcional. Resultado registrado como ATENDE / NÃO ATENDE.

1.10.2. Onboarding de terceiros - nuvem, SaaS e superfície externa

Objetivo: Comprovar o onboarding não intrusivo de ambientes de terceiros.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Pré-requisitos: Conta(s) de nuvem de demonstração com falhas propositalis; domínio público para EASM.

Roteiro de execução:

1.10.2.1. Realizar, ao vivo, o onboarding de uma conta de nuvem pública (mínimo uma entre AWS, Azure ou GCP; as demais - incluindo Huawei Cloud e OCI - poderão ser comprovadas por demonstração de tela e documentação) utilizando credencial com acesso somente leitura a metadados;

1.10.2.2. Comprovar tecnicamente que a credencial utilizada é somente leitura, limitada a parâmetros de configuração e metadados (exibição da política/role aplicada);

1.10.2.3. Realizar o onboarding de superfície externa de ataque (EASM) a partir de domínio DNS indicado pela comissão, com descoberta automática de ativos sem cadastro prévio;

1.10.2.4. Demonstrar o onboarding de ao menos 1 (uma) ferramenta SaaS de produtividade (ex.: Google Workspace, Microsoft 365, GitHub ou Slack), comprovando as demais por documentação;

1.10.2.5. Demonstrar que não há limitação de quantidade de serviços ou itens de configuração testados;

1.10.2.6. Configurar agendamentos distintos por ambiente (diário e semanal) e executar varredura sob demanda.

Evidências obrigatórias: Fluxos de onboarding executados; política read-only exibida; ativos descobertos via EASM; agendamentos configurados.

Critério de aceite: Onboardings funcionais, não intrusivos e com acesso comprovadamente somente leitura. Resultado registrado como ATENDE / NÃO ATENDE.

1.10.3. Questionários de autoavaliação e evidências

Objetivo: Comprovar o ciclo completo de avaliação por questionários.

Pré-requisitos: Organização terceira fictícia com usuário respondente.

Roteiro de execução:



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.10.3.1. Criar, ao vivo, questionário personalizado com os 4 (quatro) tipos de resposta: parágrafo, escolha única, múltipla escolha e upload de arquivo, incluindo perguntas obrigatórias e opcionais;

1.10.3.2. Programar o envio recorrente (mensal, trimestral e anual) para um grupo de terceiros e realizar envio sob demanda para grupo específico;

1.10.3.3. Responder o questionário no papel do terceiro, anexando evidência (arquivo) e tentando concluir sem responder pergunta obrigatória (a plataforma deverá impedir);

1.10.3.4. Demonstrar a comunicação bidirecional: comentários na avaliação e em perguntas individuais, entre emissor e destinatário;

1.10.3.5. Demonstrar o repositório centralizado de evidências de avaliação;

1.10.3.6. Filtrar questionários por status (pendente, concluído, aguardando revisão) e por tempo de resposta; exibir o status por data de vencimento (pontuais x intempestivas);

1.10.3.7. Demonstrar a gestão de questionários ativos e inativos;

1.10.3.8. Exibir o painel de controle interativo com o número de questionários por status e o histograma de duração das avaliações.

Evidências obrigatórias: Questionário criado; agendamentos; respostas com evidências; comentários; painéis e histograma.

Critério de aceite: Ciclo completo de questionários demonstrado ao vivo, com todos os tipos de resposta e antigos controles exigidos. Resultado registrado como ATENDE / NÃO ATENDE.

1.10.4. Varreduras automatizadas e detecção de riscos

Objetivo: Comprovar a detecção automatizada das classes de risco exigidas .

Pré-requisitos: Ambiente de nuvem com falhas proposital (cenário T2).

Roteiro de execução:

1.10.4.1. Executar varredura sob demanda no ambiente de demonstração e evidenciar a detecção de, no mínimo: objeto de armazenamento exposto (ex.: bucket público); credencial/usuário sem MFA ou com privilégio excessivo; serviço indevidamente publicado (ex.:



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

RDP/SMB/FTP exposto); tecnologia ou serviço desatualizado/inseguro; ausência de criptografia (volume, armazenamento ou tráfego); e falha de parâmetros de backup/continuidade;

1.10.4.2. Na superfície externa (EASM), evidenciar a detecção de: portas e serviços expostos; certificado SSL expirado ou inválido; e tecnologia com vulnerabilidade conhecida (CVE associada), quando presente no ambiente de teste;

1.10.4.3. Demonstrar a verificação de ausência de trilha de auditoria/monitoramento e a análise de configuração de IAM (Control Plane);

1.10.4.4. Demonstrar o enriquecimento e contexto adicional nos alertas (descrição do risco, ativo afetado, recomendação de correção e referências);

1.10.4.5. Comprovar que a verificação abrange todos os ativos associados, não por amostragem, sem cadastro prévio;

1.10.4.6. Configurar as periodicidades exigidas (6h/12h/24h/7 dias para nuvem; 24h/7 dias para EASM);

1.10.4.7. Demonstrar a criação automática de alertas/vulnerabilidades a partir dos testes, com a quantidade e os tipos de dados expostos quando aplicável.

Evidências obrigatórias: Lista de detecções com evidências por classe de risco; configurações de periodicidade; alertas gerados automaticamente.

Critério de aceite: Todas as classes de risco exigidas detectadas automaticamente no ambiente de demonstração. Resultado registrado como ATENDE / NÃO ATENDE.

1.10.5. Classificação, frameworks, ciclo de vida e acurácia

Objetivo: Comprovar a classificação multidimensional e o ciclo de vida controlado de riscos .

Pré-requisitos: Detecções do cenário T4 disponíveis.

Roteiro de execução:

1.10.5.1. Filtrar riscos por severidade (crítica, alta, média, baixa, informativa), por estado (fechado, em tratamento, falso positivo, controle mitigatório, risco aceito), por data de criação e por ambiente;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.10.5.2. Demonstrar a classificação por disciplinas (compliance, resposta a incidente, auditoria, backup, confidencialidade, integridade, disponibilidade, monitoramento, hardening);

1.10.5.3. Demonstrar o mapeamento de conformidade dos achados com NIST, CIS Controls, MITRE ATT&CK, PCI DSS e a identificação de potenciais violações de LGPD e GDPR;

1.10.5.4. Tentar encerrar manualmente um alerta detectado automaticamente: a plataforma deverá impedir o fechamento sem verificação;

1.10.5.5. Corrigir, ao vivo, uma das falhas propositais no ambiente de nuvem (ex.: fechar bucket público), executar reverificação e evidenciar o fechamento automático do alerta somente após a confirmação da correção (ciclo completo);

1.10.5.6. Reintroduzir a falha e evidenciar a reabertura/recorrência do risco com manutenção do histórico de mudanças de estado.

Evidências obrigatórias: Filtros aplicados; mapeamentos de conformidade; tentativa de fechamento manual bloqueada; ciclo corrigir→verificar→fechar→reabrir demonstrado.

Critério de aceite: Ciclo de vida íntegro: fechamento somente após verificação automatizada, com histórico completo. Resultado registrado como ATENDE / NÃO ATENDE.

1.10.6. Mascaramento de dados e compartilhamento entre organizações

Objetivo: Comprovar a privacidade entre organizações e o compartilhamento controlado.

Pré-requisitos: Duas organizações configuradas (contratante e terceiro).

Roteiro de execução:

1.10.6.1. Exibir o mesmo achado sob a visão da organização terceira (dados completos) e sob a visão da CONTRATANTE, comprovando o mascaramento de: usuários e dados pessoais; recursos de nuvem; endereços IP; e demais detalhes não públicos;

1.10.6.2. Demonstrar o compartilhamento de alertas e riscos entre organizações com controles de acesso;

1.10.6.3. Gerar permalink de um risco individual e acessá-lo com usuários de ambas as organizações, comprovando a preservação do mascaramento;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.10.6.4. Comprovar a criptografia dos dados em trânsito (TLS) e a declaração/evidência de criptografia em repouso;

1.10.6.5. Comprovar que a plataforma não acessa dados de negócio e não possui permissão de alteração nos ambientes monitorados.

Evidências obrigatórias: Comparativo das duas visões; permalink funcional com mascaramento; evidências de criptografia.

Critério de aceite: Mascaramento efetivo comprovado nas duas visões e no permalink, sem acesso a dados de negócio. Resultado registrado como ATENDE / NÃO ATENDE.

1.10.7. Métricas de pontualidade e desempenho de terceiros

Objetivo: Comprovar as métricas de gestão do desempenho de terceiros.

Pré-requisitos: Base de demonstração com histórico de riscos resolvidos.

Roteiro de execução:

1.10.7.1. Exibir a métrica de pontualidade calculada a partir do tempo médio de resposta de terceiros para resolução de vulnerabilidades, com base estatística e histórico;

1.10.7.2. Exibir a métrica de pontualidade aplicada a alertas e vulnerabilidades individuais (resposta dentro de período adequado ou não);

1.10.7.3. Gerar o relatório de desempenho de pontualidade de uma organização terceira: tempo médio de resolução, frequência de respostas pontuais e visualização histórica;

1.10.7.4. Exibir os dados históricos da porcentagem de riscos tratados por terceiro, isolada e agregada, ao longo do tempo.

Evidências obrigatórias: Painéis e relatórios de pontualidade e desempenho exibidos com dados.

Critério de aceite: Métricas calculadas automaticamente e relatórios por terceiro funcionais. Resultado registrado como ATENDE / NÃO ATENDE.

1.10.8. Integração TPRM / plataforma de dashboards



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Objetivo: Comprovar a integração da plataforma TPRM com a plataforma unificada de dashboards.

Pré-requisitos: Plataforma de dashboards do cenário S8.

Roteiro de execução:

1.10.8.1. Demonstrar os painéis de TPRM na mesma plataforma de dashboards do ecossistema SOC: postura de risco por terceiro, evolução histórica, riscos por severidade/disciplina/framework, pontualidade e ranking de terceiros;

1.10.8.2. Demonstrar a visão unificada de riscos (SOC + honeypots + terceiros) em painel executivo único;

1.10.8.3. Criar, ao vivo, visualização de TPRM solicitada pela comissão;

1.10.8.4. Demonstrar o acesso aos painéis pelos perfis executivo e técnico, em português do Brasil.

Evidências obrigatórias: Painéis TPRM na plataforma unificada; visão consolidada; visualização criada ao vivo.

Critério de aceite: Dados de TPRM integrados à mesma plataforma de dashboards do SOC, com visão unificada funcional. Resultado registrado como ATENDE / NÃO ATENDE.

1.10.9. API, automação, auditoria e exportações

Objetivo: Comprovar os itens de integração e governança da plataforma.

Pré-requisitos: Acesso à API e à documentação.

Roteiro de execução:

1.10.9.1. Apresentar a documentação pública/entregável da API REST e executar, ao vivo, chamadas de listagem e consulta de riscos (com autenticação);

1.10.9.2. Demonstrar a ferramenta de linha de comando (CLI) executando operação equivalente;

1.10.9.3. Apresentar o SDK em linguagem amplamente utilizada e executar exemplo funcional;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.10.9.4. Configurar e demonstrar notificação por e-mail e por webhook para novo achado relevante;

1.10.9.5. Exportar vulnerabilidades/riscos em CSV e JSON, inclusive em lote;

1.10.9.6. Exibir a trilha de auditoria das ações de usuários, com retenção mínima de 1 (um) ano (evidência de registros antigos na base de demonstração) e exportação em lote por intervalo de datas;

1.10.9.7. Exibir o histórico de alteração de um risco (mudanças de estado e recorrências);

1.10.9.8. Acessar a página pública de status/uptime da plataforma.

Evidências obrigatórias: Chamadas de API/CLI/SDK executadas; webhooks recebidos; arquivos CSV/JSON; trilha de auditoria; status page.

Critério de aceite: Automação completa (API, CLI, SDK), notificações, exportações e auditoria comprovadas ao vivo. Resultado registrado como ATENDE / NÃO ATENDE.

1.11. ROTEIRO OBRIGATÓRIO - ÁREA 4: OBSERVABILIDADE E MONITORAMENTO UNIFICADO (NOC)

1.11.1. Monitoramento de Ativos e Integrações Multiprotocolo

Objetivo: Demonstrar as capacidades de coleta de métricas técnicas e operacionais através de consultas a banco de dados, APIs, URLs e endpoints crítica, com arquitetura resiliente baseada em microsserviços.

Pré-requisitos: Ambiente de demonstração ativo e fontes (banco de dados, endpoints e APIs) configuradas.

Roteiro de execução:

1.11.1.1. Apresentar e validar a arquitetura da solução baseada em microsserviços, comprovando independência entre os componentes, escalabilidade e alta disponibilidade;

1.11.1.2. Demonstrar o monitoramento em tempo real de ativos de infraestrutura e de aplicações/serviços críticos da CONTRATANTE;

1.11.1.3. Realizar e validar a coleta de dados e métricas através de consultas diretas estruturadas em bancos de dados;



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.11.1.4. Demonstrar o monitoramento completo de endpoints, APIs REST e URLs, incluindo a validação em tempo real de certificados digitais e o acompanhamento de latência e tempos de resposta.

Evidências obrigatórias: Telas de consoles com métricas de infraestrutura ativas; logs de consultas validadas em banco de dados; relatórios de disponibilidade de APIs.

Critério de aceite: Ativos, endpoints e APIs monitorados em tempo real, com consultas a banco de dados validadas e ingestão via API REST funcional. Resultado registrado como ATENDE / NÃO ATENDE.

1.11.2. Dashboards Customizáveis, Alarmística e Gestão de SLA/SLO/SLI

Objetivo: Comprovar a flexibilidade de edição e criação de indicadores, visualização interativa com recursos de drill-down e parametrização de thresholds estáticos e dinâmicos de alertas inteligentes.

Pré-requisitos: Métricas dos cenários anteriores ativas e dados históricos fluindo.

Roteiro de execução:

1.11.2.1. Apresentar a plataforma de dashboards operacionais e executivos exibindo indicadores em tempo real, permitindo drill-down, filtros avançados e análise temporal detalhada;

1.11.2.2. Demonstrar, ao vivo, a criação, edição e customização de dashboards e indicadores de acordo com as necessidades operacionais;

1.11.2.3. Demonstrar a parametrização de thresholds estáticos e dinâmicos para geração inteligente de alarmes baseados em eventos;

1.11.2.4. Exibir a gestão integrada de Níveis de Serviço contemplando indicadores claros de SLA (Acordos de Nível de Serviço), SLO (Objetivos de desempenho) e SLI (Métricas de disponibilidade, latência, tempo de resposta, taxa de erro e consumo de recursos);

1.11.2.5. Demonstrar a visão executiva unificada contendo tendências de disponibilidade, ranking de serviços críticos, saúde geral do ambiente e indicadores de capacidade e crescimento.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Evidências obrigatórias: Dashboards operacionais e executivos exibidos; captura da edição e criação de indicadores executada ao vivo; disparo de alarmes baseados em thresholds dinâmicos.

Critério de aceite: Dashboards executivos e operacionais disponibilizados, com ferramentas de edição funcionais ao vivo e alarmística parametrizada respondendo a thresholds. Resultado registrado como ATENDE / NÃO ATENDE.

1.11.3. Automação Operacional e Orquestração baseada em Eventos

Objetivo: Comprovar o uso de ferramentas de orquestração integradas para execução de automações corretivas e preventivas com o intuito de reduzir o MTTR.

Pré-requisitos: Geração de incidentes e alarmes operacionais integrados à esteira de automação.

Roteiro de execução:

1.11.3.1. Apresentar a ferramenta de orquestração e demonstrar a execução remota de procedimentos técnicos padronizados a partir de gatilhos operacionais;

1.11.3.2. Simular uma falha (ex.: parada de serviço crítico) e evidenciar o disparo automatizado de scripts de remediação para o reinício automático do serviço sem intervenção manual;

1.11.3.3. Demonstrar a padronização operacional decorrente do processo e a redução mensurável do MTTR (Mean Time to Resolution) através dos logs do ciclo.

Evidências obrigatórias: Logs completos da esteira de automação evidenciando o evento gatilho, a execução do script e a restauração do serviço afetado.

Critério de aceite: Automação de execução remota de scripts e procedimentos corretivos com base em eventos demonstrada integralmente de forma funcional. Resultado registrado como ATENDE / NÃO ATENDE.

1.12. FORMULÁRIO DE AVALIAÇÃO E REGISTRO DE RESULTADOS

1.12.1. A comissão técnica registrará o resultado de cada cenário no formulário abaixo. Qualquer item avaliado como NÃO ATENDE implica reprovação da POC.

1.12.2. Área 1 - SOC



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Cenário	Título	Resultado (ATENDE / NÃO ATENDE)	Obs:
1.8.1	Arquitetura, código aberto e soberania de dados		
1.8.2	Coleta, normalização e busca de eventos		
1.8.3	Correlação, detecção e MITRE ATT&CK		
1.8.4	Integração SIEM/SOAR - automação e playbooks		
1.8.5	Notificações multicanal		
1.8.6	Plataforma de bloqueio automatizado integrada ao firewall		
1.8.7	Honeypot e cadeia		



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

	completa honeypot → SIEM → bloqueio		
1.8.8	Dashboards integrados e Inteligência Artificial		
1.8.9	Threat Intelligence		
1.8.10	Relatórios, SLA e housekeeping		

8.3. Área 2 - CSIRT

Cenário	Título	Resultado (ATENDE / NÃO ATENDE)	Observações
1.9.1	Portal ITSM, processos e matriz de priorização		
1.9.2	Resposta completa a incidente simulado		



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.9.3	Forense digital e cadeia de custódia		
1.9.4	Escalonamento , comunicação segura e coordenação externa		
1.9.5	Integração SOC ↔ CSIRT - linha do tempo única		

1.12.4. Área 3 - TPRM

Cenário	Título	Resultado (ATENDE / NÃO ATENDE)	Observações
1.10.1	Plataforma, soberania e controle de acesso		
1.10.2	Onboarding de terceiros - nuvem, SaaS e superfície externa		
1.10.3	Questionários de		



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

	autoavaliação e evidências		
1.10.4	Varreduras automatizadas e detecção de riscos		
1.10.5	Classificação, frameworks, ciclo de vida e acurácia		
1.10.6	Mascaramento de dados e compartilhamento entre organizações		
1.10.7	Métricas de pontualidade e desempenho de terceiros		
1.10.8	Integração TPRM / plataforma de dashboards		
1.10.9	API, automação, auditoria e exportações		

1.12.5. Área 4 - Observabilidade e Monitoramento Unificado (NOC)



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Cenário	Título	Resultado (ATENDE / NÃO ATENDE)	Observações
1.11.1	Monitoramento de Ativos e Integrações Multiprotocolo		
1.11.2	Dashboards Customizáveis, Alarmística e Gestão de SLA/SLO/SLI		
1.11.3	Automação Operacional e Orquestração baseada em Eventos		

1.12.6. Campos de encerramento: data e local da sessão; identificação e assinaturas dos membros da comissão técnica; identificação e assinaturas dos representantes da PROPONENTE; resultado final (APROVADA / REPROVADA).

1.13. AVALIAÇÃO DE CONFORMIDADE E CRITÉRIOS DE APROVAÇÃO

1.13.1. Ao final da POC, será gerado relatório com as observações da comissão técnica, registrando os resultados obtidos e a indicação de aprovação ou reprovação da solução ofertada.

1.13.2. Será considerada APROVADA a PROPONENTE cuja solução atenda a 100% (cem por cento) dos cenários do Roteiro Obrigatório (4.1 a 4.10, 5.1 a 5.5, 6.1 a 6.9 e 7.1 a 7.3), em todos os seus passos e critérios de aceite.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

1.13.3. Será REPROVADA e desclassificada imediatamente a PROPONENTE cuja solução:

- Apresente problemas insanáveis de funcionamento durante o período da análise técnica;
- Apresente divergência a menor em relação às especificações técnicas da proposta;
- Dependendo de componentes, integrações ou funcionalidades que violem os requisitos de código aberto/desenvolvimento próprio ou de residência de dados no Brasil;
- Utilize demonstrações pré-gravadas, simuladas ou não funcionais em substituição à execução ao vivo;
- Esteja desacompanhada, ao final, de declaração formal de que entregará a mesma solução apresentada na POC e na proposta.

1.13.4. No caso de aprovação, a PROPONENTE deverá apresentar declaração de que entregará a mesma solução apresentada na POC, que vinculará a execução contratual.

1.13.5. No caso de reprovação, serão indicadas as funcionalidades não atendidas ou não demonstradas, sendo convocada a próxima proponente classificada, sujeita aos mesmos requisitos.

1.13.6. A CONTRATANTE dará publicidade aos relatórios, pareceres ou laudos decorrentes da análise realizada, firmados pelos responsáveis, e assegurará às demais proponentes prazo razoável para o exercício do direito de eventual impugnação ao resultado.

1.13.7. Ao final, a PROPONENTE deverá entregar relatório consolidado com todos os itens realizados na Prova de Conceito, incluindo as evidências coletadas, ambiente de demonstração configurado, dashboards executivos e técnicos operacionais, indicadores monitorados ativos e recomendações detalhadas para evolução produtiva.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

ANEXO VIII
DECLARAÇÃO DE SUPERVENIÊNCIA

Ref.: Pregão Eletrônico nº ____/202__

Nome da Empresa _____ CNPJ nº _____ sediada
(endereço completo) _____ **declara**, sob as
penas da lei, que até a presente data inexistem fatos impeditivos para sua habilitação na presente
Concorrência, ciente da obrigatoriedade de declarar ocorrências posteriores.

Belém – PA, ____ de _____ de _____

Assinatura



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

ANEXO IX

DECLARAÇÃO DE MENOR

Ref.: Pregão Eletrônico nº ____/202__

_____, inscrita no CNPJ nº _____, sediada
(endereço completo) _____, por intermédio de seu representante
legal o (a) Sr. (a) _____ portador (a) da Carteira de Identidade nº
_____ e do CPF nº _____ DECLARA sob as penas da Lei, que não utiliza
mão de obra direta ou indireta de menores de 18 (dezoito) anos para a realização de trabalhos
noturnos, perigosos ou insalubres, bem como não utiliza, para qualquer trabalho, mão de obra direta
ou indireta de menores de 16 (dezesesseis) anos.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz (x)

Belém (PA), ____ de _____ de _____

Assinatura (declarante)



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

ANEXO X
MODELO DE ATESTADO DE VISITA TÉCNICA

Ref.: Pregão Eletrônico nº ____/202__

OBJETO:

ATESTAMOS, para os devidos fins, que a empresa _____(nome da empresa), representada neste ato por _____(nome do responsável pela visita), RG nº _____, realizou, nesta data, visita técnica em _____(local da visita), ficando ciente de todas as condições a serem consideradas na formulação da proposta comercial, referente ao Edital Pregão Eletrônico nº ____/202__.

Por ser verdade, firmamos o presente atestado.

Belém-Pa, ____ de _____ de 2026.

Nome completo e assinatura do Servidor

Matrícula do servidor



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

ANEXO XI DO TERMO DE REFERÊNCIA

ENDEREÇO DAS LOCALIDADES PARA INSTALAÇÃO DOS LINKS
BELÉM - SEDE DETRAN End.: Avenida Augusto Montenegro – Mangueirão, Belém/Pa CEP: 66640-000 Fone: (91) 3214-6235
PARQUE DE RETENÇÃO End.: Rua do Japonês, Bairro Bengui
POSTO PATIO BELÉM SHOPPING End. Rua Pe. Eutíquio 1078, bairro Batista Campos
POSTO SHOPPING PARQUE End.: Av. Augusto Montenegro, 4300- Parque Verde, Belém - PA,
POSTO SHOPPING BOULEVARD End.: Av. Visconde de Souza Franco, 776 - Reduto, Belém - PA,
POSTO SHOPPING METRÓPOLE End.: BR 316, 4,500, KM 04 - Coqueiro, Ananindeua- PA,
ESTAÇÃO CIDADANIA SÃO BRÁS End.: Av. Governador José Malcher, S/N- São Brás, Belém - PA,
ESTAÇÃO CIDADANIA ICOARACI End.: Av. Dr. Lopo de Castro, 78 - Cruzeiro, Belém - PA,
POSTO SHOPPING KARAJAS PARAUAPEBAS Rodovia Municipal Faruk Salmen, Km 07, 510 - Primavera, Parauapebas - PA, 68515-000
Estação Cidadania de Santarém do DETRAN Terminal Hidroviário Joaquim da Costa Pereira, na Rua Aragarina, s/n, bairro Prainha

CIRETRAN "A" DE ABAETETUBA

Gerente: José de Arimatéia Pureza de Oliveira/ Cel: (91) 99195-8583

Email: jose.pureza@detran.pa.gov.br

End: Trav. D. Pedro I, 2571 - São Lourenço CEP: 68.440-000

Fone: (91) 3751-4600 / 3751-1678

CIRETRAN "A" DE BRAGANÇA

Gerente: José Elielson Barros Oliveira / Cel: (91) 98093-8574

Email: oparahojeeli@gmail.com / jose.barros@detran.pa.gov.br

End: Avenida Polidório Coelho, s/n, Bairro: Taíra - CEP: 68.600-000

Fone: (91) 3425-1920 / 3244

CIRETRAN "A" DE BREVES

Gerente: Simone Eleotério Magalhães/ Cel: (91) 993709357

Email: valdenir.neves@detran.pa.gov.br



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Endereço: Rua Cap Assis, 285 – Centro CEP: 68.800-000
Fone: (91) 3783-1660 / 1546

CIRETRAN "A" DE CAPANEMA

Gerente: Jones Rosa da Silva / Cel: (91) 98185-9432
Email:
Endereço: Avenida João Paulo II, Lotes 01, 02 e 03 da Quadra 01 – N.Sª Aparecida
Fone: (91) 3462 -1339 / 3689 / 3193 (fax)

CIRETRAN "A" DE CASTANHAL

Gerente: Arley de Sousa Barleta / Cel: (91) 98729-1025
Email: @detran.pa.gov.br
End: Av. Barão do Rio Branco, 1287 – Bairro: Nova Olinda - CEP: 66.305-505 (**Ciretran nova**)
End: Av. Presidente Vargas, 1010 – Centro (**Ciretran Antiga**)
Fone/Fax: (91) 3721-7020 / 1997 / 3862

CIRETRAN "A" DE PARAGOMINAS

Gerente: Joaquim Telmo de Brito Pinon / Cel: (91) 99292-0015
Email: joaquim.pinom@detran.pa.gov.br
End: Av. Presidente Getúlio Vargas, S/N – CEP: 68.625-970
Fone/Fax: (91) 3729-3919 / 3790 (fax)

CIRETRAN "B" DE ANANINDEUA

Gerente: Franklin Gomes de Farias / Cel: (91) 98152-2298
Email: @detran.pa.gpv.br
End: Cidade Nova 4, SN 17, S/Nº CEP: 67.000-000
Fone: (91) 3263-2855

CIRETRAN "B" DE MARITUBA

End: Rua da Assembleia 477, Mirizal CEP: 67.000-000
Fone:

CIRETRAN "B" DE BARCARENA

Gerente: Rosângela Noriko Oda Dias / Cel: (91) 99147-4020
Email: rosangela.dias@detran.pa.gov.br
Endereço: Rua Magalhães Barata, S/Nº - Centro - CEP: 68.445-000
Fone: (91) 3753-1260 (fax)

CIRETRAN "B" DE CAMETÁ

Gerente: Adrielson Souza Pacheco / Cel: (91) 99338-1385
Email: Andrinhopacheco@gmail.com
End: Rua Inácio Moura, 1549 - S. Benedito – CEP: 68.400-000 (**Ciretran Antiga**)
End: Avenida Benjamin Constant, nº 285 (**Ciretran nova**)
Fone: (91) 3781- 1853 / 1719 (fax)

CIRETRAN "B" DE CAPITÃO POÇO

Gerente: Cleber Mesquita da Silva / Cel: (91) 98567-8887 / 98196-2011
Email: cleber.silva@detran.pa.gov.br
Endereço: Trav. José Barros da Silva, 844 – Centro – CEP: 68.650-000
Fone: (91) 3468- 1988 / 1144 (fax)



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

CIRETRAN "B" DE DOM ELISEU

Gerente: Tchella Vieira da Silva / Cel: (94) 98446-7728

Email: tchellavieira@outlook.com

End: Av. JK de Oliveira, 1021- Bairro: Redenção

Fone: (94) 3335-2116 / 1076 (fax)

CIRETRAN "B" DE IGARAPÉ AÇU

Gerente: Marcos Antonio de Souza Abdoral Lopes/ Cel: (91) 98497-5665

Email: @detran.pa.gov.br

End: Av. Barão do Rio Branco, S/N CEP: 68.725-000

Fone: (91) 3441-1302

CIRETRAN "B" DE IGARAPÉ MIRI

Gerente: Jonelson Pantoja da Silva / Cel: (91) 98561-2015

Email: jonelson.silva@detran.pa.gov.br

End: Rod. Gov. Moura Carvalho, S/N, CEP: 68.430-000

Fone: (91) *****

CIRETRAN "B" DE MAE DO RIO

Gerente: Gibran Rebelo Ribeiro / Cel: (91) 99390-6376

Email: andrassi.farias@detran.pa.gov.br

Endereço: Av. Marechal Rondon, 425 B – Centro – CEP: 68.675-00

Fone: (91) 3444-1383 / 2856

CIRETRAN "B" DE SALINÓPOLIS

Gerente: Vitoria Oliveira / Cel: (91) 9233-6877

Email: vitoria.correa@detran.pa.gov.br

End: Av. São Tomé, 480 – Bairro: Centro - CEP: 68.721-000 - **Ciretran**

Fone: (91) 3423-1080

CIRETRAN "B" DE SANTA IZABEL DO PARA

Gerente: Raiane Amorim de Queiroga / Cel: (91) 98280-0075

Email: raiane.queiroga@detran.pa.gov.br

Endereço: BR316 KM36 – Piçarra - Prox Ginásio de Esporte – CEP: 68.790-000

Fone: (91) 3744-1377 (fax) / 1553

CIRETRAN "B" DE SÃO MIGUEL DO GUAMÁ

Gerente: Zacarias de Souza Sotirakis / Cel: (91) 98209-2727

Email: zacarias.sotirakis@detran.pa.gov.br

Endereço: Rua Cipriano Mendes, 429 – São Manoel – CEP: 68.660-000

Fone: (91) 3446-2513 / 1283 / 1209 (fax)

CIRETRAN "B" DE SOURE

Gerente: Antônio Bianor de Sousa / Cel: (91) 99119-5501

Email: antonio.bianor@detran.pa.gov.br / bianorsouza@yahoo.com.br

Endereço: Rua Quarta, 10 – São Pedro, CEP: 68.870-000

Fone: (91) 3741-1371/ 1801 (fax)

CIRETRAN "B" DE TAILÂNDIA

Gerente: Francisco Eduardo Firmino da Silva / Cel: (91) 98188-7990 / 99233-6494

Email: francisco.firmino@detran.pa.gov.br / fco.eduardo2013@bol.com.br

Endereço: Av. Belém, 120 – Lt II – Qdr I – Centro – CEP: 68.695-000



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Fone: (91) 3752-1281

CIRETRAN "B" DE TOME-AÇU

Gerente: Oscar dos Santos Ferreira / Cel: (91) 99138-7039

Email: oscar.ferreira@detran.pa.gov.br

End: Av. Benigno Góes Filho, nº 828 – CEP: 68680-000 (Nova agência)

Fone: (91) 3727-1516 / 1631 / 1143 / 1080

CIRETRAN "B" DE VIGIA

Gerente: Luciana Nogueira Palheta / Cel: (91) 98852-8634/

Email: luciana.palheta@detran.pa.gov.br / luciana.palheta30@gmail.com

End: Av. Raimundo Melo Vasconcelos s/n – Sol Nascente - CEP: 68.780-000

Fone: (91) 3731-1214

CIRETRAN "A" DE MARABÁ

Gerente: Francisco Thoiamy Ferreira / cel: (94) 99654-1451

Email: francisco.cavalcante@detran.pa.gov.br

End: Folha 32 – Quadra 04 lotes 53/54 – CEP: 68.501-670

Fone/Fax: (94) 2103-9700 Regilene / 9701 Marcelo / 9702 Ivonete

CIRETRAN "A" DE PARAUAPEBAS

Gerente: Wellygton Pablo O. Dos Santos / Cel: (94) 98127-2314

Email: @detran.pa.gov.br

End: Rod. Faruk Salmen Km 06 – CEP: 68.515-000

Fone/Fax: (94) 3346-0111/ 6688 (fax)

CIRETRAN "A" DE REDENÇÃO

Gerente: Emerson Monsef / Cel: (94) 99144-0498

Email: ronnegley.barros@detran.pa.gov.br

End: Av. Min. Oscar Thompson Filho, 44. Entroncamento - CEP: 68.550-000

Fone: (94) 3424-2046 / 0896 / 2157 / 2150 (fax)

CIRETRAN "A" DE SAO FELIX DO XINGU

Gerente: Geane da Silva Dantas / Cel: (94) 984067307

Email: geane.dantas@detran.pa.gov.br

End: Avenida São Paulo, nº 955 -esquina c/ Independencia-Setor Alecrim

Fone/Fax: (94) 3435-1397

CIRETRAN "A" DE TUCURUI

Gerente: Iraneide de Fátima Cardoso da Silva / Cel: (94) 991632304

Email: iraneide.silva@detran.pa.gov.br / iraneidecardoso38@gmail.com

End: Av. Raimundo Veridiano Cardoso S/N - Bela Vista - Trevo da Cohab - CEP: 68.455-000

Fone/Fax: (94) 3787-1341 / 3787 -1915 / 3787 -2929 (fax)

CIRETRAN "B" DE CANAA DOS CARAJAS

Gerente: Luzlara / Cel: (94) 99212-0222

Email: @Detran.gov.br

End: Rua do Ouro, S/N – Bairro: Jardim das Palmeiras – CEP: 68.537-000

Fone/Fax: (94) 3358-1386

CIRETRAN "B" DE CONCEIÇÃO DO ARAGUAIA



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

Gerente: Tamires da Silva Ferreira/ Cel: (94) 99151-5580
Email: tamires.ferreira@detran.pa.gov.br
End: Av. Rio Araguaia, Quadra 349, Lote 1 - Bairro: Vila Cruzeiro – CEP: 68.540-000
Fone: (94) 3421-1828 / 1715 (fax)

CIRETRAN "B" DE CURIONOPOLIS
Gerente: Lucivaldo Araujo de Souza / Cel: (94) 99117-1903
Email: lucivaldo.souza@detran.pa.gov.br
End: Av. Maranhão, 151-Bairro: Da paz – CEP: 68.522-000
Fone/Fax: (94) 3348-1394

CIRETRAN "B" DE ELDORADO DOS CARAJAS
Gerente: DÉCIO CAMPOS DE ARAÚJO / Cel: (94) 98811-3319
Email: decio.araujo@detran.pa.gov.br
End: Rua Rio Vermelho nº 13, km 100 – Centro – CEP: 68.524-000
Fone/Fax: *****

CIRETRAN "B" DE ITUPIRANGA
Gerente: Flávio Anísio Gonçalves Borges / Cel: (94) 99180-5877
Email: flavio.borges@detran.pa.gov.br / flavio.anisio@hotmail.com
End: Av. 14 de julho, 15 – Centro – CEP: 68.580-000
Fone/Fax: (94) 3333-1670 / 1128 / 1765

CIRETRAN "B" DE JACUNDA
Gerente: Cleane Mota Ungaratti / Cel: (94) 9166-2850
Email:
End: Rua José Soares, 158 – CEP: 68.590-000
Fone: (94) 3345-1400

CIRETRAN "B" DE NOVO REPARTIMENTO
Gerente: Rodrigo Silva / Cel: (94) 99280-0229
Email: @detran.pa.gov.br
Endereço: Trav. Rio Jordão, S/N, Praça da Bíblia, Parque Espigão
Fone/Fax: *****

CIRETRAN "B" DE OURILANDIA DO NORTE
Gerente: Cleydson Silva Sousa / Cel: (94) 99181-4732
Email: cleydson.silva@detran.pa.gov.br
Endereço: Av. das Nações nº 3298 – Bairro: Novo Horizonte – CEP: 68.390.000
Fone/Fax: (94) 3434-1271

CIRETRAN "B" DE RONDON DO PARA
Gerente: Erasmo Carias Pereira / Cel: (94) 99194-4204
Email: natallia.anjos@detran.pa.gov.br
End: Rua Rio Grande do Sul, 465 – Centro - CEP: 68.638-000.
Fone: (94) 3326-1038 (fax)

CIRETRAN "B" DE SANTANA DO ARAGUAIA
Gerente: Hevanuir Martins da Silva / Cel: (63) 98431-9909
Email:
End: Av. Manoel Venuzan, S/N Bairro: Bíblia – CEP: 68.560-000
Fone/Fax: (94) 3431-2995



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

CIRETRAN "B" DE SAO GERALDO DO ARAGUAIA

Gerente: Venicio Santos Costa/ Cel: (94) 99226-6788

Email: venicio.costa@detran.pa.gov.br

End: Av. Castelo Branco s/n – Centro - CEP: 68.570-000

Fone: (94) 3331-1300 / 3331 -1565 / 3331 -1122(fax)

CIRETRAN "B" DE TUCUMA

Gerente: Juliana Pelegrini de Castro / Cel: (94) 99175-7500

Email: juliana.castro@detran.pa.gov.br / jupelegrini_8@hotmail.com

End: Rua dos Tucanos, 68 – Centro, CEP: 68.385-000

Fone: (94) 3433-1818

CIRETRAN "B" DE XINGUARA

Gerente: Ricardo moreira de Oliveira / Cel: (94) 98420-9462

Email: @detran.pa.gov.br

End: Av. Xingu, 733, esquina com a Rua Guriatã, Bairro: Centro – CEP: 68.555-000

Fone/Fax: (94) 3426-2020 / 2021 / 1802

CIRETRAN "A" DE ALTAMIRA

Gerente: Raphael Caroso Pinheiro / Cel:(93) 99218-9730

Email: @detran.pa.gov.br

End: Trav. Duque de Caxias, 370 - Jd do Sol– CEP: 68.371-010

Fone/Fax: (93) 3515-0796 / 1099 / 2448 (fax)

CIRETRAN "A" DE ITAITUBA

Gerente: ZEDEQUIAS CARLOS DE MELO / Cel: 93 99123-3735

Email: @detran.pa.gov.br

End: Trav. 15 de agosto, 251 – CEP: 68.180-610

Fone/Fax: (93) 3518-1460 / 2119 / 1678 (fax)

CIRETRAN "A" DE SANTARÉM

Gerente: Edney Martins Pimentel / Cel: (93) 9111-2006

Email: wfreirew@gmail.com

End: Av. Cuiabá, 890 - Liberdade - CEP: 68.040-400

Fone/Fax: (93) 3522-2401 / 9607 / 9610 (fax) gerente 3523- 4877

CIRETRAN "B" DE ALENQUER

Gerente: Juscelino Pontes Figueiras / Cel: (93) 99100-4263

Email:

End: Trav. Colombiano Marvão, S/N – Planalto – CEP: 68.200-000

Fone: (93) 3265-1030

CIRETRAN "B" DE ALMEIRIM / M. DOURADO

Gerente: Antonio Francisco de Souza Jambo / Cel: (91) 99154-3511

Email: antonio.jambo@detran.gov.pa.br

End: Rua K, S/N ao lado do escritório da Jari - Industrial - CEP: 68.240-000

Fone: (93) 3735-2068 /1388 (fax)

CIRETRAN "B" DE MEDICILANDIA

Gerente: Gislaine Teles Avelino Nadler/ Cel: (93) 99146-3969

Email: gislaine.avelino@detran.pa.gov.br /



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

End: Rua Doze de Maio, 53 Centro – CEP: 68.145-000
Fone/Fax: (93) 3531-1544

CIRETRAN "B" DE MONTE ALEGRE

Gerente: PAULO ROBERTO VASCONCELOS DA SILVA fone (93) 99122-1429
Email: l@detran.pa.gov.br
End: Trav. Major Mariano, 418 - Cidade Alta - CEP: 68.220-000
Fone: (93) 3533-2926 / 1660 (fax)

CIRETRAN "B" DE NOVO PROGRESSO

Gerente: Edemar Onetta / Cel: (93) 981213097
Email: edemar.onetta@detran.pa.gov.br
End: Av. Isaias Pinheiro s/n – Lt 16- Qd 133- Bela Vista CEP, 68.193-000
Fone/Fax: (93) 3528-0177 / 0188 (fax)

CIRETRAN "B" DE OBIDOS

Gerente: Romulo Ferreira de Andrade / Cel: (93) 99204-5739
Email: romulo.andrade@detran.pa.gov.br / saofrancisco.romulo@gmail.com
End: Trav. Lauro Sodré, 482 – Bairro: Lourdes, CEP: 68.250-000
Fone: (93) 3547-2580 / 1707 / 2380 (fax)

CIRETRAN "B" DE ORIXIMINÁ

Gerente: Jean Rudstedt Gato Barros / Cel: (93) 99141-5160
Email: jean@detran.pa.gov.br
End: R. Barão do Rio Branco, 2848- Santa Terezinha CEP: 68.270-000
Fone: (93) 3544-2539 / 1170 (fax)

CIRETRAN "B" DE URUARA

Gerente: Jaden Sousa Rocha / Cel: (93) 99125-6096
Email: @detran.pa.gov.br /
End: R. Adilson Lopes, 48 – Quadra 15, Lote 17 – Santo Antonio
Fone/Fax: (93) 3532-2303 / 2004 (fax)

CIRETRAN "B" DE RUROPOLIS

Gerente: André Luis Sousa Silva / Cel: (93) 99110-8882
Email: André.luiz@detran.pa.gov.br
End: Av. Haroldo Veloso com Av. Isaias Buaz, S/N, Rurópolis/PA CEP: 68.165-000
Fone/Fax:



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

ANEXO XII

DECLARAÇÃO PARA MICROEMPRESA E EMPRESA DE PEQUENO PORTE

Ref.: Pregão Eletrônico nº ____/202__

(nome da empresa), inscrita no CNPJ nº _____, por intermédio de seu representante legal o(a) Sr(a) _____, portador(a) da Carteira de Identidade nº _____ e do CPF nº _____, DECLARA, para fins do disposto no Edital do Pregão Eletrônico SRP nº ____/202__, sob as sanções administrativas cabíveis e sob as penas da lei, ser microempresa ou empresa de pequeno porte nos termos da legislação vigente, não possuindo nenhum dos impedimentos previstos no §4º do artigo 3º da Lei Complementar nº 123/2006.

Belém, ____ de _____ de 2026.

(representante legal)



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ

ANEXO XIII DO TERMO DE REFERÊNCIA
DECLARAÇÃO DE COTA DE PESSOAS COM DEFICIÊNCIA NO
QUADRO DE EMPREGADOS

Ref.: Pregão Eletrônico nº ____/202__

(nome da empresa), inscrita no CNPJ nº _____, por
intermédio de seu representante legal o(a)
Sr(a) _____, portador(a) da Carteira de
Identidade nº _____ e do CPF nº _____,
DECLARA, para fins do disposto no Edital do Pregão Eletrônico SRP nº ____/202__, que
possui em seu quadro de empregados um percentual mínimo de 5% (cinco por cento)
de pessoas com deficiência.

Belém, _____ de _____ de 2026.

(representante legal)



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

ANEXO XIV

ATA DE REGISTRO DE PREÇOS Nº 00/2026 – DETRAN/PA

**ATA DE REGISTRO DE PREÇOS RELATIVA AO PREGÃO ELETRÔNICO SRP Nº 90005/2025 -
DETRAN-PA**

O DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ – DETRAN/PA, com sede na Avenida Augusto Montenegro, km 03, s/nº, Mangueirão, Belém, Pará, inscrito no CNPJ/MF sob o nº 04.822.060/0001-40, neste ato representada pela sua Diretora Geral Sra. RENATA MIRELLA FREITAS GUIMARÃES DE SOUZA COELHO, brasileira, CPF/MF nº xxxxxxxx, considerando o julgamento da licitação na modalidade PREGÃO ELETRÔNICO, para REGISTRO DE PREÇOS, Nº 90005/2025, processo administrativo nº 2024/229253, RESOLVE registrar os preços da empresa indicada e qualificada nesta ATA, de acordo com a classificação por ela alcançada e na quantidade cotada, atendendo as condições previstas no edital de licitação, sujeitando-se as partes às normas constantes na Lei Federal nº 14.133/2021, Lei Complementar Federal nº 123/2006, Lei de Diretrizes Orçamentárias vigente, Lei Estadual nº 8.417/2016, Instrução Normativa SEGES/MP nº 05/2017, Instrução Normativa SEGES/MP nº 03/2018; Decretos Estaduais nº 2.939/2023, nº 2.940/2023 e nº 3.371/2023, e em conformidade com as disposições a seguir:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. A presente Ata tem por objeto o registro de preços para a eventual contratação de empresa especializada na prestação de serviços de telecomunicações e transmissão de dados, através de uma rede de comunicação digital, determinística, privativa e independente, com locação de roteadores (Solução UTM/NGFW), no-breaks, switches e firewall, cuja finalidade é a interligação corporativa das redes locais (LAN) das unidades do Departamento de Trânsito do Estado do Pará (CIRETRANS e Postos de Atendimento) e acesso IP (Internet Protocol) a rede mundial de internet centralizada na sede do DETRAN/PA, prestação de serviço de transmissão de dados, voz e imagem via satélite, através de solução portátil, móvel com locação de equipamentos e o fornecimento de toda infraestrutura necessária para a solução móvel de fiscalização, incluindo equipamentos, veículos e logística, cujas especificações se encontram detalhadas no Termo de Referência, anexo do edital de licitação referente ao Pregão Eletrônico SRP nº 90005/2025, que é parte integrante desta Ata, assim como as propostas cujos preços tenham sido registrados, independentemente de transcrição.

CLÁUSULA SEGUNDA - DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. O preço registrado, as especificações do objeto, as quantidades mínimas e máximas de cada item, fornecedor(es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

FORNECEDOR: razão social, CNPJ nº, endereço, telefone, nome do representante.

Lote	Item	Descrição	Und	Qtd.	Valor Unitário Estimado Mensal	Valor Total 24 meses
I	1	Solução de Telecomunicação Intranet	Und	01	R\$	R\$
	2	Solução de Telecomunicação – Sub Redes – Sob Demanda	Und	01	R\$	R\$
	3	Solução de Telecomunicação UPGRADE de 100% de Link de Intranet/Internet a partir do 13º Mês – Sob Demanda	Und	01	R\$	R\$
	4	Solução de Telecomunicação – Link de Internet	Und	01	R\$	R\$



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

	Determinístico – DETRAN/PA – Sede				
5	Solução de Telecomunicação Portátil para Acesso Via Satélite	Und	01	R\$	R\$
6	Tabela de Valores de Consumo da Solução de Telecomunicação Portátil e Veicular para Acesso Via Satélite	Und	01	R\$	R\$
7	Composição de Preço para Solução de Telecomunicação Móvel de Fiscalização	Und	01	R\$	R\$
8	Composição de Preço de Instalação e Configuração de Todos os Equipamentos nas Localidades	Und	01	R\$	R\$
9	Composição de Preço para Instalação da Base de Infraestrutura para Solução de Telecomunicação Móvel de Fiscalização	Und	01	R\$	R\$
10	Composição de Preço para Serviços de segurança da informação para a Rede de Telecomunicações nas CIRETRANS, POSTOS AVANÇADOS E POSTOS DE FISCALIZAÇÃO	Und	01	R\$	R\$
11	Composição de Preço para Serviços de segurança da informação para a Rede de Telecomunicações para o DETRAN SEDE	Und	01	R\$	R\$
12	Composição de Preço para implantação de Serviços de Gestão da Segurança da Informação para a Rede de Telecomunicações	Und	01	R\$	R\$
VALOR GLOBAL ESTIMADO				R\$	

2.2. Valor Total Mensal: R\$ 00,00 (valor por extenso).

2.3. Valor Total Anual: R\$ 00,00 (valor por extenso).

CLÁUSULA TERCEIRA – DO ÓRGÃO GERENCIADOR E PARTICIPANTES

3.1. O órgão gerenciador será o DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ – DETRAN/PA.

CLÁUSULA QUARTA - DA ADESAO À ATA DE REGISTRO DE PREÇOS

4.1. Durante a vigência da ata, os órgãos e as entidades da Administração Pública federal, estadual, distrital e municipal, que não participaram do procedimento de IRP, poderão aderir à ata de registro de preços na condição de não participantes, observados os seguintes requisitos:

4.1.1. apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

4.1.2. demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei nº 14.133, de 2021; e

4.1.3. consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.

4.2. A autorização do órgão ou entidade gerenciadora apenas será realizada após a aceitação da adesão pelo fornecedor.

4.2.1. Caberá à entidade gerenciadora, após a aceitação da adesão pelo fornecedor, analisar a viabilidade da aceitação do requerimento de adesão do órgão ou entidade não participante, observados os limites



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

estabelecidos no artigo 32 do Decreto nº 3.371, de 29 de setembro de 2023.

4.2.2. O órgão ou entidade gerenciadora poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.

4.3. Após a autorização do órgão ou da entidade gerenciadora, o órgão ou entidade não participante deverá efetivar a aquisição ou a contratação solicitada em até noventa dias, observado o prazo de vigência da ata.

4.4. O prazo de que trata o subitem anterior, relativo à efetivação da contratação, poderá ser prorrogado excepcionalmente, mediante solicitação do órgão ou da entidade não participante aceita pelo órgão ou pela entidade gerenciadora, desde que respeitado o limite temporal de vigência da ata de registro de preços.

4.5. O órgão ou a entidade poderá aderir a item da ata de registro de preços da qual seja integrante, na qualidade de não participante, para aqueles itens para os quais não tenha quantitativo registrado, observados os requisitos do item 4.1.

Dos limites para as adesões

4.6. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o gerenciador e para os participantes.

4.7. O quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o gerenciador e os participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.

Da vedação a acréscimo de quantitativos

4.8. É vedado efetuar acréscimos nos quantitativos fixados na Ata de Registro de Preços.

CLAÚSULA QUINTA - DA VALIDADE, FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

5.1. A validade da Ata de Registro de Preços será de 1 (um) ano, contado a partir do primeiro dia útil subsequente à data de divulgação no Diário Oficial do Estado do Pará, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

5.1.1. O contrato decorrente da Ata de Registro de Preços terá sua vigência estabelecida no próprio instrumento contratual e observará no momento da contratação e a cada exercício financeiro a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro.

5.1.2. No caso de prorrogação da presente Ata, os preços registrados serão reajustados pelo ÍNDICE DE PREÇOS AO CONSUMIDOR AMPLO - IPCA.

5.1.3. Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

5.2. A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de instrumento contratual, conforme rege o art. 95 da Lei nº 14.133, de 2021.

5.2.1. O instrumento contratual de que trata o item 5.2 deverá ser assinado no prazo de validade da ata de registro de preços.

5.3. Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133, de 2021.

5.4. Após a homologação da licitação ou da contratação direta, deverão ser observadas as seguintes condições para formalização da ata de registro de preços:

5.4.1. Serão registrados na ata os preços e os quantitativos do adjudicatário, devendo ser observada a possibilidade de o licitante oferecer ou não proposta em quantitativo inferior ao máximo previsto no edital e se obrigar nos limites dela;

5.4.2. Será incluído na ata, na forma de anexo, o registro dos licitantes ou dos fornecedores que:

5.4.2.1. Aceitarem cotar os bens, as obras ou os serviços com preços iguais aos do adjudicatário, observada a



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

classificação da licitação; e

5.4.2.2. Mantiverem sua proposta original.

5.4.3. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou dos fornecedores registrados na ata.

5.5. O registro a que se refere o item 5.4.2 tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.

5.6. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.

5.7. A habilitação dos licitantes que comporão o cadastro de reserva a que se refere o item 5.4.2.2 somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

5.7.1. Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos *no edital*; e

5.7.2. Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas na Cláusula Nona.

5.8. O preço registrado com indicação dos licitantes e fornecedores será divulgado no PNCP e ficará disponibilizado durante a vigência da ata de registro de preços.

5.9. Após a homologação da licitação ou da contratação direta, o licitante mais bem classificado ou o fornecedor, no caso da contratação direta, será convocado para assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital de licitação ou no aviso de contratação direta, sob pena de decair o direito, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

5.9.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante ou fornecedor convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela Administração.

5.10. A Ata de Registro de Preços será assinada por meio de assinatura digital e disponibilizada no sítio eletrônico www.compraspara.pa.gov.br e no Portal Nacional de Contratações Públicas (PNCP).

5.11. Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital ou no aviso de contratação, e observado o disposto no item 5.7 e subitens, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

5.12. Na hipótese de nenhum dos licitantes que trata o item 5.4.2.1, aceitar a contratação nos termos do item anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

5.12.1. Convocar para negociação os demais licitantes ou fornecedores remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

5.12.1. Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

5.13. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

CLÁUSULA SEXTA - DA ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

6.1. Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

6.1.1. Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

da alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

6.1.2. Em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

6.1.3. Na hipótese de previsão no edital ou no aviso de contratação direta de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos da Lei nº 14.133, de 2021.

CLÁUSULA SÉTIMA - DA NEGOCIAÇÃO DE PREÇOS REGISTRADOS

7.1. Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado.

7.1.1. Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas.

7.1.2. Na hipótese prevista no item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado e não convocará os licitantes ou fornecedores que tiveram seu registro cancelado.

7.1.3. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciador(a) convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado.

7.1.4. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, adotando as medidas cabíveis para obtenção de contratação mais vantajosa.

7.1.5. Na hipótese de redução do preço registrado, o gerenciador comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços para que avaliem a conveniência e a oportunidade de diligenciar negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

7.2. Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.

7.2.1. Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou a planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.

7.2.2. Na hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão ou entidade gerenciadora e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

7.2.3. Na hipótese de cancelamento do registro do fornecedor, nos termos do item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados.

7.2.4. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, nos termos do item 9.1, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.

7.2.5. Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto nos itens 7.1.1 e 7.2, o órgão ou entidade gerenciadora atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

7.2.6. O órgão ou entidade gerenciadora comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços sobre a efetiva alteração do preço registrado, para que avaliem a



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

necessidade de alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

CLÁUSULA OITAVA - DO REMANEJAMENTO DAS QUANTIDADES REGISTRADAS NA ATA DE REGISTRO DE PREÇOS

8.1. As quantidades previstas para os itens com preços registrados nas atas de registro de preços poderão ser remanejadas pelo órgão ou entidade gerenciadora entre os órgãos ou as entidades participantes e não participantes do registro de preços.

8.2. O remanejamento somente poderá ser feito:

8.2.1. De órgão ou entidade participante para órgão ou entidade participante; ou

8.2.2. De órgão ou entidade participante para órgão ou entidade não participante.

8.3. O órgão ou entidade gerenciadora que tiver estimado as quantidades que pretende contratar será considerado participante para efeito do remanejamento.

8.4. Na hipótese de remanejamento de órgão ou entidade participante para órgão ou entidade não participante, serão observados os limites previstos no art. 32 do Decreto nº 3.371, de 2023.

8.5. Competirá ao órgão ou à entidade gerenciadora autorizar o remanejamento solicitado, com a redução do quantitativo inicialmente informado pelo órgão ou pela entidade participante, desde que haja prévia anuência do órgão ou da entidade que sofrer redução dos quantitativos informados.

8.6. Caso o remanejamento seja feito entre órgãos ou entidades dos Estados, do Distrito Federal ou de Municípios distintos, caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente do remanejamento dos itens.

8.7. Compete ao órgão ou entidade requerente do remanejamento obter a anuência o órgão ou entidade cedente e informar ao órgão ou entidade gerenciadora a transferência do quantitativo remanejado para que este promova a análise de viabilidade e o controle e o gerenciamento da Ata.

CLÁUSULA NONA - DO CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS

9.1. O registro do fornecedor será cancelado pelo gerenciador, quando o fornecedor:

9.1.1. Descumprir as condições da ata de registro de preços, sem motivo justificado;

9.1.2. Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;

9.1.3. Não aceitar manter seu preço registrado; ou

9.1.4. Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021.

9.1.4.1. Na hipótese de aplicação de sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021, caso a penalidade aplicada ao fornecedor não ultrapasse o prazo de vigência da ata de registro de preços, poderá o órgão ou a entidade gerenciadora poderá, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

9.2. O cancelamento de registros nas hipóteses previstas no item 9.1 será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos os princípios do contraditório e da ampla defesa.

9.3. Na hipótese de cancelamento do registro do fornecedor, o órgão ou a entidade gerenciadora poderá convocar os licitantes que compõem o cadastro de reserva, observada a ordem de classificação.

9.4. O cancelamento dos preços registrados poderá ser realizado pelo gerenciador, em determinada ata de registro de preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:

9.4.1. Por razão de interesse público;

9.4.2. A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

9.4.3. Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado tornar-se superior ou inferior ao preço registrado, nos termos do artigo 22 do Decreto Estadual nº 3371/2023.

CLÁUSULA DÉCIMA - DAS PENALIDADES

10.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no edital.

10.1.1. As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente após terem assinado a ata.

10.2. É da competência do gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço (art. 6º, inc. X, do Decreto Estadual nº 3371/2023), exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos ou entidade participante, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 7º, inc. VI, do Decreto Estadual nº 3371/2023).

10.3. O órgão ou entidade participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no item 9.1, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

CLÁUSULA DÉCIMA PRIMEIRA - DAS CONDIÇÕES GERAIS

11.1. As condições gerais de execução do objeto, tais como os prazos para entrega e recebimento, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, anexo ao edital.

11.2. No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação de parte de itens do grupo se houver prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade.

CLÁUSULA DÉCIMA SEGUNDA – DO FORO

12.1. Fica eleito o Foro da cidade de Belém, Capital do Estado do Pará, com renúncia a qualquer outro, por mais privilegiado que seja, para dirimir as questões que porventura surgirem na execução da presente Ata de Registro de Preços.

Belém/PA, _____ de _____ de 2026.

RENATA MIRELLA FREITAS GUIMARÃES DE SOUSA COELHO
Diretora Geral
DETRAN/PA

Adjudicatária/Proponente



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

ANEXO XV

CONTRATO Nº 00/2026 – DETRAN/PA
PAE nº E-2025/2089963

RESUMO

CONTRATANTE

Departamento de Trânsito do Estado do Pará
CNPJ nº 04.822.060/0001-40

CONTRATADO

CNPJ nº

OBJETO

Contratação de empresa especializada na prestação de serviços de telecomunicações e transmissão de dados, através de uma rede de comunicação digital, determinística, privativa e independente, com locação de roteadores (Solução UTM/NGFW), no-breaks, switches e firewall, cuja finalidade é a interligação corporativa das redes locais (LAN) das unidades do Departamento de Trânsito do Estado do Pará (CIRETRANS e Postos de Atendimento) e acesso IP (Internet Protocol) a rede mundial de internet centralizada na sede do DETRAN/PA, prestação de serviço de transmissão de dados, voz e imagem via satélite, através de solução portátil, móvel com locação de equipamentos e o fornecimento de toda infraestrutura necessária para a solução móvel de fiscalização, incluindo equipamentos, veículos e logística, cujas especificações se encontram detalhadas no Termo de Referência e seus anexos.

VALOR TOTAL

R\$

REAJUSTE

Índice: IPCA

Período: a cada 12 (doze) meses, a contar de dd/mm/aaaa.

PAGAMENTO

Forma: Ordem Bancária

Prazo: até 30 (trinta) dias corridos, a contar do recebimento da Nota Fiscal ou fatura, atestada pelo fiscal do Contrato.

FISCALIZAÇÃO

O fiscal do Contrato é o servidor (nome do servidor), CPF nº 000.000.000-00, matrícula nº 00000, lotado no (setor).

VIGÊNCIA

Prazo: 24 (vinte e quatro) meses, prorrogável na forma do artigo 107 da Lei Federal nº 14.133/2021.

Início: dd/mm/aaaa

Fim: dd/mm/aaaa



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

CLÁUSULA PRIMEIRA – DAS PARTES

CONTRATANTE: O DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ - DETRAN/PA, CNPJ nº 04.822.060/0001- 40, Autarquia Estadual, com sede à Avenida Augusto Montenegro, Km 03, s/nº, neste ato representado por sua Diretora Geral Renata Mirella Freitas Guimarães de Sousa Coelho, brasileira, _____, CI/RG nº 0000-SEGUP/PA e CPF/MF nº 000,

CONTRATADO: (nome da empresa), inscrita no CNPJ/MF, sob o nº _____ estabelecida nesta cidade à _____, bairro de _____, neste ato representada por _____, brasileiro(a), portador da CI/RG nº _____ e do CPF/MF nº _____, com domicílio na _____.

CLÁUSULA SEGUNDA - DA FUNDAMENTAÇÃO LEGAL

2.1. O presente Contrato é oriundo do **Pregão Eletrônico SRP nº 90005/2025**, constante no PAE nº 2024/2528582 e é regido pela Lei Federal nº 14.133/2021, Lei Complementar Federal nº 123/2006, Lei de Diretrizes Orçamentárias vigente, Lei Estadual nº 8.417/2016, Instrução Normativa SEGES/MP nº 05/2017, Instrução Normativa SEGES/MP nº 03/2018; Decretos Estaduais nº 2.939/2023, nº 2.940/2023, nº 3.371/2023 e nº 3.813/2024.

CLÁUSULA TERCEIRA - DO OBJETO

3.1. O objeto do certame é a contratação de empresa especializada na prestação de serviços de telecomunicações e transmissão de dados, através de uma rede de comunicação digital, determinística, privativa e independente, com locação de roteadores (Solução UTM/NGFW), no-breaks, switches e firewall, cuja finalidade é a interligação corporativa das redes locais (LAN) das unidades do Departamento de Trânsito do Estado do Pará (CIRETRANS e Postos de Atendimento) e acesso IP (Internet Protocol) a rede mundial de internet centralizada na sede do DETRAN/PA, prestação de serviço de transmissão de dados, voz e imagem via satélite, através de solução portátil, móvel com locação de equipamentos e o fornecimento de toda infraestrutura necessária para a solução móvel de fiscalização, incluindo equipamentos, veículos e logística, cujas especificações se encontram detalhadas no Termo de Referência, o qual **ADERE** a este documento para todos os fins.

3.2. Este instrumento se vincula ao edital licitatório citado na Cláusula 2, à proposta do licitante vencedor, e aos anexos desses documentos.

3.3. Os serviços contratados são os seguintes itens descritos no Termo de Referência:

Lote	Item	Descrição	Und	Qtd.	Valor Unitário Estimado Mensal	Valor Total 24 meses
I	1	Solução de Telecomunicação Intranet	Und	01	R\$	R\$
	2	Solução de Telecomunicação – Sub Redes – Sob Demanda	Und	01	R\$	R\$
	3	Solução de Telecomunicação UPGRADE de 100% de Link de Intranet/Internet a partir do 13º Mês – Sob Demanda	Und	01	R\$	R\$
	4	Solução de Telecomunicação – Link de Internet Determinístico – DETRAN/PA – Sede	Und	01	R\$	R\$
	5	Solução de Telecomunicação Portátil para Acesso Via Satélite	Und	01	R\$	R\$
	6	Tabela de Valores de Consumo da Solução de Telecomunicação Portátil e Veicular para Acesso Via Satélite	Und	01	R\$	R\$



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

7	Composição de Preço para Solução de Telecomunicação Móvel de Fiscalização	Und	01	R\$	R\$
8	Composição de Preço de Instalação e Configuração de Todos os Equipamentos nas Localidades	Und	01	R\$	R\$
9	Composição de Preço para Instalação da Base de Infraestrutura para Solução de Telecomunicação Móvel de Fiscalização	Und	01	R\$	R\$
10	Composição de Preço para Serviços de segurança da informação para a Rede de Telecomunicações nas CIRETRANS, POSTOS AVANÇADOS E POSTOS DE FISCALIZAÇÃO	Und	01	R\$	R\$
11	Composição de Preço para Serviços de segurança da informação para a Rede de Telecomunicações para o DETRAN SEDE	Und	01	R\$	R\$
12	Composição de Preço para implantação de Serviços de Gestão da Segurança da Informação para a Rede de Telecomunicações	Und	01	R\$	R\$

2.2. Valor Total Mensal: R\$ 00,00 (valor por extenso).

2.3. Valor Total Anual: R\$ 00,00 (valor por extenso).

2.4. Valor Total por 24 (vinte e quatro) meses: R\$ 00,00 (valor por extenso).

CLÁUSULA QUARTA - DO LOCAL E HORA DA PRESTAÇÃO DO SERVIÇO

4.1. O local e a hora da prestação dos serviços contratados são aqueles previstos no Termo de Referência e seus Anexos.

CLÁUSULA QUINTA - DO MODELO DE EXECUÇÃO E GESTÃO DOS SERVIÇOS

5.1. O regime de execução contratual, o modelo de gestão, assim como os prazos e condições de conclusão, entrega, observação e recebimento definitivo constam no Termo de Referência, anexo a este Contrato.

CLÁUSULA SEXTA – DO PREÇO

6.1. O valor global estimado mensal do Contrato é **R\$ xxx.xxx,xx** (extenso) e todas as despesas ordinárias diretas e indiretas decorrentes de sua execução estão *inclusas* neste preço, como tributos, encargos sociais, trabalhistas, previdenciários, comerciais, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do Contrato.

CLÁUSULA SÉTIMA – DA DOTAÇÃO ORÇAMENTÁRIA

7.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria do orçamento do Estado do Pará, para o exercício de 2026, na classificação abaixo:

66.201 – Departamento de Trânsito do Estado do Pará;		
Função	06	Segurança Pública
Subfunção	126	Tecnologia da Informação
Programa	1510	Segurança Pública
Projeto Atividade	2346	Implementação de Soluções em Tecnologia da Informação e Comunicação



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

Elemento de Despesa	339040 449052 (12/33/42/46/34)	Serviços Técnicos da Informação Pessoa Jurídica Equipamentos e Material Permanente
Fonte de Recursos	01752000061 02752000061	Recursos Próprios Recursos Próprios - Superavit

CLÁUSULA OITAVA – DO REAJUSTE

- 8.1. O contrato será reajustado pelo ÍNDICE DE PREÇOS AO CONSUMIDOR AMPLO - IPCA.
- 8.2. É devido reajuste contratual apenas a cada 12 (doze) meses, a contar da data do orçamento estimado.
- 8.3. O reajuste se restringirá ao valor do saldo contratual existente na data em que aquele for devido.
- 8.4. O reajuste será realizado de ofício pelo CONTRATANTE mediante a aplicação do índice de correção monetária mencionado no item 8.1, na base de cálculo do item 8.3.
- 8.5. O reajuste será automático e independerá de requerimento do CONTRATADO.
- 8.6. O reajuste será realizado por simples apostila.
- 8.7. No caso de atraso ou não divulgação do índice do item 8.1, o CONTRATANTE utilizará a sua última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.
- 8.8. Caso o índice do item 8.1 venha a ser extinto ou não possa mais ser utilizado, as PARTES elegerão novo índice, fixando-o por meio de termo aditivo.
- 8.9 Não será devido reajuste quando o atraso na entrega do bem for atribuível ao CONTRATADO.

CLÁUSULA NONA – DO PAGAMENTO

- 9.1. O pagamento será realizado em até 30 (trinta) dias corridos, a contar do recebimento da nota fiscal ou fatura atestada pelo fiscal do Contrato.
- 9.2. O pagamento será efetuado por ordem bancária para conta de titularidade da CONTRATADO, cujos dados são:

Banco BANPARÁ
Agência XXXXX-X
Conta-corrente nº XXXX-X

- 9.3. Havendo erro na apresentação da nota fiscal, fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que o CONTRATADO adote as medidas para saneamento das pendências.
- 9.4. Na hipótese do item 9.3, o prazo para pagamento começará a correr depois da comprovação da regularização da pendência, sem ônus à CONTRATANTE.
- 9.5. A data do efetivo pagamento será considerada aquela que constar da ordem bancária emitida para quitação da nota fiscal ou fatura.
- 9.6. A regularidade fiscal do CONTRATADO deve ser verificada pelo CONTRATANTE por ocasião do pagamento por meio de consulta ao Sistema de Cadastramento Unificado de Fornecedores (SICAF) ou, na impossibilidade de acesso a ele, devem ser consultados sítios eletrônicos oficiais ou, ainda, ser solicitada a documentação física listada no art. 68 da Lei Federal nº 14.133/21.
- 9.7. A constatação de irregularidade fiscal do CONTRATADO não impede o pagamento do que foi executado, mas constitui falta contratual, a ser sancionada em procedimento de inexecução contratual.
- 9.8. Antes da instauração do procedimento de inexecução contratual a que faz menção o item 8.7, o CONTRATADO deve ser notificado para regularizar a pendência no prazo de **5 dias úteis**. Não sendo regularizada, deve-se instaurar o procedimento de inexecução contratual, ofertando contraditório e ampla defesa ao CONTRATADO.
- 9.9. A instauração do procedimento de inexecução contratual não impede o pagamento do serviço que já foi



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

prestado.

9.10. Diante da gravidade do caso concreto e para proteger o Erário e o interesse público, a autoridade competente pode decidir pela suspensão do contrato, ocasião em que somente será pago o serviço que já foi prestado.

9.11. Caso ao final do procedimento a que faz menção a parte final do item 8.8 a autoridade decida pela rescisão contratual, o pagamento será sustado automaticamente.

9.12. A inadimplência do CONTRATADO junto ao SICAF é causa de rescisão contratual, exceto se a autoridade máxima do CONTRATANTE justificar a necessidade de manutenção do contrato por motivo de economicidade, segurança estadual ou outro de interesse público de alta relevância.

9.13. O CONTRATANTE efetuará a retenção tributária prevista na legislação aplicável por ocasião do pagamento.

9.14. O CONTRATADO optante do Simples Nacional não sofrerá retenção tributária em relação aos impostos e contribuições abrangidos por aquele regime, mas o pagamento ficará condicionado à comprovação, por documento oficial, de que o CONTRATADO é beneficiário do tratamento tributário previsto na Lei Complementar Federal nº 123/2006.

CLÁUSULA DÉCIMA – DA GARANTIA DE CUMPRIMENTO CONTRATUAL

10.1. O CONTRATADO garantirá o cumprimento do contrato mediante a prestação de uma das modalidades de garantia previstas no art. 96, §1º, da Lei Federal nº 14.133/21, a sua escolha.

10.2. A garantia corresponderá a 1% (hum por cento) do valor atualizado do contrato.

10.3. A garantia em dinheiro deverá ser efetuada em conta bancária de titularidade do CONTRATANTE, cujos dados são:

Banco Banpará

Agência nº xxxx-x

Conta-corrente nº xxxxxx-x.

10.4. Na hipótese de suspensão do contrato por ordem ou inadimplemento do CONTRATANTE, o CONTRATADO ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pelo CONTRATANTE.

10.5. No caso de alteração do valor do Contrato, ou prorrogação de sua vigência, a garantia deverá ser atualizada ou renovada nas mesmas condições.

10.6. Se a garantia for utilizada em pagamento de qualquer obrigação, o CONTRATADO fica obrigado a recompor o que tiver sido usado no prazo máximo de 5 dias úteis, a contar de sua notificação.

10.7. O CONTRATANTE executará a garantia na forma prevista na legislação.

10.8. A garantia prestada pelo CONTRATADO será liberada ou restituída após a execução total do contrato ou após a sua extinção por culpa exclusiva do CONTRATANTE.

10.9. Quando a garantia for em dinheiro, o valor a ser devolvido, nos termos do item 10.8, será corrigido monetariamente.

10.10. A garantia de execução do contrato não desobriga o CONTRATADO de apresentar a garantia contratual dos bens adquiridos, legal e do fabricante, a qual deve ser de 15 (quinze) dias úteis (conforme Termo de Referência), no mínimo.

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DAS PARTES

11.1. O Contratante tem a obrigação de:

- a) Exigir o cumprimento de todas as obrigações assumidas pelo CONTRATADO, de acordo com este contrato, Termo de Referência e anexos,
- b) Receber o objeto no prazo e condições estabelecidas no Termo de Referência,
- c) Notificar o CONTRATADO sobre vícios, defeitos ou incorreções verificadas no objeto fornecido para que ele



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

seja substituído, reparado ou corrigido às suas expensas,

- d) Notificar o CONTRATADO por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se de que as soluções por ele propostas sejam as mais adequadas,
- e) Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações do CONTRATADO,
- f) Efetuar o pagamento do objeto fornecido no prazo, forma e condições aqui estabelecidos,
- g) Aplicar ao CONTRATADO as sanções decorrentes da inexecução total ou parcial do contrato,
- h) Decidir sobre as solicitações e reclamações relacionadas à execução do contrato, ressalvados os requerimentos meramente protelatórios, manifestamente impertinentes ou de nenhum interesse à boa execução do ajuste.

11.2. O CONTRATADO tem a obrigação de:

- a) Cumprir todas as obrigações constantes deste contrato e seus anexos, além daquelas dispostas no termo de referência, assumindo exclusivamente os riscos e as despesas decorrentes de sua execução,
- b) Entregar o objeto no prazo constante no Termo de Referência, acompanhado do manual do usuário com uma versão em português e da relação da rede de assistência técnica autorizada,
- c) Aceitar acréscimos ou supressões unilaterais impostos pelo CONTRATANTE de até **25%** do valor atualizado do contrato, nas mesmas condições pactuadas inicialmente,
- d) Responsabilizar-se pelos vícios e danos do objeto, nos termos dos arts. 12, 13 e 17 a 27, da Lei Federal nº 8.078/90,
- e) Comunicar ao CONTRATANTE, no prazo de até **24 horas** antes da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação,
- f) Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior e prestar esclarecimentos ou informações por eles solicitados.
- g) No prazo fixado pelo fiscal do contrato, reparar, corrigir, remover, reconstruir ou substituir às suas expensas os bens nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução contratual ou dos materiais empregados.
- h) Responsabilizar-se pelos vícios e danos decorrentes do cumprimento deste contrato e de todo dano causado ao CONTRATANTE ou a terceiros, cuja responsabilidade não será reduzida pela fiscalização ou acompanhamento da execução contratual pelo CONTRATANTE, o qual ficará autorizado a descontar o valor dos danos sofridos dos pagamentos devidos ou da garantia.
- i) Na hipótese do item 8.6, parte final, quando solicitado o CONTRATADO deverá entregar ao CONTRATANTE os seguintes documentos:
 - 1. Prova de regularidade relativa à Seguridade Social.
 - 2. Certidão conjunta relativa aos tributos federais e à Dívida Ativa da União.
 - 3. Certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital da sede do CONTRATADO.
 - 4. Certidão de Regularidade do FGTS.
 - 5. Certidão Negativa de Débitos Trabalhistas.
 - 6. Nota fiscal atestada pelo fiscal do contrato.
- j) Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato e obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao CONTRATANTE.
- k) Comunicar ao fiscal do contrato, no prazo de **24 horas**, qualquer ocorrência anormal que se verifique no local da execução do objeto contratual.
- l) Manter durante a vigência do contrato todas as condições exigidas para habilitação na licitação ou para qualificação, na contratação direta.
- m) Cumprir durante todo o período de execução do contrato a reserva de cargos para pessoa com deficiência,



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

reabilitado da Previdência Social, aprendiz e outras reservas de cargos previstas na legislação.

n) Comprovar o cumprimento da alínea acima no prazo fixado pelo fiscal do contrato, indicando os empregados que preencheram as referidas vagas.

o) Arcar com o ônus decorrente de eventual equívoco no dimensionamento do quantitativo de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos do art. 124, II, *d*, da Lei Federal nº 14.133/21.

p) Cumprir as normas de segurança do CONTRATANTE, além da legislação vigente em âmbito federal, estadual e municipal.

q) Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

r) Manter preposto aceito pelo CONTRATANTE no local da prestação do serviço para o representar na execução do contrato.

r.1) A indicação do preposto do CONTRATADO ou a sua manutenção poderá ser recusada pelo CONTRATANTE mediante justificativa, devendo o CONTRATADO designar outro para o exercício da atividade.

s) Alocar os empregados em número compatível para o cumprimento deste contrato e com a habilitação e conhecimento adequados para a execução do serviço, fornecendo os materiais, equipamentos, ferramentas e utensílios necessários para tanto, cuja quantidade, qualidade e tecnologia deverão atender às recomendações dos órgãos de regulação responsáveis e à legislação aplicável.

t) Durante a vigência do contrato, não contratar cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o 3º grau, de dirigente do CONTRATANTE ou de agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato.

u) Não permitir:

u.1) o trabalho de pessoa menor de 16 anos no objeto deste contrato, exceto na condição de aprendiz para os maiores de 14 anos; e

u.2) a utilização do trabalho da pessoa menor de 18 anos em trabalho noturno, perigoso ou insalubre, em qualquer hipótese.

v) Submeter previamente e por escrito ao CONTRATANTE qualquer mudança nos métodos executivos especificados no memorial descritivo ou documento similar para sua análise e aprovação.

CLÁUSULA DÉCIMA SEGUNDA - DA RESPONSABILIDADE POR DANOS

12.1. A responsabilidade pelos danos causados por ato do CONTRATADO, de seus empregados, prepostos ou subordinado, é exclusivamente do CONTRATADO.

12.2. A responsabilidade pelos compromissos assumidos pelo CONTRATADO com terceiros é exclusivamente sua.

12.3. O CONTRATANTE não responderá pelos compromissos assumidos pelo CONTRATADO com terceiros, ainda que vinculados à execução deste contrato, ou por qualquer dano causado por ato do CONTRATADO, de seus empregados, prepostos ou subordinados.

CLÁUSULA DÉCIMA TERCEIRA – DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

13.1. Constituem infrações administrativas do CONTRATADO a serem punidas com as seguintes sanções:

INFRAÇÃO	PENALIDADE



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

a. Dar causa à inexecução parcial do contrato.	Advertência* * Exceto quando se justificar a imposição de penalidade mais grave, ocasião em que poderá ser aplicada a sanção de “ <i>Impedimento de licitar e contratar</i> ”.
b. Dar causa à inexecução parcial do contrato que cause grave dano ao CONTRATANTE ou ao funcionamento dos serviços públicos ou ao interesse coletivo. c. Dar causa à inexecução total do contrato. d. Deixar de entregar a documentação exigida para o certame. e. Deixar de manter sua proposta, salvo em decorrência de fato superveniente devidamente justificado. f. Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado.	Impedimento de licitar e contratar* * Exceto quando se justificar a imposição de penalidade mais grave, ocasião em que poderá ser aplicada a sanção de “ <i>Declaração de inidoneidade para licitar e contratar</i> ”.
g. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou execução do contrato. h. Fraudar a contratação ou praticar ato fraudulento na execução do contrato. i. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza. j. Praticar atos ilícitos com vistas a frustrar os objetivos do certame. k. Praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846/13.	Declaração de inidoneidade para licitar e contratar

13.2. O atraso superior a 15 (quinze) dias corridos autoriza a rescisão do contrato por seu descumprimento, nos termos do art. 137, I, da Lei Federal nº 14.133/21.

13.3. A aplicação das sanções previstas neste contrato não exclui a obrigação de reparação integral do dano causado ao CONTRATANTE.

13.4. As sanções podem ser cumuladas com as seguintes multas:

MULTA	
Moratória a. 0,1% (zero vírgula um por cento) sobre o valor da parcela inadimplida por dia de atraso injustificado até o limite de 15 dias corridos. b. 1% (um por cento) sobre o valor total do contrato por dia de atraso injustificado até o limite de 30 dias corridos, pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.	Compensatória 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do seu objeto.

13.5. Antes da aplicação das sanções, o CONTRATADO será notificado para apresentar defesa no prazo de 15 (quinze) dias úteis, contado de sua intimação.

13.6. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor devido ao CONTRATADO, além da perda deste valor, a diferença será descontada da garantia prestada e/ou será cobrada judicialmente.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

13.7. Antes do ajuizamento da cobrança, a multa poderá ser recolhida administrativamente em até 15 (quinze) dias úteis, a contar do trânsito em julgado da decisão administrativa.

13.8. A aplicação das sanções será precedida de processo administrativo em que seja assegurado o contraditório e a ampla defesa ao CONTRATADO, observando o rito especial previsto no art. 158 da Lei Federal nº 14.133/21 para as penalidades de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar.

13.9. A aplicação das sanções deve observar:

- a) A natureza e gravidade da infração.
- b) As peculiaridades do caso.
- c) As circunstâncias agravantes e/ou atenuantes.
- d) Os danos causados ao CONTRATANTE.

13.10. A implantação ou aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

13.11. As infrações administrativas tipificadas como atos lesivos na Lei Federal nº 12.846/13 serão apuradas e julgadas em conjunto com as infrações previstas neste contrato, nos mesmos autos.

13.12. A personalidade jurídica do CONTRATADO poderá ser desconsiderada quando for utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste contrato ou para provocar confusão patrimonial e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o CONTRATADO, observados o contraditório, ampla defesa e a obrigatoriedade de análise jurídica prévia.

13.13. No prazo de 15 (quinze) dias úteis, a contar da data de aplicação da sanção, o CONTRATANTE informará e manterá atualizados os dados relativos às sanções aplicadas por ela, para publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

13.14. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação, na forma do art. 163 da Lei Federal nº 14.133/21.

13.15. Caso ocorra degradação do tipo, aumento no tempo de resposta, ou aumento na taxa de erro, ou aumento na latência (entende-se por degradação como sendo toda interferência que venha causar sucessivas retransmissões de pacotes no circuito de dados), acumulativa superior a 4 (quatro) horas no período de 30 (trinta) dias, a CONTRATADA será penalizada com multa compensatória sobre o valor mensal do circuito a cada hora pelas interrupções temporárias a serem descontadas no preço da fatura do circuito, cumulativa até o máximo de 10% (dez por cento) do valor total da fatura mensal do circuito, conforme a tabela abaixo:

<i>Criticidade</i>	<i>Multa por hora</i>
<i>1</i>	<i>0,1%</i>
<i>2</i>	<i>0,25%</i>
<i>3</i>	<i>0,5%</i>
<i>4</i>	<i>0,75 %</i>
<i>5</i>	<i>1 %</i>

Tabela 2 - Aplicação de Penalidades por Degradação

13.15.1. Para aplicação do disposto neste item a CONTRATANTE terá que registrar junto a Central de Atendimento da CONTRATADA a ocorrência de degradação. Após o registro a CONTRATADA terá o período de 04 (quatro) horas para circuitos da Região Metropolitana de Belém e 12 (doze) horas para os demais circuitos para testes e recuperação dos mesmos. Terminados estes prazos as multas compensatórias serão praticadas conforme a criticidade acima definida, considerando o período total de degradação registrado conforme o item 6.3.2 do Anexo I do Termo de Referência.

13.16. Haverá desconto dos valores na fatura da CONTRATADA, nos termos deste item, conforme critérios de



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

cálculo estabelecidos em caso de interrupções da prestação do serviço, que não sejam causadas por:

- a) Caso fortuito ou força maior (entende-se como caso fortuito como sendo qualquer ocorrência que não seja proveniente de qualquer ação humana).
- b) Operação inadequada, falha ou mau funcionamento de equipamentos não mantidos pela CONTRATADA.
- c) Falha de equipamento de propriedade ou sob responsabilidade da CONTRATADA, ocasionada pela CONTRATANTE ou seus clientes.
- d) Falha na infraestrutura da CONTRATANTE.
- e) Realização de testes, ajustes e manutenção necessários à prestação do serviço, devidamente comunicados à CONTRATANTE com antecedência mínima de 5 (cinco) dias úteis ou em caso comprovado de urgência, conforme item 6.4.5 do Anexo I do Termo de Referência.
- f) Impedimento, por qualquer motivo, do acesso de pessoal técnico da CONTRATADA às dependências da CONTRATANTE, onde estejam localizados os equipamentos da CONTRATADA ou por estes mantidos, desde que devidamente comunicados a CONTRATANTE.
- g) Falta de energia elétrica nas dependências da CONTRATANTE.

13.17. A CONTRATADA trabalhará de forma proativa informando à CONTRATANTE sobre o andamento do processo de recuperação em até 30 (trinta) minutos após o registro do problema e a cada intervalo de 2 (duas) horas, informando inclusive a estimativa de tempo para a completa solução do problema.

13.18. Falhas em equipamentos ou serviços de propriedade ou responsabilidade da CONTRATADA que impliquem em suspensão dos serviços prestados pela CONTRATANTE, motivarão a aplicação de multas compensatórias e descontos referentes à hora parada, ressalvado as condições listadas no item 14.17.

13.19. A CONTRATADA deverá executar a recuperação do circuito com problema em prazo determinado na coluna “Tempo Máximo de Reparo” do Anexo IV deste edital. Caso a CONTRATADA não consiga cumprir o prazo determinado pela CONTRATANTE para resolução do problema, incidirão multas compensatórias de 1% (um por cento) do valor mensal do circuito, para cada hora de paralisação, cumulativa até o máximo de 10% (dez por cento) do valor total da fatura mensal do circuito. Fica a critério da CONTRATANTE o desconto sobre a fatura mensal ao qual o circuito em questão esteja inserido, ou seu respectivo pagamento em conta, no prazo de até 30 (trinta) dias consecutivos.

Item	Critérios
Penalidade sobre o tempo de interrupção no circuito (fim-a-fim). Previsto para o não cumprimento do “Tempo Máximo de Reparo”	A cada hora de interrupção, após decorrido o tempo máximo de reparo constante no anexo IV, nas 2 (duas) primeiras horas
	A cada hora de interrupção contada após as 2 (duas) primeiras horas

Tabela 3 - Aplicação de Penalidades por Tempo Máximo de Reparo

13.20. O desconto referente à Hora Parada do Circuito será aplicado ao valor do circuito parado sob responsabilidade da CONTRATADA, conforme fórmula abaixo. Fica a critério da CONTRATANTE o desconto sobre a fatura mensal ao qual o circuito em questão esteja inserido, ou seu respectivo pagamento em conta, no prazo máximo de 30 (trinta) dias consecutivos.

Valor do desconto por Hora Parada = (Valor do circuito / 720) Quant. de Horas Paradas.

Valor do desconto mensal = Quant. de Horas Paradas x Valor do desconto por Hora Parada.

13.20.1. Para efeito de cálculo, as penalidades deverão ser aplicadas baseadas em horas fracionadas.

CLÁUSULA DÉCIMA QUARTA – DAS ALTERAÇÕES DO CONTRATO

14.1. As eventuais alterações contratuais serão disciplinadas pelo art. 124 e seguintes da Lei Federal nº 14.133/21.

14.2. Caso haja interesse público, o CONTRATANTE pode alterar unilateralmente o contrato para impor



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor atualizado do contrato, mantidas as mesmas condições pactuadas inicialmente.

14.3. As PARTES podem acordar suprimir o objeto do contrato em percentual superior a 25% do valor inicial atualizado do contrato.

14.4. Os acréscimos ou supressões não podem transfigurar o objeto da contratação.

14.5. Registros que não caracterizem alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, conforme art. 136 da Lei Federal nº 14.133/21.

CLÁUSULA DÉCIMA QUINTA – DA EXTINÇÃO DO CONTRATO

15.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes,

15.2. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

15.3. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

15.4. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

15.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

15.6. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

15.7. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

15.8. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

15.9. O termo de extinção, sempre que possível, será precedido:

- a) Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;
- b) Relação dos pagamentos já efetuados e ainda devidos;
- c) Indenizações e multas.

15.10. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, caput, da Lei n.º 14.133, de 2021).

CLÁUSULA DÉCIMA SEXTA – DA FISCALIZAÇÃO

16.1. O cumprimento do contrato será fiscalizado pelo servidor nome do servidor, CPF nº xxx.xxx.xxx-xx, matrícula nº nnnn, lotado na DTI, conforme ato a ser publicado no Diário Oficial do Estado.

CLÁUSULA DÉCIMA SÉTIMA – DAS OBRIGAÇÕES PERTINENTES À LGPD

17.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

17.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

17.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

17.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

17.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

17.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

17.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

17.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

17.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

17.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

17.11. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

17.12. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

CLÁUSULA DÉCIMA OITAVA – DA INTERPRETAÇÃO

18.1. As dúvidas interpretativas sobre as cláusulas deste contrato deverão ser suscitadas ao CONTRATANTE e serão decididas por ele, de acordo com a Lei Federal nº 14.133/21, seus regulamentos, Lei Estadual nº 8.972/20 e observando a jurisprudência dos Tribunais sobre o assunto.

CLÁUSULA DÉCIMA NONA – DO TRATAMENTO ADEQUADO DOS CONFLITOS DE INTERESSE

19.1. Observado o disposto na Cláusula 18, permanecendo o conflito de interesse, as PARTES se comprometem a submeter a disputa *preferencialmente* à CÂMARA DE NEGOCIAÇÃO, CONCILIAÇÃO, MEDIAÇÃO E ARBITRAGEM DA ADMINISTRAÇÃO PÚBLICA ESTADUAL para dirimir os conflitos decorrentes deste contrato de maneira consensual, conforme Lei Complementar Estadual nº 121/2019.

CLÁUSULA VIGÉSIMA – DA DIVULGAÇÃO E PUBLICAÇÃO

20.1. O CONTRATANTE divulgará este contrato no Portal Nacional de Contratações Públicas (PNCP) em até **20 dias úteis** e o publicará no Diário Oficial do Estado em forma de extrato, no prazo de **10 dias úteis**.

20.2. Os prazos contidos no item 20.1 são contados da data da assinatura do contrato.

CLÁUSULA VIGÉSIMA PRIMEIRA – DA VIGÊNCIA

21.1. O Contrato terá vigência de 24 (vinte e quatro) meses a partir da data de sua publicação no Diário Oficial do Estado, com início em **dd/mm/aaaa** e término em **dd/mm/aaaa**, podendo ser prorrogado em até 10 (dez) anos, com base nos artigos 106 e 107 da Lei Federal nº 14.133/2021.



GOVERNO DO ESTADO DO PARÁ
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL
DEPARTAMENTO DE TRÂNSITO DO ESTADO DO PARÁ
COMISSÃO DE CONTRATAÇÃO

21.2. A prorrogação de que trata este item é condicionada ao atesto, pela autoridade competente, de que as condições e os preços permanecem vantajosos, ainda para o cumprimento dos seguintes requisitos:

- a) Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;
- b) Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;
- c) Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;
- d) Haja manifestação expressa do CONTRATADO informando o interesse na prorrogação;
- e) Seja comprovado que o CONTRATADO mantém as condições iniciais de habilitação;

21.3. O CONTRATADO não tem direito subjetivo à prorrogação.

21.4. A prorrogação de Contrato deverá ser promovida mediante celebração de termo aditivo.

21.5. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

21.6. O contrato não poderá ser prorrogado quando o CONTRATADO tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com o poder público, observadas as abrangências de aplicação.

CLÁUSULA VIGÉSIMA SEGUNDA – DO FORO

22.1. As PARTES elegem o foro da Comarca de Belém-PA para resolver os litígios oriundos deste Contrato, observado o disposto na Cláusula 19.

Belém, ____ de _____ de 2026.

DIRETORA GERAL DO DETRAN/PA

EMPRESA

TESTEMUNHAS:

1. _____

RG nº xxxxx PC/UF

CPF nº 000.000.000-00

2. _____

RG nº xxxxx PC/UF

CPF nº 000.000.000-00

DOE nº:

DATA: ____/____/____