

PREGÃO ELETRÔNICO Nº 02/2026/ITERPA
PAE nº 2026/2933349

RESUMO



PROMOTOR

Estado do Pará | Instituto de Terras do Pará – ITERPA
CNPJ nº 05.089.495/0001-90



OBJETO

Contratação de empresa especializada para o fornecimento de solução integrada de segurança de rede, abrangendo a entrega, a instalação, a configuração, a integração e a operação dos equipamentos a seguir, acompanhada do serviço continuado de detecção e resposta a ameaças nos computadores e servidores do Instituto de Terras do Pará – ITERPA, conforme quantidades, condições e especificações constantes no Termo de Referência.



MÉTODO DE DISPUTA

- ☐ Aberto
- ☒ Aberto e fechado
- ☐ Fechado e aberto



CRITÉRIO DE JULGAMENTO

- ☒ Menor preço
- ☐ Maior desconto



LOCAL DA PRESTAÇÃO DO SERVIÇO

Local:

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque
Guajará - Icoaraci – CEP: 66.821-000



VALOR TOTAL

R\$ 6.596.398,75 (seis milhões, quinhentos e noventa e seis mil, trezentos e noventa e oito reais e setenta e cinco centavos)

PAGAMENTO

Forma

Ordem bancária.

Prazo

20 dias úteis, a contar do recebimento da nota fiscal ou fatura atestada pelo fiscal do contrato.



ABERTURA DA SESSÃO PÚBLICA

Data

21/10/2026.

Hora

09h00min (Horário de Brasília).

Endereço Eletrônico:

Portal de Compras do Governo Federal -
<https://www.gov.br/compras>

SUMÁRIO

CLÁUSULA 1	
Promotor do pregão	4
CLÁUSULA 2	
Fundamento legal.....	4
CLÁUSULA 3	
Objeto	4
CLÁUSULA 4	
Condições para participar da licitação.....	5
CLÁUSULA 5	
Fases da licitação, apresentação da proposta e documentos de habilitação	7
CLÁUSULA 6	
Preenchimento da proposta	9
CLÁUSULA 7	
Abertura da sessão, classificação das propostas e formulação de lances	10
CLÁUSULA 8	
<i>Julgamento</i> das propostas.....	16
CLÁUSULA 9	
Habilitação.....	19
CLÁUSULA 10	
Adjudicação e homologação	24
CLÁUSULA 11	
Recursos.....	24
CLÁUSULA 12	
Contratação	245
CLÁUSULA 13	
Infrações e sanções administrativas.....	26
CLÁUSULA 14	
Impugnação ao edital	29
CLÁUSULA 15	
Disposições finais.....	30

REGULAMENTO DA COMPETIÇÃO

CLÁUSULA 1

Promotor do pregão

O PROMOTOR deste pregão é o **ESTADO DO PARÁ**, por intermédio do **INSTITUTO DE TERRAS DO PARÁ -ITERPA**, Autarquia, Pessoa Jurídica de Direito Público da Administração Indireta do Estado do Pará, inscrito no CNPJ nº 05.089.495/0001-90, com sede à Rod. Augusto Montenegro, SN, km 09, Bairro Parque Guajará, Distrito – Icoaraci, CEP: 66.821-000, Belém-PA, neste ato representada pelo Presidente do Órgão Sr. **FLÁVIO RICARDO ALBUQUERQUE AZEVEDO**, CPF: **727.811.222-20**. Tendo como pregoeira a Sra. Carla Suellem A. da Rocha indicada pela portaria nº 321/2026 de 07 de maio de 2026 publicada no DOE 36.623 de 08 de maio de 2026.

CLÁUSULA 2

Fundamento legal

2.1 A presente licitação será realizada por meio de **PREGÃO ELETRÔNICO** e observará a Lei Federal nº 14.133/21, Decreto Estadual nº 2.940/2023, Lei Complementar Federal nº 123/06, demais normas aplicáveis e as condições estabelecidas neste Edital.

CLÁUSULA 3

Objeto

3.1 O objeto desta licitação é a **contratação de empresa especializada para o fornecimento de solução integrada de segurança de rede**, abrangendo a entrega, a instalação, a configuração, a integração e a operação dos equipamentos a seguir, acompanhada do serviço continuado de detecção e resposta a ameaças nos computadores e servidores do Instituto de Terras do Pará – ITERPA, conforme descrito no Termo de Referência (TR), o qual **ADERE** a este documento para todos os fins.

3.1.1 Havendo discordância entre as especificações deste objeto descritas no **COMPRASNET-CATMAT** e as especificações constantes do **ANEXO I** – Termo de Referência e seus adendos, prevalecerão as últimas.

3.2. A licitação será realizada em **grupo/lote único, formados por 05 (cinco) itens**, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

3.3 A licitação observará o seguinte:

- ☐ **Item único;**
- ☐ **Divisão em itens**, conforme tabela do [item 3.2](#) deste edital;

- ☐ **Lotes**, formados por um ou mais itens, conforme tabela constante do TR, facultando-se ao LICITANTE a participação em quantos grupos forem de seu interesse, devendo oferecer proposta para todos os itens que os compõem; ou
- ☒ **Lote único, formados por 5 (cinco) itens**, conforme tabela constante no TR, devendo o LICITANTE oferecer proposta para todos os itens que o compõem.

CLÁUSULA 4

Condições para participar da licitação

4.1 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.

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

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

4.3 É de responsabilidade do LICITANTE conferir a exatidão dos seus dados cadastrais nos sistemas relacionados no [item 4.1](#) e mantê-los atualizados junto aos órgãos responsáveis pela informação.

4.4 A incorreção dos dados registrados nos sistemas relacionados no [item 4.1](#) poderá motivar a inabilitação do LICITANTE por descumprimento do dever constante no item anterior.

4.5 Neste certame, o **LOTE ÚNICO**, cujo valor original estimado é superior a R\$ 80.000,00 (oitenta mil reais), não possuirá cota reservada destinado exclusivamente à participação de microempresas e empresas de pequeno porte, conforme art. 49, III, Lei Complementar 123/2006 e art. 13, II, Lei Estadual nº 8.417/2016, pois o lote exige a contratação de serviço e a natureza do objeto não possibilita a criação de cota, conforme art. 48, III, Lei Complementar 123/2006, de 14 de dezembro de 2006 e art. 11, Lei Estadual nº 8.417, de 7 de novembro de 2016;

4.5.1 No **LOTE ÚNICO não será concedido** nesta Licitação tratamento favorecido para microempresas, empresas de pequeno porte e figuras equiparadas, nos termos da Lei Complementar nº 123, de 2006 e da Lei Estadual nº 8.417, de 7 de novembro de 2016, em razão da incidência, no caso, do inciso I, art. 4º, § 1º da Lei nº 14.133, de 2021.

4.5.2 No **LOTE ÚNICO será vedada** a participação de empresas em consórcio, nos termos dos art.15 da Lei 14.133/2021 e no art. 40, § 2º, do mesmo diploma, por se tratar de serviço ofertado, de forma usual, por fornecedor único no mercado de soluções integradas de segurança de rede, circunstância que afasta a necessidade de agregação de competências de diferentes empresas, conforme exigência no item **4.10 e 8.7** do termo de referência, anexo I do Edital.

4.6 Não poderão disputar esta licitação:

- a.** Aquele que não atenda às condições deste Edital e seus anexos;
- 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 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.

4.7 É vedada a participação direta ou indireta de agente público do órgão ou entidade contratante na licitação ou da execução do contrato.

4.8 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.

4.9 O impedimento de que trata a [alínea d do item 4.6](#) 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.

4.10 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 4.6](#) 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.

4.11 As empresas integrantes do mesmo grupo econômico também são consideradas como autoras do projeto.

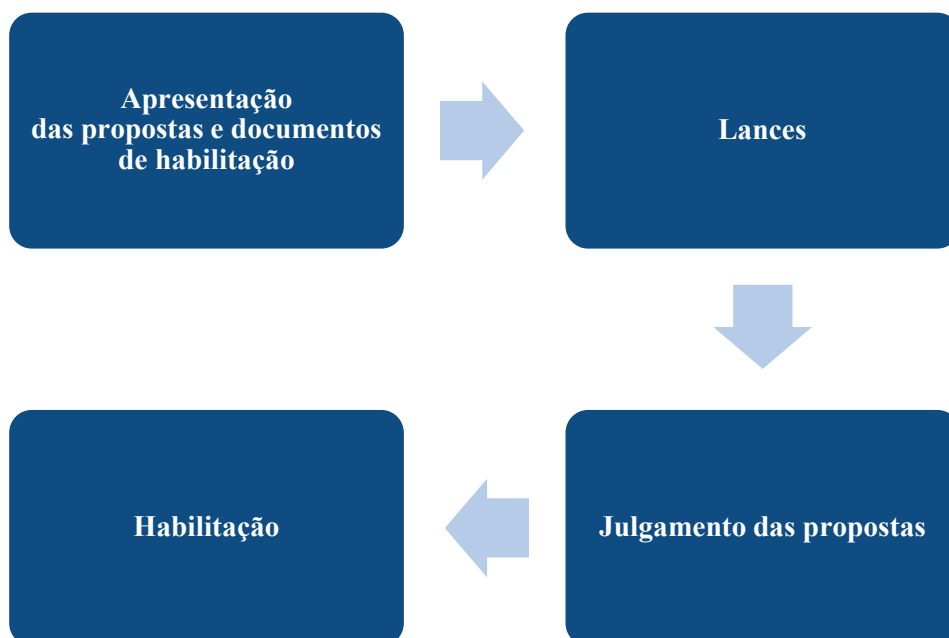
4.12 O disposto nas [alíneas b e c do item 4.6](#) não impede a licitação ou a contratação de serviço que inclua como obrigação do contratado a elaboração do projeto executivo.

4.13 A proibição do [item 4.7](#) 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.

CLÁUSULA 5

Fases da licitação, apresentação da proposta e documentos de habilitação

5.1 A licitação terá as seguintes fases:



5.2 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 data e o horário estabelecidos para abertura da sessão pública, **sendo vedada a proposta com ocorrência de registro de oportunidade**.

5.3 No cadastramento da proposta inicial, o LICITANTE declarará em campo próprio que:

- 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.

5.4 As MEs, EPPs 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.

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

5.4.2 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.

5.5 Sob pena de desclassificação, na apresentação da proposta adequada ao último lance ofertado após a negociação, o licitante enviará **declaração que ateste a não ocorrência do registro de oportunidade**, de modo a garantir o princípio da competitividade, conforme o disposto no art. 5º da Lei nº 14.133, de 2021.

5.6 A realização de declarações falsas nos itens 5.3 e 5.4 sujeitará o LICITANTE às sanções previstas na Lei Federal nº 14.133/21 e neste Edital.

5.7 Os LICITANTES poderão retirar ou substituir a proposta ou os documentos de habilitação inseridos no sistema até a abertura da sessão pública.

5.8 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.

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

5.10 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.

5.11 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*.

5.12 O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do [item 5.9](#) será **sigiloso** para os demais LICITANTES e para o PROMOTOR, mas pode ser disponibilizado aos órgãos de controle externo e interno da administração.

5.13 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.

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

CLÁUSULA 6

Preenchimento da proposta

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

- a.** ☒ valor do item.
- ☐ (percentual) desconto.
- b.** Marca.
- c.** Fabricante.
- d.** Descrição do objeto, contendo informações similares à especificação do TR.

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

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

6.4 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 7.13](#).

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

6.6 A apresentação das propostas obrigar cumprir o que nelas estão contidas e em conformidade com o TR.

6.7 Em virtude do compromisso previsto no [item 6.6](#), o LICITANTE que apresenta proposta está obrigado a executar o objeto licitado nos termos da proposta, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios em quantidades e qualidades adequadas à execução contratual, promovendo sua substituição, quando requerido.

6.8 O prazo de validade da proposta não será inferior a **60 dias**, a contar da data de sua apresentação.

6.8.1. O prazo de validade ficará suspenso pelo tempo necessário à conclusão de eventuais diligências e no caso de interposição de recursos, inclusive até seu julgamento.

6.8.2. A proposta deverá conter preço total, fixo e irrevogável, expresso em moeda corrente nacional, apurado à data da apresentação da proposta, sem a inclusão de encargos financeiros ou previsão inflacionária.

6.8.3. Não caberá desistência de proposta, salvo em decorrência de fato superveniente devidamente justificado.

6.8.4. A licitante não poderá, em qualquer hipótese, alegar desconhecimento do objeto a ser executado, nem modificar preços, quantidades ou condições de sua proposta depois de aberta, alegando insuficiência de dados ou informações.

6.9 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:
 - 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
 - 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.

CLÁUSULA 7

Abertura da sessão, classificação das propostas e formulação de lances

7.1 A abertura da presente licitação será realizada em sessão pública e eletrônica, na data, horário e local indicados neste Edital.

7.2 A proposta que identifique o LICITANTE será desclassificada.

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

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

7.5 O sistema ordenará automaticamente as propostas classificadas.

7.6 Apenas as propostas classificadas participarão da fase de lances.

7.7 O sistema disponibilizará campo próprio para troca de mensagens entre o PREGOEIRO e os LICITANTES.

7.8 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.

7.9 O lance deverá ser ofertado do seguinte modo:

7.10 Os LICITANTES poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas neste Edital.

7.11 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.

7.12 O intervalo mínimo de diferença de valores ou percentuais entre os lances ofertados pelos LICITANTES, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de cem reais (R\$100,00).

7.13 O LICITANTE poderá, uma única vez, excluir seu último lance ofertado, no intervalo de 15 segundos após o registro no sistema, na hipótese de lance inconsistente ou inexecutable.

7.14 O procedimento observará modo de disputa adotado da seguinte forma:

Modo de Disputa	Regras
☐ 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 minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 minutos da sessão pública. c. A prorrogação automática da etapa de lances, de que trata a alínea anterior, será de 2 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%, o PREGOEIRO, 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.

☒ **Aberto
e fechado**

- a. No modo de disputa **aberto e fechado**, os LICITANTES apresentarão lances públicos e sucessivos, com lance final e fechado.
- b. A fase de lances da sessão pública terá duração inicial de 15 minutos. Após esse tempo, o sistema encaminhará aviso de fechamento iminente dos lances e, a partir daí, será aleatoriamente determinado um tempo de até 10 minutos para envio de lances. Terminado este prazo adicional, a recepção de lances será automaticamente encerrada.
- c. Encerrado o prazo previsto na alínea anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% superiores àquela possam ofertar um lance final e fechado, no prazo de 5 minutos. Este lance será *sigiloso* até o encerramento do prazo de 5 minutos.
- d. No procedimento de que trata a alínea anterior, o LICITANTE poderá manter o seu último lance da etapa aberta ou ofertar um lance melhor.
- e. Não havendo pelo menos 3 ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de 3, oferecer um lance final e fechado no prazo de 5 minutos. Durante este prazo, o lance terá caráter *sigiloso*.

☐ **Fechado
e aberto**

- a. No modo de disputa **fechado e aberto**, somente podem participar os LICITANTES que apresentarem a proposta de menor preço/menor percentual de desconto e os das propostas até 10% superiores/inferiores àquela.
- b. Neste modo de disputa, os LICITANTES apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.
- c. Não havendo 3 propostas nas condições definidas na forma da alínea a, poderão os LICITANTES que apresentaram as 3 melhores propostas, considerados as empatadas, oferecer novos lances sucessivos.

- d. A fase de lances da sessão pública terá duração de 10 minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 minutos do período de duração da sessão pública.
- e. A prorrogação automática da etapa de lances, de que trata a alínea anterior, será de 2 minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.
- f. Não havendo novos lances na forma estabelecida nas alíneas anteriores, a sessão pública se encerrará automaticamente e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.
- g. Definida a melhor proposta, se a diferença em relação à proposta classificada em 2º lugar for de pelo menos 5%, o PREGOEIRO, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.
- h. Após o reinício previsto na alínea anterior, os LICITANTES serão convocados para apresentar lances intermediários, podendo optar por manter o seu último lance.

7.15 Após o término dos prazos estabelecidos no [item 7.14](#), o sistema ordenará e divulgará os lances segundo a ordem *crescente*, por se tratar de critério de julgamento por menor preço de valores.

7.16 Não serão aceitos 2 ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em 1º lugar.

7.17 Durante o transcurso da sessão pública, os LICITANTES serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do LICITANTE.

7.18 No caso de desconexão com o PREGOEIRO durante a etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos LICITANTES para a recepção dos lances.

7.19 Quando a desconexão do sistema eletrônico para o PREGOEIRO durar mais de 10 minutos, a sessão pública será suspensa e reiniciada somente após decorridas 24 horas da comunicação deste fato pelo PREGOEIRO aos LICITANTES, no sítio eletrônico utilizado para divulgação.

7.20 Caso o LICITANTE não apresente lances, concorrerá com o valor de sua proposta.

7.21 Em relação a itens não exclusivos para participação de MEs e EPPs, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as MEs e EPPs 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 123/06, regulamentada pela Lei Estadual nº 8.417/16.

7.21.1 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.

7.21.2 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.

7.21.3 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.

7.21.4 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.

7.22 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.

7.23 Havendo empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60, da Lei nº 14.133, de 2021, nesta ordem:

Disputa final

Os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação.

Avaliação do desempenho contratual prévio

Deverão ser utilizados preferencialmente registros cadastrais para efeito de atesto de cumprimento de obrigações contratuais prévias.

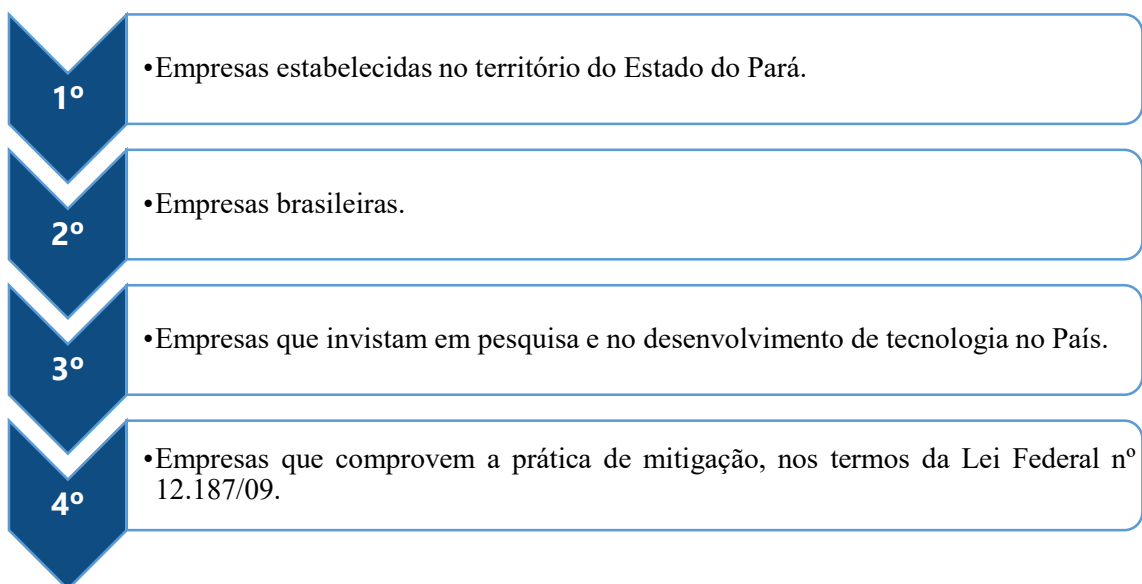
Desenvolvimento de ações de equidade entre homens e mulheres no ambiente de trabalho

Conforme regulamento.

Desenvolvimento de programa de integridade

Conforme orientações dos órgãos de controle.

7.24 Persistindo o empate, será assegurada preferência sucessivamente às:



7.25 Encerrada a etapa de envio de lances da sessão pública, 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, o PREGOEIRO poderá negociar condições mais vantajosas depois de definido o resultado do julgamento.

7.26 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.

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

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

7.29 O PREGOEIRO solicitará ao LICITANTE mais bem classificado que, no prazo de **2 horas**, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada da **DECLARAÇÃO DE NÃO OCORRÊNCIA DE REGISTRO DE OPORTUNIDADE** (anexo IV do edital) e, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

7.30 É facultado ao PREGOEIRO 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.

7.31 Após a negociação do preço, o PREGOEIRO iniciará a fase de aceitação e julgamento da proposta.

CLÁUSULA 8

Julgamento das propostas

8.1 Encerrada a negociação do preço, o PREGOEIRO 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 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>).

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

8.2.1 A consulta no CEIS quanto às sanções previstas na Lei nº 8.429/92, também ocorrerá no nome e no CPF do sócio majoritário da empresa licitante, se houver, por força do art. 12 da citada lei.

8.3 Caso a consulta mostre OCORRÊNCIAS IMPEDITIVAS INDIRETAS, o PREGOEIRO 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.

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

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

8.6 Verificadas as condições de participação e de utilização do tratamento favorecido, o PREGOEIRO 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.

8.7 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 inexequíveis 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.

8.8 É indício de inexequibilidade das propostas valores inferiores a 50% do valor orçado pela administração, devendo o PREGOEIRO 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.

8.9 Somente a verificação dos fatos referidos nas alíneas **a** e **b** do item anterior autoriza a constatação da inexequibilidade da proposta e a sua consequente desclassificação.

8.10 Em contratação de serviços de engenharia, além das disposições dos [itens 8.8](#) e [8.9](#), a análise de exequibilidade e sobrepreço considerará o seguinte:

- a. Nos regimes de execução por tarefa, empreitada por preço global ou empreitada integral, a caracterização do sobrepreço se dará pela superação do valor global estimado;
- b. No regime de empreitada por preço unitário, a caracterização do sobrepreço se dará pela superação do valor global estimado e pela superação de custo unitário tido como relevante, conforme planilha anexa ao edital;
- c. No caso de serviços de engenharia, serão consideradas inexequíveis as propostas cujos valores forem inferiores a 75% do valor orçado pela Administração, independentemente do regime de execução.
- d. Será exigida garantia adicional do LICITANTE vencedor cuja proposta for inferior a 85% do valor orçado pela Administração, equivalente à diferença entre este último e o valor da proposta, sem prejuízo das demais garantias exigíveis de acordo com a Lei.

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

8.12 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.

8.12.1 Em se tratando de serviços de engenharia, o LICITANTE vencedor será convocado a apresentar à Administração, por meio eletrônico, as planilhas com indicação dos quantitativos e dos custos unitários, seguindo o modelo elaborado pela Administração, bem como com detalhamento das Bonificações e Despesas Indiretas (BDI) e dos Encargos Sociais (ES), com os valores adequados ao valor final da proposta vencedora, admitida a utilização dos preços unitários, no caso de empreitada por preço global e empreitada integral, exclusivamente para eventuais adequações indispensáveis no cronograma físico-financeiro e para balizar excepcional aditamento posterior do contrato.

8.13 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.

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

8.13.2 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.

8.14 Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

8.15 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.

8.16 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.

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

8.18 A proposta do LICITANTE será recusada nos seguintes casos:

- a.** Não entrega ou entrega atrasada da amostra, sem que tenha havido justificativa aceita pelo PREGOEIRO; ou
- b.** Entrega no prazo, mas fora das especificações previstas no TR.

8.19 Se a amostra apresentada pelo 1º classificado não for aceita, o PREGOEIRO analisará a aceitabilidade da proposta ou lance ofertado pelo 2º classificado. Seguir-se-á com a verificação das amostras e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no TR.

CLÁUSULA 9

Habilitação

9.1 Para habilitação dos licitantes, serão exigidos os documentos necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, nos termos do art. 36 e seguintes, do Decreto Estadual nº 2.940, de 2023, e dos arts. 62 a 70, da Lei nº 14.133, de 2021.

9.1.1 Habilitação jurídica

9.1.1.1 No caso de Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

9.1.1.2 No caso de 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>;

9.1.1.3 No caso de 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;

9.1.1.4 No caso de 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;

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

9.1.1.6 No caso de 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;

9.1.1.7 No caso de 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 1971;

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

9.1.2 Habilitação fiscal, social e trabalhista

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

9.1.2.2 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.

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

9.1.2.4. 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;

9.1.2.5. 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;

9.1.2.6. 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;

9.1.2.7. Caso o fornecedor seja considerado isento dos tributos 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.

9.1.2.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

9.1.3 Qualificação Econômico-Financeira

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

9.1.3.2 Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta:

9.1.3.2.1 Para que a documentação exigida no subitem anterior seja considerada como apresentada na forma da lei e normativos contábeis, as licitantes devem observar que:

I - As empresas de Grande Porte que adotam a NBC TG 26(5) e as Pequenas e Médias empresas que adotam a NBC TG 1000 devem apresentar os seguintes demonstrativos: *Balanço Patrimonial, Demonstração do Resultado do Exercício, Demonstração das Mutações do Patrimônio Líquido, Demonstração dos Fluxos de Caixa do Período e Notas Explicativas. Caso haja necessidade, poderão ser solicitados em diligência os demais demonstrativos.*

II - As microentidades que adotam o ITG 1000 (procedimento simplificado) devem apresentar os seguintes demonstrativos: Balanço Patrimonial, Demonstração do Resultado do

Exercício e Demonstrações dos Lucros ou Prejuízos Acumulados, desde que a nota explicativa o modelo contábil adotado (ITG 1000). Caso esta informação não esteja explícita, entender-se-á que foi adotada NBC TG 1000, implicando na apresentação dos documentos contábeis correspondentes, quais sejam: *Balanço Patrimonial, Demonstração do Resultado do Exercício, Demonstração das Mutações do Patrimônio Líquido, Demonstração dos Fluxos de Caixa do Período e Notas Explicativas.*

9.1.3.2.2 No caso de empresa constituída no exercício social vigente, admite-se a apresentação de Balanço Patrimonial e Demonstrações Contábeis referentes ao período de existência da sociedade;

9.1.3.2.3 O Balanço Patrimonial e as Demonstrações Contábeis, acompanhados dos respectivos Termos de Abertura e de Encerramentos, deverão estar assinados por representante legal da empresa e pelo profissional de Contabilidade, devidamente registrado no Conselho Regional de Contabilidade.

9.1.3.2.4 O Balanço e as Demonstrações Contábeis deverão estar registrados ou na Junta Comercial ou no Registro Civil das Pessoas Jurídicas ou no Sistema Público de Escrituração Digital – SPED (Decreto nº 8.683/2016), para as empresas que utilizam o sistema eletrônico de escrituração.

9.1.3.2.5 É admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

9.1.3.2.6 Caso o licitante seja cooperativa, tais documentos deverão ser acompanhados da última auditoria contábil-financeira, conforme dispõe o artigo 112 da Lei nº 5.764, de 1971, ou de uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

9.1.3.2.7 Será obtida a Comprovação da boa situação financeira da empresa mediante obtenção de índices de **Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC)**, superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

I. *Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante);*

II. *Solvência Geral (SG) = (Ativo Total) / (Passivo Circulante + Passivo não Circulante); e*

III. *Liquidez Corrente (LC) = (Ativo Circulante) / (Passivo Circulante).*

9.1.3.2.8 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.

9.1.3.2.9 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.

9.1.3.2.10 Será exigido para fins de habilitação capital social ou patrimônio líquido mínimo de 10% do valor total estimado da contratação, na forma do art. 69, § 4º da Lei nº 14.133/2021.

9.1.3.2.11 O atendimento dos índices econômicos previstos para comprovação da qualificação econômico-financeira da empresa, citados nos subitens 9.1.3.2.7 e 9.1.3.2.9 deverá ser atestado

mediante Declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

9.1.4. Qualificação Técnica

9.1.4.1 Comprovar qualificação técnica, conforme exigência no item 8.3 e subitens do termo de referência, anexo I do Edital.

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

9.3 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.

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

9.5 Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

9.5.1 Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o TR exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de **10%** para o consórcio em relação ao valor exigido para os LICITANTES individuais.

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

9.7 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.

9.8 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.

9.9 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.

9.10 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.

9.11 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.

9.11.1 O LICITANTE que optar por realizar vistoria prévia terá disponibilizado pela Administração data e horário exclusivos, a ser agendado através do e-mail ca.iterpa@gmail.com, de modo que seu agendamento não coincida com o agendamento de outros LICITANTES.

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

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

9.12.1 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. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

9.12.2 É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicafe e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN nº 3/2018, art. 7º, caput).

9.12.3 A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. (IN nº 3/2018, art. 7º, parágrafo único).

9.13 A verificação em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões pelo PREGOEIRO constitui prova para fins de habilitação.

9.14 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 horas**, prorrogável por igual período, contado da solicitação do PREGOEIRO.

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

9.15.1 Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

9.15.2 Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

9.16 Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em diligência para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

- 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.
- c. A vedação à inclusão de novo documento, prevista no art. 64 da Lei 14.133/2021, não alcança documento ausente, comprobatório de condição atendida pelo licitante quando apresentou sua proposta, que não foi juntado com os demais comprovantes de habilitação e/ou da proposta, por equívoco ou falha, o qual deverá ser solicitado e avaliado pelo pregoeiro (ACÓRDÃO Nº 1211/2021 – TCU – Plenário).

9.17 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.

9.18 Se o LICITANTE não atender às exigências para habilitação, o PREGOEIRO 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 9.14](#).

9.19 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.

9.20 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.

CLÁUSULA 10

Adjudicação e homologação

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

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

CLÁUSULA 11

Recursos

11.1 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.

11.2 O prazo recursal é de **3 dias úteis**, contados da data da notificação da decisão a ser recorrida ou de lavratura da ata.

11.3 Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do LICITANTE, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

- a.** A intenção de recorrer deverá ser manifestada imediatamente, sob pena de não ser possível apresentar o recurso; e
- b.** o prazo para a manifestação da intenção de recorrer não será inferior a **10 (dez) minutos**;
- 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.

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

11.5 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 dias úteis**; ou
- b.** Encaminhar o recurso, no prazo de **3 dias úteis**, para a autoridade superior, que deverá decidi-lo no prazo de **10 dias úteis**, contado do recebimento dos autos.

11.6 Os recursos apresentados fora do prazo não serão conhecidos.

11.7 O prazo para apresentação de contrarrazões ao recurso pelos demais LICITANTES será de **3 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.

11.8 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.

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

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

CLÁUSULA 12

Contratação

12.1 Após a homologação e adjudicação, caso se conclua pela contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

12.2 O adjudicatário terá o prazo de **06 (seis) dias úteis**, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste edital.

12.3 Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato, a Administração poderá encaminhá-lo para assinatura, mediante

correspondência postal com aviso de recebimento (AR), disponibilização de acesso à sistema de processo eletrônico para esse fim ou outro meio eletrônico, para que seja assinado e devolvido no prazo de 06 (seis) dias úteis, a contar da data de seu recebimento ou da disponibilização do acesso ao sistema de processo eletrônico.

12.4 O Aceite da Nota de Empenho ou do instrumento equivalente, emitida ao fornecedor adjudicado, implica o reconhecimento de que:

12.4.1 referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 14.133, de 2021;

12.4.2 a contratada se vincula à sua proposta e às previsões contidas neste Edital;

12.4.3 a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 137 e 138 da Lei nº 14.133, de 2021 e reconhece os direitos da Administração previstos nos artigos 137 a 139 da mesma Lei.

12.5 Os prazos dos itens 12.2. e 12.3 poderão ser prorrogados, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

12.6 O prazo de vigência da contratação é o estabelecido no Termo de Referência.

12.7 Na assinatura do contrato ou do instrumento equivalente será exigida a comprovação das condições de habilitação e contratação consignadas neste aviso, que deverão ser mantidas pelo fornecedor durante a vigência do contrato.

12.8 Quando o adjudicatário optar pela oferta de seguro-garantia, deverá fazê-lo previamente à assinatura do contrato, no prazo máximo de 30 dias corridos, contado da data de homologação da licitação (art. 96, §3º, da Lei n.º 14.133/2021) devendo indicar essa opção já na proposta financeira.

12.9 Administração poderá, quando a convocada não assinar o Contrato ou não retirar a nota de empenho no prazo e condições estabelecidos, convocar demais licitantes, segundo a ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pela primeira classificada, inclusive de preços, assinar o contrato, sem prejuízo das multas previstas em Ato Convocatório e no contrato e das demais cominações legais.

CLÁUSULA 13

Infrações e sanções administrativas

13.1 Constituem infrações administrativas do LICITANTE a serem punidas com as seguintes sanções:

Infração	Penalidade
a. Deixar de entregar a documentação exigida para a licitação ou não entregar qualquer documento que tenha sido solicitado pelo PREGOEIRO durante o certame;	Multa 0,5% a 15% do valor do contrato licitado.

b. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta, em especial quando:

1. Não enviar a proposta adequada ao último lance ofertado ou após a negociação;
2. Recusar-se a enviar o detalhamento da proposta quando exigível;
3. Pedir para ser desclassificado quando encerrada a etapa competitiva;
4. Deixar de apresentar amostra;
5. Apresentar proposta ou amostra em desacordo com as especificações do edital;

c. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

d. Recusar-se, sem justificativa, a assinar o contrato, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

e. Apresentar declaração ou documentação falsa ou prestar declaração falsa durante a licitação;

f. Fraudar a licitação;

g. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

1. Agir em conluio ou contra a lei;
2. Induzir deliberadamente a erro no julgamento;
3. Apresentar amostra falsificada ou deteriorada;

h. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

i. Praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846/13.

e

Impedimento de licitar e contratar*

* Exceto quando se justificar a imposição de penalidade mais grave, ocasião em que poderá ser aplicada a sanção de “*Declaração de inidoneidade para licitar e contratar*”.

Multa

15% a 30% do valor do contrato licitado.

e

Declaração de inidoneidade para licitar e contratar

13.2 As sanções somente poderão ser aplicadas após o contraditório e ampla defesa do LICITANTE ou adjudicatário.

13.3. As sanções previstas no [item 13.1](#) não excluem as responsabilidades civil e criminal dos envolvidos.

13.4 Na aplicação das sanções serão considerados:

- a.* A natureza e a gravidade da infração cometida.
- b.* As peculiaridades do caso concreto.
- c.* As circunstâncias agravantes ou atenuantes.
- d.* Os danos que dela provierem para a Administração Pública.
- e.* A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

13.5 A multa será de **0,5% a 30%** incidente sobre o valor do contrato licitado, recolhida no **prazo máximo de 15 (quinze) dias úteis**, a contar da comunicação oficial.

13.5.1 Para as infrações previstas nas [alíneas a, b, c e d do item 13.1](#), a multa será de 0,5% a 15% do valor do contrato licitado.

13.5.2 Para as infrações previstas nas [alíneas e, f, g, h e i do item 13.1](#), a multa será de 15% a 30% do valor do contrato licitado.

13.6 As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas cumulativamente ou não com a penalidade de multa.

13.7 Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de **15 dias úteis**, contado da data de sua intimação.

13.8 A sanção de impedimento de licitar e contratar impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do Estado do Pará. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas as [alíneas a, b, c e d do item 13.1](#), quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do Estado do Pará, pelo prazo máximo de **3 (três) anos**.

13.9 Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nas [alíneas e, f, g, h e i do item 13.1](#), bem como pelas infrações administrativas previstas nas [alíneas a, b, c e d do item 13.1](#) que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, § 5º, da Lei n.º 14.133, de 2021.

13.10 A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração descrita na [alínea c e d do item 13.1](#), caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do PROMOTOR.

13.11 A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o LICITANTE ou o adjudicatário para, no prazo de **15 dias úteis**, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

13.12 Da aplicação das sanções multa e impedimento de licitar e contratar, caberá recurso no prazo de **15 dias úteis** observado o seguinte:

- a.** O prazo para recorrer se inicia na data da intimação;
- b.** O recurso será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de **5 dias úteis**, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de **20 dias úteis**, contado do recebimento dos autos.

13.13 Da aplicação da sanção de declaração de inidoneidade para licitar ou contratar, caberá a pedido de reconsideração no prazo de **15 dias úteis**, contado da data da intimação.

13.14 O recurso a que se refere o [item 13.13](#) deverá ser decidido no prazo máximo de **20 dias úteis**, contado do seu recebimento.

13.15 O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que a autoridade competente decida sobre ele.

13.16 A aplicação das sanções previstas neste edital não exclui a obrigação de reparação integral dos danos causados.

CLÁUSULA 14

Impugnação ao edital

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

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

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

14.4 A impugnação e a solicitação de esclarecimento poderão ser realizadas por meio eletrônico, por meio do e-mail: ca.iterpa@gmail.com.

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

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

14.7 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 Dec. Estadual nº 2.940, de 2023.

CLÁUSULA 15

Disposições finais

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

15.2 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, pelo PREGOEIRO.

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

15.4 A homologação do resultado desta licitação não implicará direito à contratação.

15.5 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.

15.6 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.

15.7 Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento.

15.8 Só se iniciam e vencem os prazos em dias de expediente na Administração.

15.9 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.

15.10 Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerão as deste Edital.

15.11 O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas e no Portal ComprasPará.

15.12 Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

ANEXO I – Termo de Referência

Apêndice I - Especificações Técnicas

Apêndice II - Planilha de Itens e Quantitativos

Apêndice III - Memória de Cálculo da Pesquisa de Preços

Apêndice IV - Justificativa da Pesquisa de Preços

Apêndice V - Modelo de Termo de Vistoria

Apêndice VI - Modelo de Termo de Dispensa de Vistoria

Apêndice VII - Termo de Confidencialidade e Sigilo

Apêndice VIII - Modelo de Declaração de Conformidade Técnica (DCT)

ANEXO II - Estudo Técnico Preliminar (ETP)

Apêndice I – Referências de Preços e Fonte de Consulta

Apêndice II – Memória de Cálculo

ANEXO III - Modelo de Declaração de Índices de Liquidez

ANEXO IV - Declaração de Não Ocorrência de Registro de Oportunidade

ANEXO V - Minuta de Termo de Contrato

Cidade (PA), 30 de setembro de 2026.

FLAVIO RICARDO

ALBUQUERQUE

AZEVEDO:7278112222

0

FLÁVIO RICARDO ALBUQUERQUE AZEVEDO

PRESIDENTE DO ITERPA

Assinado de forma digital por
FLAVIO RICARDO ALBUQUERQUE
AZEVEDO:72781122220
Dados: 2026.09.30 11:40:42 -03'00'

ANEXO I

TERMO DE REFERÊNCIA Nº 003/2026 – ITERPA

CONTRATAÇÃO DE SOLUÇÃO INTEGRADA DE SEGURANÇA DE REDE

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Objeto

Constitui objeto deste Termo de Referência a contratação de empresa especializada para o fornecimento de solução integrada de segurança de rede, abrangendo a entrega, a instalação, a configuração, a integração e a operação dos equipamentos a seguir, acompanhada do serviço continuado de detecção e resposta a ameaças nos computadores e servidores do Instituto de Terras do Pará – ITERPA, em conformidade com o Estudo Técnico Preliminar nº 003/2026-ITERPA e com o Documento de Formalização da Demanda integrante do Processo nº 2026/2933349.

A solução compreende os seguintes componentes:

- a) firewall de próxima geração (NGFW), em arranjo de alta disponibilidade, com os dois equipamentos ativos simultaneamente;
- b) comutadores de acesso de 48 portas Gigabit, com alimentação elétrica integrada pelo cabo de rede (PoE+);
- c) comutadores de núcleo de 24 portas de fibra óptica, em arquitetura redundante;
- d) pontos de acesso sem fio do padrão Wi-Fi 6 (IEEE 802.11ax), com gerenciamento centralizado;
- e) serviço continuado de detecção e resposta a ameaças (EDR) nos computadores e servidores conectados à rede, em regime ininterrupto.

Os componentes formam sistema único e integrado e serão adjudicados em lote único, pelo critério de menor preço global, em conformidade com a justificativa de não parcelamento constante do item 8 do ETP nº 003/2026-ITERPA e com o art. 40, §§ 2º e 3º, da Lei nº 14.133/2021.

1.2. Natureza do objeto e vigência contratual

A contratação caracteriza-se como prestação de bem e serviço de natureza continuada, na forma do art. 6º, XV, da Lei nº 14.133/2021, com vigência inicial de 36 (trinta e seis) meses, contados da assinatura do contrato, prorrogáveis por períodos sucessivos, observado o limite decenal previsto no art. 107 da mesma Lei, desde que mantidas a vantajosidade econômica e a adequada execução contratual.

A natureza continuada da contratação decorre da indispensabilidade da proteção cibernética à prestação dos serviços finalísticos do ITERPA, cuja interrupção comprometeria, de forma imediata, a operação do Sistema de Cadastro Rural e Fundiário – SICARF, dos bancos de dados corporativos e dos demais sistemas informatizados essenciais à execução da política fundiária estadual.

1.3. Justificativa para não aplicação do tratamento diferenciado a ME/EPP

Instituto de Terras do Pará - ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951

CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com

Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

Nos termos do art. 4º, § 1º, I, da Lei nº 14.133/2021, da Lei Complementar nº 123/2006 (arts. 42 a 49) e da Lei Estadual nº 8.417, de 7 de novembro de 2016 – Estatuto Paraense da Microempresa e Empresa de Pequeno Porte –, não se aplicará à presente contratação o tratamento diferenciado e simplificado previsto nas referidas normas.

A vedação fundamenta-se em três ordens de razões. Primeira, **o valor global estimado de R\$ 6.021.958,62** supera o teto de receita bruta admitido para o enquadramento como empresa de pequeno porte na forma do art. 3º, II, da Lei Complementar nº 123/2006 e do art. 2º, II, da Lei Estadual nº 8.417/2016. Segunda, o caráter técnico-operacional do objeto – fornecimento integrado de solução de segurança de rede em arranjo de alta disponibilidade, com equipe certificada por fabricante para os componentes críticos da solução e atendimento em regime ininterrupto pelo prazo de 36 meses – demanda capacidade técnica e operacional incompatível com o porte das microempresas e das empresas de pequeno porte. Terceira, a fragmentação do objeto, para fins de tratamento diferenciado, importaria desnaturação da solução integrada justificada no item 8 do ETP nº 003/2026-ITERPA, com risco à interoperabilidade dos componentes e à unicidade da responsabilização contratual.

Não obstante a vedação acima, observar-se-ão os benefícios não dependentes de enquadramento por porte, em especial o tratamento favorecido às microempresas e empresas de pequeno porte sediadas no Estado do Pará nos termos do art. 8º da Lei Estadual nº 8.417/2016, quando aplicáveis a etapas específicas do procedimento.

1.4. Especificação conforme catálogo (SIMAS)

Os componentes do objeto serão indicados, sempre que houver registro compatível, conforme o catálogo do Sistema de Materiais e Serviços – SIMAS, mantido pela Administração Pública Estadual. A indicação dos códigos correspondentes integra a Planilha de Itens e Quantitativos (Apêndice II).

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. Remissão ao Estudo Técnico Preliminar

A fundamentação pormenorizada da contratação consta do Estudo Técnico Preliminar nº 003/2026-ITERPA, elaborado pelo Núcleo de Tecnologia da Informação – NTI, nos termos do art. 6º, XX, e do art. 18, § 1º, da Lei nº 14.133/2021, do art. 3º, II, do Decreto Estadual nº 2.939/2023 e da Instrução Normativa SEGES/ME nº 58/2022, aplicada subsidiariamente. O ETP integra os autos como parte da fase preparatória da contratação, sendo seus fundamentos técnico, econômico e jurídico incorporados, por remissão, a este Termo de Referência.

2.2. Descrição da necessidade

O Instituto de Terras do Pará – ITERPA é autarquia estadual responsável pela execução da política fundiária do Estado, com atribuições ampliadas pela Lei Estadual nº 8.878/2019, que lhe conferiu competência para atuar na Regularização Fundiária Urbana – REURB. A prestação desse

serviço depende, de forma indissociável, da existência de infraestrutura tecnológica protegida, apta a suportar o SICARF, os bancos de dados corporativos, as aplicações de geoprocessamento e os demais sistemas informatizados da autarquia.

O Contrato nº 08/2020, que assegurava os serviços de segurança da informação do ITERPA, encerrou sua vigência em abril de 2025, ao atingir o limite temporal máximo então aplicável, sem possibilidade de nova prorrogação. Desde então, a instituição opera em situação de descobertura cibernética progressiva.

Registra-se, neste ponto, o histórico de tentativas de equacionamento da demanda. O projeto de segurança da informação do ITERPA foi originalmente elaborado de forma abrangente, com o propósito de proteger, em arquitetura unificada, os ativos digitais, os dados sensíveis e os sistemas críticos da instituição, implementando controles de segurança eficazes para assegurar a confidencialidade, a integridade e a disponibilidade das informações, e ponderando a escalabilidade dos processos de regularização fundiária do SICARF e o crescimento do volume de dados que transitam na rede computacional do Instituto. Tal projeto, contudo, não logrou ser licitado, por restrições orçamentárias e financeiras supervenientes ao planejamento.

Em razão dessa impossibilidade, e diante do encerramento do Contrato nº 08/2020, a Administração viabilizou contratação emergencial, com fundamento no art. 75, VIII, da Lei nº 14.133/2021, pelo prazo de doze meses e no valor estimado de R\$ 2.656.276,77, com o exclusivo propósito de manter, em padrões mínimos e pelo período estritamente necessário, os mesmos serviços anteriormente compreendidos no contrato encerrado, evitando que o Instituto permanecesse totalmente descoberto de proteção cibernética. A medida emergencial tem, portanto, natureza de contenção: dirige-se a interromper o estado de descobertura enquanto se conclui o planejamento estruturante.

A presente contratação possui natureza diversa. Não substitui a emergencial nem com ela se confunde. Volta-se à recomposição definitiva da arquitetura de segurança de rede do Instituto, com solução integrada – firewall de próxima geração, switches PoE e de fibra, pontos de acesso Wi-Fi 6 e serviço continuado de EDR –, dimensionada para o triênio e ajustada à atual realidade orçamentária do ITERPA. Trata-se da segunda iteração do planejamento original, redesenhada para conciliar a integralidade da proteção pretendida com a capacidade financeira efetiva do órgão, em prevenção à perpetuação de soluções de contingência cujo custo total de propriedade cresce de modo desproporcional ao benefício.

2.3. Justificativa técnica e econômica da solução

A opção pela contratação de solução integrada, com fornecedor único, decorre das análises desenvolvidas no item 5 do ETP nº 003/2026-ITERPA, que avaliou quatro alternativas (renovação isolada das licenças do parque atual; aquisição fragmentada de cada componente junto a fabricantes distintos; solução integrada de fornecedor único; e contratação de proteção cibernética como serviço em

nuvem). A solução integrada foi identificada como a economicamente mais vantajosa e tecnicamente adequada, pelas seguintes razões:

- a) economia de aproximadamente 16% em relação à aquisição fragmentada e de 28% em relação à contratação em nuvem, no horizonte de 36 meses, com diluição do investimento e estabilização do fluxo orçamentário;
- b) preservação da soberania dos dados sob custódia do Instituto, que permanecem em equipamentos instalados em suas dependências;
- c) responsabilização contratual unificada, com ponto único de contato para níveis de serviço, suporte e gestão de incidentes;
- d) atualidade tecnológica da proteção, com integração nativa entre o firewall, a rede e o serviço de detecção e resposta nos computadores e servidores, em aderência à Lei nº 13.709/2018 (LGPD).

3. DESCRIÇÃO DA SOLUÇÃO

A solução abrange o fornecimento, a instalação, a configuração e a operação de quatro grupos de componentes técnica e operacionalmente interdependentes, conforme detalhamento do Apêndice I.

3.1. Firewall de Próxima Geração (NGFW)

Dois equipamentos físicos em arranjo de alta disponibilidade, com inspeção profunda do conteúdo do tráfego, detecção e prevenção de tentativas de invasão, controle granular de aplicações por identidade do usuário, inspeção de tráfego criptografado e integração com bases de inteligência de ameaças mantidas pelo fabricante.

3.2. Comutadores de acesso e de núcleo

Vinte e cinco comutadores de acesso de 48 portas Gigabit com alimentação elétrica integrada pelo cabo de rede (PoE+) e dois comutadores de núcleo de 24 portas de fibra óptica, em arquitetura redundante, com gerenciamento centralizado e integração à console unificada da solução.

3.3. Pontos de acesso sem fio (Wi-Fi 6)

Quarenta pontos de acesso do padrão Wi-Fi 6 (IEEE 802.11ax), com gerenciamento centralizado, segmentação lógica da rede, separação entre a rede interna e a rede para visitantes, criptografia robusta e continuidade da conexão durante a mobilidade dentro do ambiente.

3.4. Serviço continuado de detecção e resposta nos computadores e servidores (EDR)

Serviço prestado em regime ininterrupto, com monitoramento contínuo dos equipamentos conectados à rede, detecção comportamental de ameaças avançadas, resposta automatizada (isolamento do equipamento comprometido, encerramento de processos maliciosos e remoção de artefatos), análise técnica pós-incidente e integração com o firewall para aplicação coordenada de bloqueios.

3.5. Serviços associados

Integram a solução o projeto executivo de implantação; o plano de transição com a contratação emergencial em curso, com operação simultânea durante a janela de migração; o treinamento da equipe técnica do NTI/ITERPA, com carga horária mínima de 40 (quarenta) horas, em conformidade com o art. 18, § 1º, X, da Lei nº 14.133/2021; a manutenção preventiva e corretiva durante toda a vigência contratual; e a operação assistida do serviço de EDR.

3.6. Ciclo de vida do objeto

O ciclo de vida compreende as fases de planejamento, implantação, operação contínua, manutenção, atualização tecnológica e descomissionamento. A vida útil estimada dos equipamentos físicos é de 60 (sessenta) meses; o suporte e a garantia, de 36 (trinta e seis) meses, foram dimensionados em coerência com a depreciação técnica e o ciclo de inovação do segmento. Ao término da vigência, os equipamentos substituídos serão objeto de logística reversa pela contratada, na forma do item 4.6.3 deste Termo de Referência.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos gerais

A contratada assumirá integralmente a responsabilidade pela disponibilidade da solução, compreendendo equipamentos, programas, manutenção preventiva programada, manutenção corretiva e atualização dos itens fornecidos, durante toda a vigência contratual. Responderá, ainda, pelos prejuízos decorrentes de indisponibilidade causada por ações praticadas em desacordo com as normas técnicas e com os critérios definidos neste Termo de Referência.

Todos os materiais auxiliares necessários à execução dos serviços serão fornecidos pela contratada, devendo seus empregados portar crachá de identificação e uniforme, e observar os regulamentos de disciplina, segurança e medicina do trabalho aplicáveis às dependências do ITERPA.

4.2. Requisitos técnicos específicos

As especificações técnicas detalhadas de cada componente constam do Apêndice I deste Termo de Referência. Sem prejuízo delas, a contratada deverá:

- a) elaborar e entregar projeto executivo descrevendo a forma de implantação e manutenção da solução, no prazo de até 15 (quinze) dias da emissão da Ordem de Serviço;
- b) fornecer e instalar a totalidade dos equipamentos descritos no Apêndice I, novos, em linha de produção e fabricação, com embalagem original de fábrica lacrada;
- c) executar o plano de transição com a contratação emergencial em curso, com operação simultânea das duas soluções durante a janela de migração e procedimentos de retorno seguro à configuração anterior em caso de falha;

- d) prover gerenciamento da solução, com substituição presencial de peças, atualização de programas, supervisão remota, suporte e manutenção durante toda a vigência contratual;
- e) disponibilizar ao ITERPA acesso de leitura aos painéis e relatórios da console de gerenciamento e da plataforma de EDR, sem custo adicional de licenciamento para os usuários da contratante.

4.3. Requisitos de suporte técnico, manutenção e garantia

O suporte técnico e a garantia da solução vigorarão durante todo o período contratual, observados os seguintes requisitos:

- a) as intervenções de manutenção observarão as normas técnicas aplicáveis e preservarão as características de funcionamento dos equipamentos;
- b) semestralmente, será entregue Calendário de Manutenção Preventiva com a respectiva programação;
- c) mensalmente, será apresentado Relatório de Manutenção contendo os serviços realizados;
- d) a manutenção e a atualização dos componentes serão realizadas durante toda a vigência contratual, sem acréscimo de custo ao ITERPA;
- e) a garantia será do tipo presencial, com substituição de peças em até 72 (setenta e duas) horas úteis após a notificação, admitida a manutenção de estoque de peças sobressalentes nas dependências do ITERPA para agilização logística, em razão das peculiaridades de deslocamento do Estado do Pará.

4.4. Requisitos de segurança da informação e proteção de dados pessoais

Em observância à Lei nº 13.709/2018 (LGPD), em particular ao seu art. 46, e aos parâmetros técnicos definidos no item 3.1.5 do ETP nº 003/2026-ITERPA, a contratada deverá assegurar:

- a) criptografia robusta para os dados em repouso (padrão AES-256 ou superior) e em trânsito (protocolo TLS 1.2 ou superior);
- b) autenticação em dois fatores para o acesso administrativo, com registro de eventos de auditoria mantidos pelo prazo mínimo de 12 (doze) meses;
- c) gestão de vulnerabilidades, com varreduras periódicas e aplicação tempestiva de correções críticas;
- d) plano de resposta a incidentes cibernéticos, com comunicação ao ITERPA em até 24 (vinte e quatro) horas da detecção de evento relevante;
- e) adoção de medidas técnicas e administrativas para a proteção de dados pessoais tratados durante a execução contratual, na forma dos arts. 46 a 49 da LGPD.

A contratada atuará, conforme o caso, como operadora dos dados pessoais tratados por conta do ITERPA, observadas as obrigações próprias dessa condição, em especial o dever de sigilo, a vedação de

tratamento para finalidade diversa daquela contratada e a obrigação de eliminação dos dados ao término da vigência, salvo hipóteses legais de retenção.

4.5. Reversibilidade e portabilidade dos dados e configurações

Ao término da vigência contratual, a contratada deverá entregar ao ITERPA, em formatos abertos e não proprietários, as configurações, políticas, registros de eventos e bases de inteligência específicas do Instituto, sem custos adicionais, em prevenção ao aprisionamento tecnológico, em conformidade com a orientação firmada pelo Tribunal de Contas da União no Acórdão nº 1.739/2015-Plenário.

4.6. Sustentabilidade ambiental, social e econômica

A contratação observará os critérios de sustentabilidade estabelecidos no art. 18, § 1º, XII, da Lei nº 14.133/2021, no Decreto Estadual nº 4.193/2024 (arts. 14 a 17), no Guia Nacional de Contratações Sustentáveis da AGU (7ª edição, 2024), na Instrução Normativa SGD/ME nº 94/2022 (art. 16, I, “g”) e na Portaria SGD/MGI nº 2.751/2023, além do item 12 do ETP, compreendendo:

4.6.1. Segurança, compatibilidade eletromagnética e eficiência energética

Os equipamentos utilizados na execução dos serviços apresentarão segurança, compatibilidade eletromagnética e eficiência energética equivalentes às exigidas pela Portaria INMETRO nº 170, de 10 de abril de 2012, para os Bens de Informática. Por se tratar de certificação voluntária, admitir-se-á a comprovação por certificado do fabricante, laudo pericial emitido por entidade técnica independente ou qualquer outro meio idôneo, na forma do art. 5º, § 1º, da Instrução Normativa SLTI/MPOG nº 01/2010 e do art. 42, § 1º, da Lei nº 14.133/2021.

4.6.2. Substâncias perigosas – Diretiva RoHS

Os equipamentos não conterão substâncias perigosas em concentração superior aos limites fixados pela diretiva RoHS, a saber: mercúrio, chumbo, cromo hexavalente, cádmio, bifenilas polibromadas (PBBs) e éteres difenílicos polibromados (PBDEs), em conformidade com o art. 5º, IV, da IN SLTI/MPOG nº 01/2010. A comprovação poderá ser feita por certificação emitida por instituição pública oficial ou credenciada, ou por qualquer outro meio idôneo de prova.

4.6.3. Logística reversa dos equipamentos substituídos

Os equipamentos do parque legado, substituídos em razão desta contratação, terão destinação ambientalmente adequada, em conformidade com a Lei nº 12.305/2010 (Política Nacional de Resíduos Sólidos), com o Decreto nº 10.936/2022, com o Decreto nº 10.240/2020 e com a IN SLTI/MPOG nº 01/2010. Caberá à contratada o recolhimento e o encaminhamento dos equipamentos a entidades recicladoras credenciadas, com apresentação semestral de declaração quanto à destinação dos componentes substituídos durante a execução contratual.

4.6.4. Cadastro Técnico Federal de Atividades Potencialmente Poluidoras (CTF/APP)

A contratada comprovará, mediante certidão negativa ou regular, que os fabricantes dos equipamentos ofertados encontram-se regularmente inscritos no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais – CTF/APP, instituído pela Lei nº 6.938/1981 e regulamentado pela IN IBAMA nº 06/2013, conforme orientação do Guia Nacional de Contratações Sustentáveis da AGU.

4.6.5. Conformidade da proposta e homologação

A conformidade dos equipamentos ofertados com os critérios de sustentabilidade será verificada na fase de aceitação da proposta. Os custos indiretos relativos ao ciclo de vida do produto (manutenção, consumo energético e descarte) integram a análise de vantajosidade da contratação, em conformidade com o art. 144 da Lei nº 14.133/2021.

4.7. Indicação de marca por compatibilidade com plataformas e padrões já adotados

4.7.1. Fundamento e delimitação da hipótese

A regra geral na definição do objeto é a descrição objetiva, sem indicação de marca, em decorrência dos princípios da isonomia e da competitividade do art. 5º da Lei nº 14.133/2021 e da vedação do art. 9º, I, "a", do mesmo diploma. Excepcionalmente, o art. 41, I, admite que a Administração indique uma ou mais marcas ou modelos, mediante justificativa formal.

Nos termos do art. 41, I, alínea "b", da Lei nº 14.133/2021, a indicação de marca constante deste Termo de Referência funda-se exclusivamente na necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração.

Cumprir observar que não se invoca, nesta contratação, a hipótese da alínea "a" do mesmo inciso. O Instituto não instaurou o processo de padronização de que trata o art. 43 da Lei nº 14.133/2021, e a indicação de marca ora estabelecida não decorre de padronização, não produz seus efeitos e não substitui aquele procedimento.

4.7.2. Elementos de fato que caracterizam a compatibilidade

A plataforma de segurança de rede em operação no ITERPA é da marca Fortinet, adotada durante toda a vigência do Contrato nº 08/2020 e mantida na contratação emergencial em curso, fundada no art. 75, VIII, da Lei nº 14.133/2021. Dessa adoção decorrem os seguintes elementos:

a) ativos remanescentes em operação, compreendidos os dois firewalls FortiGate 500e, que permanecerão em uso durante a janela de transição e cuja interoperabilidade nativa com a nova solução é condição de continuidade da proteção;

b) políticas de segurança consolidadas, construídas ao longo da vigência contratual e diretamente portáteis entre equipamentos da mesma plataforma, cuja reconstrução em tecnologia distinta demandaria reparametrização integral do perímetro;

c) integrações em produção com os sistemas finalísticos do Instituto, notadamente com o Sistema de Cadastro Rural e Fundiário (SICARF);

d) capacitação da equipe técnica do Núcleo de Tecnologia da Informação na operação da plataforma;

e) coexistência obrigatória com a contratação emergencial em curso durante o período de migração, previsto no plano de transição do item 10 do Estudo Técnico Preliminar nº 003/2026-ITERPA, que pressupõe operação simultânea das duas soluções.

4.7.3. Caráter referencial da indicação

A indicação de marca prevista neste item possui caráter exclusivamente referencial e não implica exclusividade. Será admitida a oferta de solução de qualquer outro fabricante, desde que a licitante demonstre equivalência técnica e funcional integral com os requisitos do Apêndice I deste Termo de Referência, na forma do art. 42, I a III, da Lei nº 14.133/2021.

Vale ressaltar que a equivalência será aferida em relação aos requisitos do Apêndice I, e não em relação a características proprietárias da marca indicada. Nenhum requisito do Apêndice I poderá ser interpretado de modo a exigir atributo que apenas a marca de referência possua.

4.7.4. Critérios objetivos de aferição da matriz de equivalência

A demonstração de equivalência far-se-á por meio da Declaração de Conformidade Técnica constante do Apêndice VIII, apresentada com a proposta, observados os seguintes critérios objetivos de aferição:

a) **unidade de aferição.** Cada requisito do Apêndice I constitui unidade autônoma de aferição, transcrita integralmente na matriz, vedado o agrupamento de requisitos em declaração única;

b) **meio de prova admitido.** O atendimento será comprovado por ficha técnica do fabricante, manual técnico, certificação, laudo de instituição independente ou documento similar, na forma do art. 42, I a III, da Lei nº 14.133/2021, com indicação da página exata do documento em que a característica se encontra descrita. Declaração da própria licitante, desacompanhada de documento do fabricante, não constitui meio de prova suficiente;

c) **regra de decisão.** O requisito será considerado atendido quando a documentação comprovar característica igual ou superior à exigida. Característica inferior, ou não localizável no documento indicado, importa não atendimento;

d) **requisitos de desempenho.** Nos requisitos expressos em grandeza mensurável, a aferição far-se-á pelo valor nominal declarado pelo fabricante para a configuração ofertada, vedada a extrapolação a partir de modelos diversos da mesma linha;

e) **requisitos de integração.** Nos requisitos de integração entre componentes, a aferição far-se-á pela demonstração de que a funcionalidade opera de modo nativo na solução ofertada, sem desenvolvimento específico, sem intermediação de terceiros e sem custo adicional;

f) **diligência.** O Instituto poderá, a qualquer tempo, promover diligência junto ao fabricante da solução ofertada para confirmação das características declaradas, na forma do art. 64 da Lei nº 14.133/2021;

g) **consequência.** O não atendimento de qualquer requisito do Apêndice I acarreta a desclassificação da proposta, na forma do item 8.6, "b", deste Termo de Referência, assegurado o contraditório prévio.

4.8. Exigência de amostra

Não será exigida a apresentação de amostra. A verificação de conformidade técnica será realizada por meio da documentação técnica exigida no item 8.5 deste Termo de Referência e, quando necessário, por diligência durante a fase de aceitação da proposta.

4.9. Subcontratação

Admite-se a subcontratação parcial do objeto, limitada a 30% (trinta por cento) do valor total do contrato, exclusivamente para os serviços de operação assistida do EDR e manutenção preventiva de equipamentos, na forma do art. 122, caput e § 2º, da Lei nº 14.133/2021. A subcontratação depende de autorização prévia do ITERPA, mediante apresentação da documentação de qualificação da subcontratada, e não exime a contratada da integral responsabilidade pela execução do objeto.

4.10. Vedação de participação em consórcio

Não se admitirá a participação de empresas em consórcio, por se tratar de objeto ofertado de forma usual no mercado de soluções integradas de segurança de rede, circunstância que afasta a necessidade de agregação de competências de diferentes empresas. A vedação fundamenta-se no art. 15 da Lei nº 14.133/2021 e no art. 40, § 3º, II, do mesmo diploma.

4.11. Garantia contratual

Será exigida garantia contratual correspondente a 5% (cinco por cento) do valor atualizado do contrato, em uma das modalidades previstas no art. 96, § 1º, da Lei nº 14.133/2021, a critério da contratada, a ser apresentada no prazo de até 10 (dez) dias úteis contados da assinatura do contrato.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. Local da prestação dos serviços

Os serviços de instalação e os equipamentos serão entregues e operados na Sede do ITERPA, na Rodovia Augusto Montenegro, s/nº, Km 09, Parque Guajará, Icoaraci, CEP 66.821-000, Belém/PA,

e nas unidades regionais do Instituto, conforme cronograma de implantação. O serviço de detecção e resposta a ameaças será prestado remotamente, a partir do centro de operações de segurança da contratada, com integração à infraestrutura local.

5.2. Fases da execução e cronograma físico

A execução observará as seguintes fases:

Fase 1 – Planejamento e Projeto Executivo: até 15 (quinze) dias úteis da emissão da Ordem de Serviço, para elaboração e aprovação do Projeto Executivo pelo NTI/ITERPA, incluindo o Plano de Transição com a contratação emergencial em curso.

Fase 2 – Fornecimento e Instalação: até 60 (sessenta) dias úteis da aprovação do Projeto Executivo, para entrega, instalação e configuração de firewalls, comutadores e pontos de acesso, na Sede.

Fase 3 – Implantação do Serviço de EDR: até 30 (trinta) dias úteis da conclusão da Fase 2, para licenciamento, instalação dos agentes em todos os computadores e servidores e validação da integração com o firewall.

Fase 4 – Testes e Validação: até 15 (quinze) dias úteis da conclusão da Fase 3, para realização de testes de funcionalidade, integridade da rede, desempenho e adequação dos controles de segurança.

Fase 5 – Treinamento: concomitante às Fases 3 e 4, com carga horária mínima de 40 (quarenta) horas, em temas de gerenciamento, monitoramento e resposta a incidentes, em atendimento ao art. 18, § 1º, X, da Lei nº 14.133/2021.

Fase 6 – Operação Assistida: 30 (trinta) dias após a conclusão da implantação, para acompanhamento e suporte técnico contínuo até a estabilização do ambiente.

Fase 7 – Operação Plena e Monitoramento Ininterrupto: pelo período remanescente do contrato, com operação regular, monitoramento contínuo, manutenção preventiva e corretiva, e suporte técnico conforme os níveis de serviço pactuados.

5.3. Prazo total de implantação

A contratada concluirá a implantação integral da solução (Fases 1 a 5) no prazo máximo de 120 (cento e vinte) dias úteis, contados da emissão da Ordem de Serviço pelo NTI/ITERPA, observado o cronograma físico do item 5.2. A extrapolação do prazo sujeitará a contratada às sanções previstas neste Termo de Referência.

5.4. Recebimento provisório e definitivo

O recebimento do objeto observará o disposto no art. 140 da Lei nº 14.133/2021, nos seguintes termos:

- a) recebimento provisório – ao término de cada fase de implantação, pelo fiscal técnico, mediante Termo de Recebimento Provisório, no prazo de até 10 (dez) dias úteis após a comunicação formal da contratada;
- b) recebimento definitivo – após a conclusão integral da implantação e do período de operação assistida, mediante Termo de Recebimento Definitivo, no prazo de até 15 (quinze) dias úteis após o recebimento provisório da última fase, precedido de verificação de conformidade com as especificações técnicas e operacionais pactuadas.

5.5. Transição contratual ao término

Na hipótese de encerramento do contrato sem prorrogação, a contratada executará, nos últimos 90 (noventa) dias de vigência, plano de transição apto a assegurar a continuidade dos serviços, contemplando a transferência integral das configurações, políticas e bases técnicas ao ITERPA ou à nova contratada, a entrega de documentação técnica atualizada, o suporte remoto pós-encerramento por período mínimo de 30 (trinta) dias e a destinação ambientalmente adequada dos equipamentos substituídos, na forma do item 4.6.3.

6. MODELO DE GESTÃO DO CONTRATO

O modelo de gestão descreve a forma de acompanhamento e fiscalização da execução contratual, em conformidade com o art. 6º, XXIII, alínea “F”, da Lei nº 14.133/2021 e com o Decreto Estadual nº 3.813/2024.

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei 14.133/2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial (Lei 14.133/2021, art.115, caput).

6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila. (Lei 14.133/2021, art.115, §5º)

6.3. A execução do contrato deverá ser acompanhada e fiscalizada por 1 (um) ou mais fiscais do contrato, representantes da Administração especialmente designados conforme requisitos estabelecidos no art. 7º da Lei 14.133/2021, ou pelos respectivos substitutos, permitida a contratação de terceiros para assisti-los e subsidiá-los com informações pertinentes a essa atribuição.

6.4. O fiscal do contrato anotar em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados. (Lei 14.133/2021, art.117, §1º)

6.5. O fiscal do contrato informará a seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência (Lei 14.133/2021, art.117, §2º).

6.6. O fiscal do contrato será auxiliado pelos órgãos de assessoramento jurídico e de controle interno da Administração, que deverão dirimir dúvidas e subsidiá-lo com informações relevantes para prevenir riscos na execução contratual.

6.7. O contratado será obrigado a reparar, corrigir, remover, reconstruir ou substituir, a suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes de sua execução ou de materiais nela empregados. (Lei nº 14.133/2021, Art. 119)

6.8. O contratado será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante. (Lei nº 14.133/2021, art. 121)

6.9. Somente o contratado será responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato (Lei nº 14.133/2021, art. 121, caput).

6.10. A inadimplência do contratado em relação aos encargos trabalhistas, fiscais e comerciais não transferirá à Administração a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato (Lei nº 14.133/2021, art. 121, § 1º).

6.11. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se, excepcionalmente, o uso de mensagem eletrônica para esse fim. (IN SEGES nº 98/2022).

6.12. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato. (IN SEGES nº 98/2022).

6.13. Após a assinatura do contrato ou instrumento equivalente, a fiscalização convocará o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros (IN SEGES nº 98/2022).

6.14. Antes do pagamento da nota fiscal ou da fatura, em casos excepcionais, quando por motivos alheios ao controle da CONTRATADA, uma das etapas não puder ser concluída totalmente, a CONTRATANTE poderá a seu critério determinar um pagamento parcial da etapa em questão que será complementado quando da entrega total da referida etapa.

7. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

7.1. Critérios de medição

A medição dos serviços será realizada mensalmente pelo fiscal técnico, com base nos seguintes critérios:

- a) infraestrutura de rede (firewall, comutadores e pontos de acesso) – disponibilidade mensal mínima de 99,5% (noventa e nove vírgula cinco por cento), aferida pela console de gerenciamento da contratada e validada pelo NTI/ITERPA;
- b) serviço de EDR – cobertura de 100% (cem por cento) dos computadores e servidores licenciados, com cumprimento dos prazos máximos de detecção e resposta previstos no item 4 do Apêndice I;
- c) suporte técnico – cumprimento dos prazos pactuados, por severidade de chamado, conforme item 4.2 do Apêndice I.

7.2. Procedimento de pagamento

O pagamento será efetuado mensalmente, por meio de ordem bancária, para crédito em conta indicada junto ao Banco do Estado do Pará S.A. – BANPARÁ, em conformidade com o Decreto Estadual nº 877/2008, no prazo de até 20 (vinte) dias úteis contados do atesto da nota fiscal pelo fiscal do contrato, observada a ordem cronológica de pagamentos do art. 141 da Lei nº 14.133/2021. É vedada a antecipação injustificada de pagamento, na forma do art. 145 da mesma Lei.

A nota fiscal será acompanhada de:

- a) relatório mensal de disponibilidade da infraestrutura;
- b) relatório mensal do serviço de EDR, com indicação dos incidentes detectados, respondidos e mitigados;
- c) comprovação da regularidade fiscal, social e trabalhista, mediante consulta ao SICAF ou apresentação dos documentos indicados no art. 68 da Lei nº 14.133/2021.

7.3. Glosas por descumprimento dos níveis de serviço

Na hipótese de disponibilidade mensal inferior ao índice mínimo, será aplicada glosa proporcional, sem prejuízo das sanções cabíveis, nas seguintes faixas:

- a) disponibilidade entre 99% e 99,49%: glosa de 5% (cinco por cento) sobre o valor mensal do item afetado;
- b) disponibilidade entre 97% e 98,99%: glosa de 10% (dez por cento) sobre o valor mensal do item afetado;
- c) disponibilidade inferior a 97%: glosa de 20% (vinte por cento) sobre o valor mensal do item afetado, com notificação formal para apresentação de plano de ação corretiva no prazo de até 5 (cinco) dias úteis.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

8.1. Modalidade e critério de julgamento

A contratação será realizada mediante licitação na modalidade Pregão Eletrônico, na forma do Decreto Estadual nº 2.940/2023, pelo critério de julgamento de menor preço global (lote único), com fundamento na Lei nº 14.133/2021. Não se aplica, neste caso, a obrigatoriedade do critério técnica e preço prevista no art. 36, § 1º, da Lei nº 14.133/2021, por tratar-se de bem e serviço comum cujas especificações são objetivamente verificáveis.

8.2. Modo de disputa

Adotar-se-á o modo de disputa aberto e fechado, com lances sucessivos, na forma do art. 56 da Lei nº 14.133/2021 e dos artigos 22 a 24 do Decreto Estadual nº 2.940/2023.

8.3. Qualificação técnica para habilitação

Para fins de habilitação técnica, a licitante apresentará:

- atestado(s) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, comprovando o fornecimento e a operação de solução integrada de segurança de rede em ambiente com características compatíveis com as do objeto, observado o limite de 50% (cinquenta por cento) das parcelas de maior relevância técnica, nos termos do art. 67, II e § 2º, da Lei nº 14.133/2021;
- indicação do responsável técnico pela execução do contrato, com comprovação de vínculo profissional com a licitante, admitidas quaisquer das formas previstas no art. 67, § 5º, da Lei nº 14.133/2021;
- comprovação, no momento da assinatura do contrato, de que a licitante dispõe de equipe técnica certificada nas quatro categorias indicadas no quadro a seguir, com vínculo profissional compatível com a execução do objeto e quantitativos mínimos por categoria:

Certificação exigida	Quantidade mínima de profissionais
PMP – Project Management Professional, emitida pelo Project Management Institute (PMI)	01 (um)
CISSP – Certified Information System Security Professional, emitida pelo International Information System Security Certification Consortium (ISC²)	01 (um)
Certificação técnica do fabricante da solução de Firewall de Próxima Geração ofertada	02 (dois)
Certificação técnica do fabricante da solução de EDR ofertada	01 (um)

8.3.1. Justificativa de proporcionalidade das certificações exigidas

A exigência cumulativa das quatro certificações observa o critério estabelecido na parte final do art. 37, XXI, da Constituição da República, segundo o qual a Administração deve cingir-se aos requisitos indispensáveis à garantia do cumprimento das obrigações. A correlação entre cada certificação e a função desempenhada na execução contratual é a seguinte:

PMP (Project Management Professional) – exigida do gerente do projeto de implantação, em razão da complexidade do cronograma físico de até 120 (cento e vinte) dias úteis, que compreende sete fases interdependentes (planejamento, fornecimento, implantação do EDR, testes, treinamento, operação assistida e operação plena). A certificação assegura que o profissional possui formação reconhecida em gestão de projetos, sendo apta a garantir o cumprimento dos marcos contratuais e a integração coordenada entre os componentes da solução.

CISSP (Certified Information System Security Professional, emitida pelo ISC²) – exigida do arquiteto de segurança responsável pela definição das políticas de proteção do perímetro, pela configuração do firewall de próxima geração e pela integração com o serviço de detecção e resposta a ameaças. A certificação é referência internacional em segurança da informação e, por sua amplitude temática (controle de acesso, criptografia, gestão de riscos, segurança de redes e resposta a incidentes), assegura aderência objetiva ao escopo do objeto contratado.

Certificação técnica do fabricante da solução de Firewall de Próxima Geração – exigida em quantitativo mínimo de 2 (dois) profissionais, por razões de continuidade operacional e redundância funcional: a operação em arranjo de alta disponibilidade do firewall exige equipe técnica apta a intervenções simultâneas e ao atendimento dos prazos de resposta pactuados em regime ininterrupto. A certificação do próprio fabricante é o único parâmetro objetivamente verificável de domínio técnico das especificidades da solução ofertada.

Certificação técnica do fabricante da solução de EDR – exigida em quantitativo mínimo de 1 (um) profissional, em razão da natureza continuada do serviço de detecção e resposta a ameaças, que pressupõe operação assistida durante os 36 (trinta e seis) meses de vigência. A certificação assegura que a contratada dispõe de profissional capacitado para a configuração de regras de detecção, ajuste de respostas automatizadas e análise técnica pós-incidente.

As certificações serão comprovadas no momento da assinatura do contrato, na forma do art. 92, XVI, da Lei nº 14.133/2021. A licitante deverá apresentar, naquele momento, cópia autenticada dos certificados vigentes e declaração de vínculo profissional dos respectivos titulares com a contratada.

8.4. Habilitação econômico-financeira

Será exigida apresentação de balanço patrimonial e demonstrações contábeis do último exercício social, com índices de liquidez e endividamento compatíveis com a execução do objeto, nos termos do art. 69 da Lei nº 14.133/2021. A exigência de capital social ou patrimônio líquido mínimo observará o limite de 10% (dez por cento) do valor estimado da contratação, na forma do § 4º do mesmo dispositivo.

8.5. Documentação técnica na proposta

A licitante apresentará, juntamente com a proposta comercial:

- a) fichas técnicas (datasheets) dos equipamentos ofertados (firewalls, comutadores e pontos de acesso), com as respectivas características completas;
- b) indicação expressa das marcas e modelos dos produtos ofertados (equipamentos, programas e serviços), não sendo aceitas expressões genéricas;
- c) plano e cronograma de implantação, observado o prazo máximo de 120 (cento e vinte) dias úteis;
- d) plano de atendimento de suporte técnico, com indicação dos meios de atendimento (sistema web, telefone e correio eletrônico);
- e) Declaração de Conformidade Técnica – DCT, demonstrando, em matriz, o atendimento a cada requisito técnico estabelecido neste Termo de Referência, na forma do Apêndice VIII.

8.6. Critérios de desclassificação

Serão desclassificadas as propostas que:

- a) contenham vícios ou ilegalidades;
- b) não atendam às especificações técnicas do Apêndice I;
- c) apresentem preço global superior ao valor máximo estimado;
- d) apresentem preços manifestamente inexequíveis, nos termos do art. 59, IV, da Lei nº 14.133/2021;
- e) não apresentem a documentação técnica exigida no item 8.5 deste Termo de Referência.

8.7. Vedações de participação

Não poderão participar do certame as empresas que se enquadrem nas vedações do art. 14 da Lei nº 14.133/2021, observada, quanto à vedação de consórcios, a regra do item 4.10 deste Termo de Referência.

9. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

O presente item estabelece a metodologia, os parâmetros e os critérios técnicos que disciplinarão a pesquisa de preços definitiva destinada à apuração do valor estimado da contratação, em observância ao art. 23 da Lei nº 14.133/2021, ao Decreto Estadual nº 2.734/2022 (que dispõe sobre a pesquisa de preços no âmbito estadual) e à Instrução Normativa SEGES/ME nº 65/2021, aplicada subsidiariamente como referencial de boa prática administrativa.

9.1. Valor estimado preliminar e valor estimado definitivo

O Estudo Técnico Preliminar nº 003/2026-ITERPA apurou **valor estimado preliminar de R\$ 6.021.958,62** (seis milhões, vinte e um mil, novecentos e cinquenta e oito reais e sessenta e dois

centavos) para o período de 36 (trinta e seis) meses, conforme decomposição da tabela abaixo e do Apêndice II do referido ETP.

Item	Descrição	Qtd.	Valor Unitário (R\$)	Valor Total (R\$)
1.1	Firewall NGFW (36 meses)	2	1.272.971,30	2.545.942,60
1.2	Comutador PoE+ 48 portas (36 meses)	25	43.639,88	1.090.997,00
1.3	Comutador de fibra 24 portas de fibra óptica SFP+ (36 meses)	2	495.732,91	991.465,82
1.4	Ponto de acesso Wi-Fi 6 (36 meses)	40	7.546,33	301.853,20
1.5	Serviço de EDR (mensalidade)	36	30.325,00	1.091.700,00
Valor global estimado (36 meses) – R\$				6.021.958,62

O valor estimado preliminar possui caráter indicativo e destina-se a subsidiar o juízo de viabilidade econômica da contratação. O valor estimado definitivo, apurado mediante a pesquisa de preços executada na forma deste item 9, será materializado em Mapa Comparativo de Preços, a ser anexado ao processo administrativo antes da publicação do instrumento convocatório.

9.2. Fontes de pesquisa de preços e ordem de preferência

A pesquisa utilizará, de forma combinada ou não, os parâmetros do art. 4º do Decreto Estadual nº 2.734/2022, observada a ordem de prioridade do § 1º: (a) Banco Referencial do SIMAS; (b) Portal Nacional de Compras Públicas – PNCP, no prazo de até 1 (um) ano; (c) contratações similares celebradas por órgãos e entidades da Administração Pública, no prazo de até 1 (um) ano. Subsidiariamente, poderão ser utilizados o Painel de Preços do Governo Federal, mídia especializada e sítios eletrônicos de domínio amplo, no intervalo máximo de 6 (seis) meses, bem como a base de notas fiscais eletrônicas, no prazo de até 1 (um) ano.

A pesquisa direta junto a fornecedores, na forma do art. 4º, V, do Decreto Estadual nº 2.734/2022, será admitida quando comprovadamente inviável a obtenção de preços suficientes nos parâmetros prioritários, mediante justificativa nos autos.

9.3. Metodologia de cálculo do preço estimado

Para cada item da solução, serão coletados preços nas fontes indicadas no item 9.2, observado o mínimo de 3 (três) preços válidos, quando possível, nos termos do art. 5º do Decreto Estadual nº 2.734/2022. Adota-se, como forma de cálculo, o método da mediana das referências compatíveis, atualizadas monetariamente conforme item 9.5, em coerência com o item 3 do Apêndice I do ETP. A escolha da mediana decorre da maior robustez estatística do indicador frente a valores extremos, sem sacrificar a economicidade.

9.4. Análise crítica dos valores coletados e saneamento estatístico

Os preços coletados serão submetidos a análise crítica documentada nos autos, especialmente quando houver variação significativa entre os valores. Serão desconsiderados os valores inexequíveis, inconsistentes e excessivamente elevados, conforme art. 5º, caput, do Decreto Estadual nº 2.734/2022, adotando-se critérios fundamentados e descritos no processo administrativo, nos termos do § 2º do mesmo artigo. Serão aplicados os seguintes critérios objetivos de saneamento:

- a) descarte de preços excessivamente elevados – superiores em mais de 25% à média dos demais valores;
- b) descarte de preços inexequíveis – inferiores a 75% da média dos valores remanescentes, ressalvados os preços registrados em atas e contratos firmados com o Poder Público;
- c) verificação do coeficiente de variação da amostra remanescente, para confirmação da homogeneidade do conjunto;
- d) documentação do saneamento no Mapa Comparativo de Preços, com indicação do preço descartado, do critério aplicado, da fundamentação objetiva e do responsável pela decisão.

9.5. Atualização monetária dos preços históricos

Os preços obtidos de fontes históricas serão atualizados até a data da pesquisa definitiva pelo Índice Nacional de Preços ao Consumidor Amplo – IPCA, na ausência de índice setorial específico, nos termos do art. 4º, § 3º, do Decreto Estadual nº 2.734/2022.

9.6. Materialização e conteúdo mínimo do Mapa Comparativo de Preços

A pesquisa de preços definitiva será materializada em Mapa Comparativo de Preços, parte integrante do Apêndice II deste Termo de Referência, em cumprimento ao art. 2º do Decreto Estadual nº 2.734/2022, contendo, no mínimo: descrição pormenorizada do objeto pesquisado por componente; identificação dos agentes responsáveis pela pesquisa; caracterização das fontes consultadas, com cópias dos documentos comprobatórios; série completa dos preços coletados; demonstração do saneamento efetuado; método matemático aplicado para a definição do valor estimado; e memória de cálculo do valor estimado de cada componente e do valor global.

9.7. Sigilo e publicação do orçamento estimado

O orçamento estimado da contratação será divulgado juntamente com o instrumento convocatório, conforme regra geral do art. 24 da Lei nº 14.133/2021 e por opção institucional do ITERPA pela transparência ativa. Caso a Administração opte por preservar o sigilo até a conclusão da licitação, na forma do art. 24, parágrafo único, da mesma Lei, os documentos de suporte à pesquisa serão classificados conforme a Lei nº 12.527/2011, art. 10.

9.8. Valor máximo aceitável e exequibilidade das propostas

O valor estimado apurado na pesquisa definitiva constituirá o preço máximo aceitável, tanto no valor global quanto nos valores unitários por componente. Presumir-se-ão inexequíveis, para fins de avaliação inicial, as propostas cujo valor global seja inferior a 75% (setenta e cinco por cento) do valor estimado, por aplicação analógica do parâmetro do art. 59, § 4º, da Lei nº 14.133/2021. A presunção é relativa e admite elisão mediante demonstração objetiva, pelo licitante, da viabilidade técnica e econômica da execução, em prazo não inferior a 2 (dois) dias úteis, com apresentação de planilha detalhada de composição de custos, documentação comprobatória da possibilidade de praticar os preços ofertados e declaração de respeito aos direitos trabalhistas dos profissionais alocados.

10. ADEQUAÇÃO ORÇAMENTÁRIA

A despesa decorrente da contratação correrá por conta de dotação orçamentária consignada no orçamento do ITERPA, conforme atestado de disponibilidade orçamentária a ser emitido pela Coordenadoria de Orçamento e Finanças – COF/ITERPA, observada a seguinte classificação funcional programática:

Programa de Trabalho: [a ser preenchido pela COF/ITERPA];

Natureza de Despesa: 3.3.90.40 – Serviços de Tecnologia da Informação e Comunicação; 4.4.90.52 – Equipamentos e Material Permanente, conforme aplicável a cada item;

Fonte de Recurso: [a ser preenchida pela COF/ITERPA].

A despesa será distribuída entre os exercícios financeiros alcançados pela vigência contratual (2026 a 2029), com os correspondentes ajustes a serem providenciados nas Leis Orçamentárias Anuais subsequentes, conforme cronograma esclarecido na descrição da necessidade (item 2.2 deste Termo de Referência).

Registre-se que o Plano de Contratações Anual – PCA do ITERPA encontra-se em fase de elaboração, circunstância analisada no item 2 do ETP nº 003/2026-ITERPA à luz do Decreto Estadual nº 2.227/2022 e do Enunciado nº 38 do Simpósio de Licitações e Contratos da Justiça Federal, aplicável subsidiariamente, que admitem, em caráter excepcional e motivado, a contratação cuja demanda não tenha sido formalmente incluída no PCA, com posterior inclusão para fins de transparência e monitoramento.

11. OBRIGAÇÕES E RESPONSABILIDADES

11.1. Dos direitos e obrigações da contratante

a) Sem que a isto limite seus direitos, terá o ITERPA as seguintes garantias e obrigações:

a.1) Receber o objeto de acordo com o que consta neste instrumento, no edital e nos seus anexos;

a.2) Devolver o objeto em desacordo com as especificações exigidas neste instrumento, no edital e nos seus anexos.

- a.3) A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.
- b) Sem que a isto limite sua responsabilidade, será o Órgão responsável pelos seguintes itens:
- b.1) Cumprir todos os compromissos financeiros assumidos com a CONTRATADA no prazo estipulado;
- b.2) Emitir Nota de Empenho a crédito do fornecedor;
- b.3) Proporcionar todas as facilidades, inclusive esclarecimentos atinentes ao objeto, para que a empresa possa cumprir as obrigações dentro das normas e condições da aquisição.
- b.4) Receber e conferir o objeto contratado através da FISCALIZAÇÃO, designada pela CONTRATANTE, com competência para o recebimento do objeto e atesto da Nota Fiscal, após a verificação das especificações técnicas, da qualidade, da quantidade e preços pactuados;
- b.5) Promover, através de seu representante, o acompanhamento e a fiscalização do objeto contratado, sob os aspectos qualitativos e quantitativos, prazos de vigência e entregas, anotando em registro próprio as falhas detectadas e comunicando ao Órgão por escrito as advertências e as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte desta;
- b.6) Cumprir e fazer cumprir o disposto neste instrumento, no edital e nos seus Apêndices.

11.2. Dos direitos e obrigações da CONTRATADA:

- a) Sem que a isto limite suas garantias, a CONTRATADA terá os seguintes direitos e obrigações:
- a.1) Receber informações e esclarecimentos necessários ao cumprimento das condições estabelecidas;
- a.2) Receber o Atesto do recebimento do objeto contratado após verificação das especificações;
- a.3) Receber formalmente a notificação de ocorrência de irregularidades que a fiscalização identificar na execução do objeto licitado, até para que possa a empresa proceder correções;
- a.4) Receber o pagamento nas condições estabelecidas neste instrumento.
- a.5) prestar os serviços no horário comercial (segunda a sexta-feira, das 08h às 18h) para as instalações, e em regime ininterrupto (24 horas por dia, 7 dias por semana) para o monitoramento e o suporte técnico;
- a.6) submeter-se às auditorias técnicas e de segurança realizadas pelo ITERPA ou por terceiros por ele indicados, durante a vigência contratual;
- a.7) cumprir integralmente as cláusulas de sustentabilidade constantes do item 4.6 deste Termo de Referência, inclusive as obrigações de logística reversa e de destinação ambientalmente adequada dos equipamentos.
- b) Sem que a isto limite sua responsabilidade, será a CONTRATADA responsável pelos seguintes itens:

- b.1) Cumprir fielmente as obrigações assumidas, conforme as especificações exigidas, utilizando-se de todos os recursos materiais e humanos necessários para executar os serviços licitados no prazo, no local e horário indicados, observando rigorosamente as exigências estabelecidas nas especificações e na proposta de preços apresentada pela empresa;
- b.2) Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, responsabilizando-se pelos danos causados diretamente à administração ou a terceiros, decorrentes de sua culpa ou dolo, por ocasião da entrega dos objetos licitados no local indicado, incluindo os possíveis danos causados por transportadoras, sem qualquer ônus ao contratante, ressarcindo os eventuais prejuízos causados ao Órgão e/ou terceiros, provocados por irregularidades cometidas na execução das obrigações assumidas;
- b.3) Ser responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução. A inadimplência da CONTRATADA, com referência aos encargos estabelecidos neste subitem não transfere a responsabilidade por seu pagamento à Administração do Iterpa, nem poderá onerar o objeto desta licitação, razão pela qual a CONTRATADA renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o Iterpa;
- b.4) Prestar todos os esclarecimentos que forem solicitados pelo Iterpa, credenciando junto ao Órgão, um representante para prestar os devidos esclarecimentos e atender as reclamações que porventura surgirem durante a execução do objeto;
- b.5) Manter, durante toda a execução, todas as condições para habilitação na licitação ou para qualificação na contratação direta, que sejam compatíveis com as obrigações a ser assumidas, cumprindo durante a vigência do contrato todas as leis e posturas federais, estaduais e municipais vigentes, a regularidade com o fisco, com o sistema de seguridade social, com a legislação trabalhista, normas e padrões de proteção ao meio ambiente, cumprimento do disposto no art. 7º, XXXIII da C.F/88 e cumprimento dos direitos da mulher, inclusive os que protegem a maternidade, sob pena da rescisão contratual, sem direito a indenização conforme preceitua o art. 28 §4º da Constituição do Estado do Pará, sendo a única responsável por prejuízos decorrentes de infrações a que houver dado causa, em especial a:
- b.5.1) Regularidade Fiscal com a Fazenda Nacional, o Sistema de Seguridade Social e o Fundo de Garantia do Tempo de Serviço – FGTS;
- b.5.2) Regularidade Fiscal perante as Fazendas Estaduais e Municipais da sede da licitante;
- b.5.3) Regularidade Trabalhista;
- b.6) Não transferir a outrem, no todo ou em parte, o objeto do presente, sem prévia e expressa anuência do Iterpa; não sendo aceita, sob nenhum pretexto, a transferência de responsabilidade da CONTRATADA para outras entidades, sejam fabricantes, técnicos ou quaisquer outros.
- b.7) A CONTRATADA é obrigada a reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, sem ônus para a Contratante.

- b.8) Informar o Órgão de qualquer alteração necessária à consolidação dos ajustes decorrentes da execução do objeto, tais como: mudança de endereço, razão social, telefone, e-mail, dissolução da sociedade, falência e outros;
- b.9) Disponibilizar uma conta de e-mail para fins de comunicação entre as partes, que integrará o preâmbulo do instrumento de contratação, mantendo-o permanentemente atualizado.
- b.10) Comunicar imediatamente à Administração, bem como ao responsável pela fiscalização, qualquer anormalidade verificada, inclusive de ordem funcional, para que sejam adotadas as providências de regularização necessárias, em qualquer tempo até o final da garantia.
- b.11) Manter sigilo, sob pena de responsabilidade civil, criminal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do Contrato, devendo orientar seus empregados nesse sentido, e firmando o Termo de Confidencialidade e Sigilo constante do Apêndice VII;
- b.12) Nos casos cujo objeto deste Instrumento seja serviço que envolva demolição, conserto, instalação, montagem, operação, conservação, reparação, adaptação e manutenção a ser realizada nos prédios deste. Obriga a observar os regulamentos de disciplina e segurança do ITERPA, além das normas de medicina e segurança do trabalho, dentre as quais destacam-se:
- b.12.1) Aqueles que estiverem executando serviço nesta Instituição devem utilizar os Equipamentos de Proteção Individual (EPIs) necessários, nos termos do previsto na Norma Regulamentadora nº 6 (NR 6), editada pela PORTARIA MTB nº 3.214/1978 do Ministério do Trabalho, e conforme previsão contratual;
- b.12.2) Os funcionários de empresas terceirizadas que estiverem executando serviços neste Órgão deverão apresentar crachás de identificação e estar, preferencialmente, uniformizados;
- b.12.3) O local em que haverá a realização de serviços deverá ser sinalizado durante toda a execução da atividade por meio de placas, avisos, fitas zebreadas, ou outros itens que se fizerem necessários para a finalidade;
- b.13) Nos casos descritos no subitem b.12, preencher devidamente a Ordem de Serviço, naquilo que lhe couber;

12. DO REAJUSTE

O contrato será reajustado pelo Índice Nacional de Preços ao Consumidor Amplo – IPCA, respeitada a periodicidade mínima de 12 (doze) meses, contados da data do orçamento estimado, em conformidade com o art. 92, § 4º, da Lei nº 14.133/2021. O reajuste será processado de ofício pelo ITERPA, mediante apostilamento.

13. SANÇÕES ADMINISTRATIVAS

O descumprimento das obrigações contratuais sujeitará a contratada às sanções previstas nos arts. 155 a 163 da Lei nº 14.133/2021, aplicadas conforme a gravidade da infração, sempre assegurados o contraditório e a ampla defesa. As multas moratória e compensatória observarão, respectivamente, os limites de 0,5% (meio por cento) ao dia, até o máximo de 10% (dez por cento) sobre o valor mensal do item afetado, e de 20% (vinte por cento) sobre o valor total do contrato, sem prejuízo das demais sanções cabíveis.

14. DA VISITA TÉCNICA

A visita técnica às instalações do ITERPA é facultativa, ficando a critério das empresas licitantes interessadas, mediante agendamento prévio junto ao Núcleo de Tecnologia da Informação – NTI, pelo telefone (91) 3284-9907 ou pelo endereço eletrônico nti@iterpa.pa.gov.br. A licitante que optar por não realizar a visita técnica firmará declaração de ciência das condições do local, renunciando a posterior alegação de desconhecimento das instalações.

15. FUNDAMENTAÇÃO LEGAL

A contratação observará o seguinte arcabouço normativo:

- a) Lei Federal nº 14.133, de 1º de abril de 2021 – Lei de Licitações e Contratos Administrativos;
- b) Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- c) Lei Federal nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação;
- d) Lei Federal nº 12.305, de 2 de agosto de 2010 – Política Nacional de Resíduos Sólidos;
- e) Lei Federal nº 6.938, de 31 de agosto de 1981 – Política Nacional do Meio Ambiente;
- e.1) Lei Estadual nº 8.417, de 7 de novembro de 2016 – Estatuto Paraense da Microempresa e Empresa de Pequeno Porte;
- f) Decreto Federal nº 10.240, de 12 de fevereiro de 2020 – Logística reversa de eletroeletrônicos;
- g) Decreto Federal nº 10.936, de 12 de janeiro de 2022 – Regulamento da Política Nacional de Resíduos Sólidos;
- h) Decreto Estadual nº 2.227/2022 – Plano de Contratações Anual;
- i) Decreto Estadual nº 2.734/2022 – Pesquisa de Preços;
- j) Decreto Estadual nº 2.939/2023, alterado pelos Decretos nº 3.037/2023 e nº 3.652/2024 – Estruturação de Processos de Contratação;
- k) Decreto Estadual nº 2.940/2023 – Pregão Eletrônico;
- l) Decreto Estadual nº 3.813/2024 – Fiscalização de Contratos;
- m) Decreto Estadual nº 4.193/2024 – Critérios de Sustentabilidade nas Contratações Públicas;

- n) Instrução Normativa SEGES/ME nº 58/2022 – Estudos Técnicos Preliminares;
- o) Instrução Normativa SEGES/ME nº 65/2021 – Pesquisa de Preços;
- p) Instrução Normativa SEGES/ME nº 81/2022 – Termo de Referência;
- q) Instrução Normativa SGD/ME nº 94/2022 – Contratação de Soluções de TIC no âmbito do SISP;
- r) Portaria SGD/MGI nº 2.751/2023 – Especificações Técnicas de Infraestrutura Computacional Sustentável;
- s) Portaria INMETRO nº 170, de 10 de abril de 2012 – Bens de Informática;
- t) Instrução Normativa SLTI/MPOG nº 01/2010 – Sustentabilidade nas Contratações Públicas;
- u) Instrução Normativa IBAMA nº 06/2013 – Cadastro Técnico Federal;
- v) Guia Nacional de Contratações Sustentáveis da CGU/AGU, 7ª edição, 2024.

Belém (PA), 17 de setembro de 2026.

Potyguara Prazeres de O. Ferreira

Coordenador do Núcleo de Tecnologia da Informação – NTI/ITERPA
Matrícula nº 54185591/7

Igor Alves Quadros

Analista de Sistemas do Núcleo de Tecnologia da Informação – NTI/ITERPA
Matrícula nº 5958069/1

APÊNDICE 1 – ESPECIFICAÇÕES TÉCNICAS

A licitante fornecerá solução composta por equipamentos, programas e serviços, na modalidade de serviço gerenciado, sendo responsável pela instalação, configuração, integração, operação, administração, monitoramento e manutenção durante toda a vigência do contrato. A solução deverá ser funcional e pronta para uso, observadas, no mínimo, as especificações deste Apêndice. Os itens, acessórios ou quantitativos adicionais necessários ao pleno atendimento dos requisitos serão fornecidos pela contratada, sem ônus adicional para o ITERPA.

A infraestrutura deverá assegurar, após a entrada em produção, disponibilidade mínima mensal de 99,5% (noventa e nove vírgula cinco por cento), aferida em regime ininterrupto, excluídas as paradas decorrentes de falhas na infraestrutura do contratante ou de manutenções planejadas comunicadas com antecedência mínima de 72 (setenta e duas) horas. O descumprimento desse índice sujeitará a contratada às glosas do item 7.3 do corpo do Termo de Referência.

Todos os componentes serão novos, em linha de produção e fabricação, com embalagem original de fábrica lacrada, não se admitindo equipamentos reconicionados ou anteriormente utilizados. Os produtos serão especificamente designados para uso empresarial, acompanhados de suporte oficial direto do fabricante.

1. Especificações dos componentes

1.1. Firewall de Próxima Geração (NGFW) – 2 equipamentos

1.1.1. Características gerais para firewalls de próxima geração

- 1.1.1.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.
- 1.1.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 1.1.1.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. 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;
- 1.1.1.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
- 1.1.1.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;
- 1.1.1.6. Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPsec e SSL, Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização.

1.1.2. FUNCIONALIDADES DE REDE E FIREWALL

- 1.1.2.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 1.1.2.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
- 1.1.2.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 1.1.2.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;
- 1.1.2.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- 1.1.2.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;
- 1.1.2.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 1.1.2.8. Deverá suportar sFlow ou Netflow;
- 1.1.2.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
- 1.1.2.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
- 1.1.2.11. Deve suportar o protocolo padrão da indústria VXLAN;
- 1.1.2.12. Deve implementar o protocolo ECMP;
- 1.1.2.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- 1.1.2.14. Enviar log para sistemas de monitoração externos;
- 1.1.2.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
- 1.1.2.16. Deve possuir mecanismos de proteção anti-spoofing;
- 1.1.2.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);
- 1.1.2.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- 1.1.2.19. Suportar OSPF graceful restart;
- 1.1.2.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 1.1.2.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- 1.1.2.22. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 1.1.2.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- 1.1.2.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;
- 1.1.2.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
- 1.1.2.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;
- 1.1.2.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
- 1.1.2.28. A solução deve possuir conectores nativos para integração com nuvens

- privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
- 1.1.2.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
 - 1.1.2.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
 - 1.1.2.31. Deverá suportar controle por zonas de segurança;
 - 1.1.2.32. Deverá suportar controles de políticas por porta e protocolo;
 - 1.1.2.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
 - 1.1.2.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
 - 1.1.2.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
 - 1.1.2.36. Controle, inspeção e descryptografia de SSL por política para tráfego de saída (Outbound);
 - 1.1.2.37. Deve descryptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
 - 1.1.2.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
 - 1.1.2.39. Suporte a objetos e regras IPV6;
 - 1.1.2.40. Suporte a objetos e regras multicast;
 - 1.1.2.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.1.3. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

- 1.1.3.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- 1.1.3.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- 1.1.3.3. Reconhecer pelo menos 4.000 (quatro mil) 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;
- 1.1.3.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
- 1.1.3.5. 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;
- 1.1.3.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
- 1.1.3.7. 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;
- 1.1.3.8. Para tráfego criptografado SSL, deve descryptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 1.1.3.9. 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. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;

- 1.1.3.10. Identificar o uso de táticas evasivas via comunicações criptografadas;
- 1.1.3.11. Atualizar a base de assinaturas de aplicações automaticamente;
- 1.1.3.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
- 1.1.3.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 1.1.3.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- 1.1.3.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
- 1.1.3.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 1.1.3.17. Deve alertar o usuário quando uma aplicação for bloqueada;
- 1.1.3.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
- 1.1.3.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
- 1.1.3.20. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;
- 1.1.3.21. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
- 1.1.3.22. 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);
- 1.1.3.23. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;
- 1.1.3.24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- 1.1.3.25. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

1.1.4. FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

- 1.1.4.1. 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;
- 1.1.4.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 1.1.4.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
- 1.1.4.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;
- 1.1.4.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas

- apenas em modo de monitoração;
- 1.1.4.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
 - 1.1.4.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
 - 1.1.4.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
 - 1.1.4.9. Deve permitir o bloqueio de vulnerabilidades;
 - 1.1.4.10. Deve permitir o bloqueio de exploits conhecidos;
 - 1.1.4.11. Deve incluir proteção contra-ataques de negação de serviços;
 - 1.1.4.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
 - 1.1.4.13. Detectar e bloquear a origem de portscans;
 - 1.1.4.14. Bloquear ataques efetuados por worms conhecidos;
 - 1.1.4.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
 - 1.1.4.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;
 - 1.1.4.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
 - 1.1.4.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
 - 1.1.4.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
 - 1.1.4.20. Identificar e bloquear comunicação com botnets;
 - 1.1.4.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
 - 1.1.4.22. Os eventos devem identificar o país de onde partiu a ameaça;
 - 1.1.4.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
 - 1.1.4.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
 - 1.1.4.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
 - 1.1.4.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante
 - 1.1.4.27. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
 - 1.1.4.28. 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;

1.1.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

- 1.1.5.1. 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);

- 1.1.5.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
- 1.1.5.3. 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;
- 1.1.5.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;
- 1.1.5.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 1.1.5.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
- 1.1.5.7. Possuir pelo menos 70 (setenta) categorias de URLs;
- 1.1.5.8. Deve possuir a função de exclusão de URLs do bloqueio;
- 1.1.5.9. Permitir a customização de página de bloqueio;
- 1.1.5.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;
- 1.1.5.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;
- 1.1.5.12. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;
- 1.1.5.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

1.1.6. FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

- 1.1.6.1. 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, eDirectory e base de dados local;
- 1.1.6.2. 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;
- 1.1.6.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;
- 1.1.6.4. 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;
- 1.1.6.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.1.6.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 1.1.6.7. 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);
- 1.1.6.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e

- controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 1.1.6.9. Deve suportar o envio e recebimento de credenciais via RADIUS;
 - 1.1.6.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
 - 1.1.6.11. 2.1.7. FUNCIONALIDADE DE FILTRO DE DADOS
 - 1.1.6.12. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
 - 1.1.6.13. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
 - 1.1.6.14. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
 - 1.1.6.15. 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.

1.1.7. FUNCIONALIDADE DE GEOLOCALIZAÇÃO

- 1.1.7.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 1.1.7.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.1.8. FUNCIONALIDADE DE VPN

- 1.1.8.1. Suportar VPN Site-to-Site e Cliente-To-Site;
- 1.1.8.2. Suportar IPSec VPN;
- 1.1.8.3. Suportar SSL VPN;
- 1.1.8.4. A VPN IPSEC deve suportar 3DES;
- 1.1.8.5. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
- 1.1.8.6. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- 1.1.8.7. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 1.1.8.8. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 1.1.8.9. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI
- 1.1.8.10. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 1.1.8.11. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
- 1.1.8.12. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 1.1.8.13. 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;
- 1.1.8.14. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- 1.1.8.15. 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;
- 1.1.8.16. Atribuição de DNS nos clientes remotos de VPN;
- 1.1.8.17. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 1.1.8.18. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários

- local;
- 1.1.8.19. Suportar leitura e verificação de CRL (Certificate Revocation List);
 - 1.1.8.20. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulem dentro dos túneis SSL;
 - 1.1.8.21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
 - 1.1.8.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
 - 1.1.8.23. Deverá manter uma conexão segura com o portal durante a sessão;
 - 1.1.8.24. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 11 (64 bit), Windows 10 (64 bit) e Mac OS X (v12 ou superior);

1.1.9. FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

- 1.1.9.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, 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;
- 1.1.9.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
- 1.1.9.3. Endereço de origem;
- 1.1.9.4. Endereço de destino;
- 1.1.9.5. Usuário e grupo;
- 1.1.9.6. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
- 1.1.9.7. Por porta;
- 1.1.9.8. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
- 1.1.9.9. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;
- 1.1.9.10. O QoS deve possibilitar a definição de fila de prioridade;
- 1.1.9.11. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
- 1.1.9.12. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
- 1.1.9.13. Suportar modificação de valores DSCP para o Diffserv;
- 1.1.9.14. Suportar priorização de tráfego usando informação de ToS (Type of Service);
- 1.1.9.15. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
- 1.1.9.16. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;
- 1.1.9.17. Deve possibilitar a definição de bandas distintas para download e upload;

1.1.10. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

- 1.1.10.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
- 1.1.10.2. A solução deve ser capaz de agregar vários links em uma interface virtual;
- 1.1.10.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);
- 1.1.10.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se

- em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;
- 1.1.10.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;
- 1.1.10.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);
- 1.1.10.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).
- 1.1.10.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:
- 1.1.10.9. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.
- 1.1.10.10. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;
- 1.1.10.11. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;
- 1.1.10.12. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;
- 1.1.10.13. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;
- 1.1.10.14. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);
- 1.1.10.15. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);
- 1.1.10.16. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
- 1.1.10.17. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;
- 1.1.10.18. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;
- 1.1.10.19. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;
- 1.1.10.20. A solução deve permitir a customização de intervalo de tempo em que é feita a

verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

- 1.1.10.21. A solução deve suportar nativamente conectores com clouds públicas;
- 1.1.10.22. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;
- 1.1.10.23. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);
- 1.1.10.24. Deve implementar balanceamento de link por hash do IP de origem;
- 1.1.10.25. Deve implementar balanceamento de link por hash do IP de origem e destino;
- 1.1.10.26. 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;
- 1.1.10.27. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;
- 1.1.10.28. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

1.1.11. FUNCIONALIDADE DE CONTROLADOR DE REDE SEM FIO

- 1.1.11.1. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:
- 1.1.11.2. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;
- 1.1.11.3. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;
- 1.1.11.4. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;
- 1.1.11.5. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
- 1.1.11.6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
- 1.1.11.7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
- 1.1.11.8. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;
- 1.1.11.9. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o

- concentrador através de túnel IPSec;
- 1.1.11.10. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
- 1.1.11.11. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
- 1.1.11.12. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;
- 1.1.11.13. A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;
- 1.1.11.14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
- 1.1.11.15. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;
- 1.1.11.16. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;
- 1.1.11.17. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
- 1.1.11.18. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
- 1.1.11.19. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
- 1.1.11.20. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
- 1.1.11.21. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças

- na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
- 1.1.11.22. A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
 - 1.1.11.23. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
 - 1.1.11.24. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
 - 1.1.11.25. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
 - 1.1.11.26. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
 - 1.1.11.27. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
 - 1.1.11.28. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
 - 1.1.11.29. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
 - 1.1.11.30. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
 - 1.1.11.31. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
 - 1.1.11.32. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
 - 1.1.11.33. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
 - 1.1.11.34. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
 - 1.1.11.35. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;
 - 1.1.11.36. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
 - 1.1.11.37. A solução deve suportar a configuração do BLE (Bluetooth Low Energy) nos pontos de acesso que tenham este recurso;
 - 1.1.11.38. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe

Requests sejam ignorados;

- 1.1.11.39. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;
- 1.1.11.40. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;
- 1.1.11.41. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;
- 1.1.11.42. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;
- 1.1.11.43. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;
- 1.1.11.44. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;
- 1.1.11.45. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;
- 1.1.11.46. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 1.1.11.47. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
- 1.1.11.48. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
- 1.1.11.49. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
- 1.1.11.50. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
- 1.1.11.51. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
- 1.1.11.52. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
- 1.1.11.53. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
- 1.1.11.54. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
- 1.1.11.55. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
- 1.1.11.56. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
- 1.1.11.57. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
- 1.1.11.58. A solução deve permitir a configuração do captive portal com endereço IPv6;

- 1.1.11.59. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
- 1.1.11.60. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
- 1.1.11.61. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
- 1.1.11.62. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;
- 1.1.11.63. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;
- 1.1.11.64. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
- 1.1.11.65. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
- 1.1.11.66. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
- 1.1.11.67. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
- 1.1.11.68. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;
- 1.1.11.69. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
- 1.1.11.70. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
- 1.1.11.71. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;
- 1.1.11.72. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
- 1.1.11.73. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
- 1.1.11.74. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
- 1.1.11.75. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
- 1.1.11.76. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
- 1.1.11.77. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
- 1.1.11.78. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
- 1.1.11.79. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;

- 1.1.11.80. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;
- 1.1.11.81. A solução deve possuir ferramentas de diagnósticos e debug;
- 1.1.11.82. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;
- 1.1.11.83. A solução deve suportar comunicação com elementos externos através de REST API;
- 1.1.11.84. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

1.1.12. FUNCIONALIDADE DE CONTROLADOR DE REDE CABEADA

- 1.1.12.1. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:
- 1.1.12.2. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
- 1.1.12.3. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
- 1.1.12.4. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;
- 1.1.12.5. Deve montar a topologia da rede de maneira automática;
- 1.1.12.6. Deve ser capaz de configurar os switches da rede;
- 1.1.12.7. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente em todos os switches gerenciados;
- 1.1.12.8. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
- 1.1.12.9. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
- 1.1.12.10. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
- 1.1.12.11. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;
- 1.1.12.12. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
- 1.1.12.13. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard,;
- 1.1.12.14. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
- 1.1.12.15. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
- 1.1.12.16. Deve ser capaz de configurar parâmetros SNMP dos switches;
- 1.1.12.17. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;
- 1.1.12.18. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

- 1.1.12.19. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
- 1.1.12.20. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
- 1.1.12.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
- 1.1.12.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;
- 1.1.12.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
- 1.1.12.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;
- 1.1.12.25. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:
- 1.1.12.26. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
- 1.1.12.27. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
- 1.1.12.28. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;
- 1.1.12.29. Deve montar a topologia da rede de maneira automática;
- 1.1.12.30. Deve ser capaz de configurar os switches da rede;
- 1.1.12.31. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente em todos os switches gerenciados;
- 1.1.12.32. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
- 1.1.12.33. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
- 1.1.12.34. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
- 1.1.12.35. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;
- 1.1.12.36. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
- 1.1.12.37. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard,;
- 1.1.12.38. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
- 1.1.12.39. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
- 1.1.12.40. Deve ser capaz de configurar parâmetros SNMP dos switches;
- 1.1.12.41. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;
- 1.1.12.42. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
- 1.1.12.43. A solução deve monitorar o consumo PoE das interfaces nos switches e

- apresentar esta informação de maneira gráfica;
- 1.1.12.44. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
- 1.1.12.45. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
- 1.1.12.46. Deve prover indicadores de saúde dos elementos críticos do ambiente;
- 1.1.12.47. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
- 1.1.12.48. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

1.1.13. CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW)

- 1.1.13.1. Deve suportar, no mínimo, 140 (cento e quarenta) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;
- 1.1.13.2. Deve suportar, no mínimo, 25 (vinte e cinco) milhões de conexões simultâneas;
- 1.1.13.3. Deve suportar, no mínimo, 700.000 (setecentos mil) novas conexões por segundo;
- 1.1.13.4. Deve Suportar, no mínimo, 50 (cinquenta) Gbps de throughput VPN IPSec;
- 1.1.13.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de VPN IPSEC Site-to-Site simultâneos;
- 1.1.13.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 50.000 (cinquenta mil) túneis de clientes VPN IPSEC simultâneos;
- 1.1.13.7. Deve suportar, no mínimo, 8 (oito) Gbps de throughput de VPN SSL;
- 1.1.13.8. Deve suportar, no mínimo, 10.000 (dez mil) clientes de VPN SSL simultâneos;
- 1.1.13.9. Deve suportar, no mínimo, 35 (trinta e cinco) Gbps de throughput de IPS;
- 1.1.13.10. Deve suportar, no mínimo, 10 (dez) Gbps de throughput de Inspeção SSL;
- 1.1.13.11. Deve suportar, no mínimo, 25 (vinte e cinco) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware.
- 1.1.13.12. Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
- 1.1.13.13. Deve possuir, pelo menos, 16 (dezesseis) interfaces com suporte a conectores SFP de 1 Gigabit Ethernet;
- 1.1.13.14. Deve possuir, pelo menos, 4 (quatro) interfaces com suporte a conectores SFP+ de 10 Gigabit Ethernet e SFP de 1 Gigabit Ethernet;
- 1.1.13.15. Deve possuir, pelo menos, 4 (duas) interfaces com suporte a conectores SFP28 de 25 Gigabit Ethernet;
- 1.1.13.16. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;
- 1.1.13.17. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para Alta-Disponibilidade;
- 1.1.13.18. Deve estar licenciado para gerenciar até 500 (quinhentos) pontos de acesso sem fio e 90 (noventa) switches simultaneamente em um único appliance;
- 1.1.13.19. Deve possuir fonte de alimentação AC redundante;
- 1.1.13.20. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

1.2. SWITCHS POE DE 48 PORTAS COM GARANTIA E SUPORTE DO FABRICANTE POR 36 MESES

- 1.2.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- 1.2.2. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);
- 1.2.3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;
- 1.2.4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W;
- 1.2.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
- 1.2.6. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
- 1.2.7. Deve possuir capacidade de comutação de pelo menos 170 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);
- 1.2.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
- 1.2.9. Deve possuir tabela MAC com suporte a 32.000 endereços;
- 1.2.10. Deve operar com latência igual ou inferior à 1us (microsegundo);
- 1.2.11. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
- 1.2.12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
- 1.2.13. Deve suportar a comutação de Jumbo Frames;
- 1.2.14. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;
- 1.2.15. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
- 1.2.16. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
- 1.2.17. Deve implementar serviço de DHCP Relay;
- 1.2.18. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;
- 1.2.19. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);
- 1.2.20. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo

menos 15 (quinze) instâncias de Multiple Spanning Tree;

- 1.2.21. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;
- 1.2.22. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;
- 1.2.23. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;
- 1.2.24. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;
- 1.2.25. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
- 1.2.26. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;
- 1.2.27. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;
- 1.2.28. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
- 1.2.29. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
- 1.2.30. Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;
- 1.2.31. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
- 1.2.32. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
- 1.2.33. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
- 1.2.34. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;
- 1.2.35. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;
- 1.2.36. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze)

dispositivos em cada porta através do protocolo IEEE 802.1X;

- 1.2.37. Deve suportar MAC Authentication Bypass (MAB);
- 1.2.38. Deve implementar RADIUS CoA (Change of Authorization);
- 1.2.39. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
- 1.2.40. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
- 1.2.41. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
- 1.2.42. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
- 1.2.43. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
- 1.2.44. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- 1.2.45. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
- 1.2.46. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);
- 1.2.47. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;
- 1.2.48. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- 1.2.49. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- 1.2.50. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- 1.2.51. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- 1.2.52. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- 1.2.53. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
- 1.2.54. Deve permitir ser gerenciado através de IPv6;

- 1.2.55. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- 1.2.56. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 1.2.57. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
- 1.2.58. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 1.2.59. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
- 1.2.60. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
- 1.2.61. Deverá suportar ser configurado e monitorado através de REST API;
- 1.2.62. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
- 1.2.63. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- 1.2.64. Deve suportar temperatura de operação de até 45° Celsius;
- 1.2.65. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- 1.2.66. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 1.2.67. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
- 1.2.68. Estes equipamentos deverão ser gerenciados pelo item 2.4 (Firewall de Próxima Geração com Garantia e suporte do fabricante por 36 meses);

1.3. Switchs Fibra de 24 portas de fibra óptica SFP+ com Garantia e suporte do fabricante por 36 meses – 2 equipamentos

- 1.3.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- 1.3.2. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- 1.3.3. Adicionalmente, deve possuir 2 (dois) slots QSFP+/QSFP28 para conexão de fibras ópticas do tipo 40GBase-X e 100GBase-X, operando em 40GbE e 100GbE, respectivamente. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;
- 1.3.4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do

equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

- 1.3.5. Deve possuir interface dedicada para gerenciamento local do tipo "out-of-band". Esta interface de gerenciamento deverá possuir porta 1000Base-T com conector RJ-45;
- 1.3.6. Deve possuir capacidade de comutação de pelo menos 800 Gbps e ser capaz de encaminhar até 1.3 Gpps (um bilhão e 300 milhões de pacotes por segundo);
- 1.3.7. Deve suportar ambos modos de encaminhamento de tráfego: store-and-forward e cut-through. A seleção do modo de operação deverá ser realizada através de configuração no software do equipamento;
- 1.3.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
- 1.3.9. Deve suportar Q-in-Q, recurso também conhecido como Stacked VLAN ou VLAN sobre VLAN em que é possível configurar duas TAGs de VLAN no mesmo frame;
- 1.3.10. Deve possuir tabela MAC com suporte a 64.000 endereços;;
- 1.3.11. Deve operar com latência igual ou inferior à 1us (microsegundo);
- 1.3.12. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
- 1.3.13. Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente;
- 1.3.14. Deve suportar o padrão IEEE 802.1Qbb (Priority-based Flow Control);
- 1.3.15. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
- 1.3.16. Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica;
- 1.3.17. Deve suportar a comutação de Jumbo Frames;
- 1.3.18. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
- 1.3.19. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
- 1.3.20. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
- 1.3.21. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
- 1.3.22. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;

- 1.3.23. Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;
- 1.3.24. Deve ser capaz de criar múltiplas tabelas de roteamento através de VRF (Virtual Routing and Forwarding). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação deste recurso;
- 1.3.25. Deve implementar serviço de DHCP Server e DHCP Relay;
- 1.3.26. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 4000 (quatro mil) grupos;
- 1.3.27. Recuperação de dados.
- 1.3.28. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN;
- 1.3.29. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 30 (trinta) instâncias de Multiple Spanning Tree;
- 1.3.30. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;
- 1.3.31. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;
- 1.3.32. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
- 1.3.33. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;
- 1.3.34. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
- 1.3.35. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;
- 1.3.36. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

- 1.3.37. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
- 1.3.38. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
- 1.3.39. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;
- 1.3.40. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ);
- 1.3.41. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
- 1.3.42. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;
- 1.3.43. Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement;
- 1.3.44. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
- 1.3.45. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
- 1.3.46. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;
- 1.3.47. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;
- 1.3.48. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
- 1.3.49. Deve suportar MAC Authentication Bypass (MAB);
- 1.3.50. Deve implementar RADIUS CoA (Change of Authorization);
- 1.3.51. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
- 1.3.52. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
- 1.3.53. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
- 1.3.54. Deve ser capaz de operar em modo de monitoramento para autenticações

802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

- 1.3.55. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
- 1.3.56. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- 1.3.57. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- 1.3.58. Deve implementar Netflow, sFlow ou similar;
- 1.3.59. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- 1.3.60. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- 1.3.61. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- 1.3.62. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- 1.3.63. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
- 1.3.64. Deve permitir ser gerenciado através de IPv6;
- 1.3.65. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- 1.3.66. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 1.3.67. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
- 1.3.68. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 1.3.69. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
- 1.3.70. Deverá suportar ser configurado e monitorado através de REST API;
- 1.3.71. Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark;
- 1.3.72. Deve ser capaz de armazenar no mínimo duas versões de firmware

simultaneamente em sua memória flash;

- 1.3.73. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- 1.3.74. Deve suportar temperatura de operação de até 40° Celsius;
- 1.3.75. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- 1.3.76. Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V;
- 1.3.77. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
- 1.3.78. Estes equipamentos deverão ser gerenciados pelo item 2.4 (Firewall de Próxima Geração com Garantia e suporte do fabricante por 36 meses);

1.4. Pontos de Acesso Wifi6 com Garantia e suporte do fabricante por 36 meses – 40 equipamentos

- 1.4.1. Ponto de acesso (AP) que permita acesso dos dispositivos à rede através da wireless e que possua todas as suas configurações centralizadas em controlador wireless;
- 1.4.2. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;
- 1.4.3. Deve identificar automaticamente o controlador wireless ao qual se conectará;
- 1.4.4. Deve permitir ser gerenciado remotamente através de links WAN;
- 1.4.5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;
- 1.4.6. Deve suportar operação nas faixas de frequência de 2.4GHz e 5GHz;
- 1.4.7. O ponto de acesso deve ser tri-radio Wi-Fi, ou seja, deve possuir 3 (três) rádios capazes de operar simultaneamente, sendo 1(um) rádio dedicado para função de sensor Wi-Fi e outros 2 (dois) rádios operando para servir clientes em 2.4GHz e 5GHz;
- 1.4.8. O ponto de acesso deve possuir rádio Wi-Fi dedicado para executar funções de sensor com objetivo de identificar interferências e ameaças de segurança em tempo real e com operação 24x7;
- 1.4.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;
- 1.4.10. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;

- 1.4.11. Deve possuir 1 (uma) interface Ethernet padrão 10/100/1000/2500Base-T com conector RJ-45 para permitir a conexão com a rede LAN;
- 1.4.12. Adicionalmente, deve possuir 1 (uma) interface Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir alta disponibilidade em caso de falha da interface primária;
- 1.4.13. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at em ambas interfaces ethernet. Adicionalmente deve possuir entrada de alimentação 12VDC;
- 1.4.14. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;
- 1.4.15. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;
- 1.4.16. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;
- 1.4.17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
- 1.4.18. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
- 1.4.19. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
- 1.4.20. Deve permitir operação em modo Mesh;
- 1.4.21. Deve possuir potência de irradiação mínima de 20dBm em cada rádio do ponto de acesso;
- 1.4.22. Deve suportar, no mínimo, operação MIMO 4x4 com 4 fluxos espaciais nos rádios que operam em 2.4 e 5GHz servindo clientes wireless;
- 1.4.23. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);
- 1.4.24. Deve suportar OFDMA com operações em Downlink (DL) e Uplink (UL);
- 1.4.25. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;

- 1.4.26. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;
- 1.4.27. Deve suportar BSS Coloring;
- 1.4.28. Deve permitir operação em 5GHz com canais de 20, 40, 80MHz;
- 1.4.29. Deve possuir sensibilidade mínima de -91dBm quando operando em 5GHz com MCS0 (HT20);
- 1.4.30. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5dBi em 5GHz;
- 1.4.31. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;
- 1.4.32. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
- 1.4.33. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;
- 1.4.34. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
- 1.4.35. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);
- 1.4.36. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 8 (oito) SSIDs com operação simultânea;
- 1.4.37. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 1.4.38. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;
- 1.4.39. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
- 1.4.40. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-TLS, EAP-TTLS e PEAP;
- 1.4.41. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 1.4.42. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

- 1.4.43. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
- 1.4.44. Deve implementar o padrão IEEE 802.11e;
- 1.4.45. Deve implementar o padrão IEEE 802.11h;
- 1.4.46. Deve implementar o padrão IEEE 802.3az;
- 1.4.47. Deve suportar ser gerenciado via SNMP;
- 1.4.48. Deve suportar consultas via REST API;
- 1.4.49. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;
- 1.4.50. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45° C;
- 1.4.51. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;
- 1.4.52. Deve possuir indicadores luminosos (LED) para indicação de status das interfaces ethernet, status dos rádios e status de atividade;
- 1.4.53. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
- 1.4.54. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
- 1.4.55. Deve possuir certificado emitido pela Wi-Fi Alliance;
- 1.4.56. Deve estar homologado pela ANATEL na data de execução do pregão;
- 1.4.57. Estes equipamentos deverão ser gerenciados pelo item 2.4 (Firewall de Próxima Geração com Garantia e suporte do fabricante por 36 meses);

1.5. Serviço de detecção e resposta a ameaças nos computadores e servidores por 36 meses (EDR)

- 1.5.1. Solução de Segurança para Servidores de Rede (físicos e virtuais):
- 1.5.2. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:
 - 1.5.2.1. Windows Server 2008 (32-bit/64-bit), 2008 R2, 2012, 2012 R2, 2016, 2019, 2022;
 - 1.5.2.2. Red Hat Enterprise 7, 8, 9;
 - 1.5.2.3. SUSE Enterprise 12, 15;
 - 1.5.2.4. CentOS 7, 8, 9;
 - 1.5.2.5. Ubuntu 18, 20, 22;
 - 1.5.2.6. Debian 9, 10, 11, 12;

2.5.2.6. Oracle Solaris 10, 11 (64-bit SPARC), 10, 11 (64-bit x86) e AIX 6.1, 7.1, 7.2.

- 1.5.3. A solução deverá ser totalmente compatível e homologada com o ambiente VMware;
- 1.5.4. A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: VMware Vcloud, MS Azure e AWS;
- 1.5.5. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;
- 1.5.6. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;
- 1.5.7. A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer e Firefox. Deve ainda suportar certificado digital para gerenciamento;
- 1.5.8. A console de administração deverá permitir o envio de notificações via SMTP;
- 1.5.9. Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;
- 1.5.10. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas.
- 1.5.11. A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos.
- 1.5.12. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;
- 1.5.13. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou agendado com o envio automático do relatório via e-mail;
- 1.5.14. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF e RTF.
- 1.5.15. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;
- 1.5.16. A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS e Firewall.
- 1.5.17. A console deve se integrar com o Active Directory para que os usuários do Active Directory possam administrar a solução de acordo com as permissões;
- 1.5.18. A console deve se integrar com o Active Directory para que possa ser efetuado o controle das máquinas no Active Directory;
- 1.5.19. Para efeito de administração, deve ser possível de se replicar a estrutura do

Active Directory na console de administração;

- 1.5.20. A solução de segurança ter a capacidade de identificar ataques entre contêineres;
- 1.5.21. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";
- 1.5.22. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar políticas de segurança;
- 1.5.23. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;
- 1.5.24. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;
- 1.5.25. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;
- 1.5.26. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;
- 1.5.27. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;
- 1.5.28. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;
- 1.5.29. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;
- 1.5.30. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;
- 1.5.31. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;
- 1.5.32. A solução deverá vir com perfis default pré-definidos e aptos a funcionarem de acordo com sua denominação;
- 1.5.33. A solução deverá mostrar quais máquinas estão usando determinada política;
- 1.5.34. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações

de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;

- 1.5.35. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;
- 1.5.36. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;
- 1.5.37. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;
- 1.5.38. Também deverá ser possível realizar o rastreamento por portas abertas, identificando possíveis serviços ativos e escutando;
- 1.5.39. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;
- 1.5.40. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;
- 1.5.41. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;
- 1.5.42. A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, IBMQradar e HP ArcSight de modo a permitir enviar os seus logs para essas soluções;
- 1.5.43. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;
- 1.5.44. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;
- 1.5.45. A solução deverá permitir exportar relatórios para no mínimo os formatos PDF e RTF;
- 1.5.46. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;
- 1.5.47. A lista de contatos de recebimento de relatório poderá ser obtida através do Active Directory;
- 1.5.48. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;
- 1.5.49. Após a atualização deve ser informado o que foi modificado ou adicionado;
- 1.5.50. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não distribuí-las aos clientes;
- 1.5.51. A console de gerenciamento deve apresentar a capacidade de gerar rollback de suas atualizações de regras;

- 1.5.52. A solução deverá ter capacidade de gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;
- 1.5.53. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;
- 1.5.54. No gerenciamento de licenças, deve ser informada quantidade LICITANTE e quantidade em utilização de clientes;
- 1.5.55. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;
- 1.5.56. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;
- 1.5.57. Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;
- 1.5.58. O fabricante deverá participar do programa “Microsoft Application Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;
- 1.5.59. A console de gerenciamento deve se integrar com o VmwarevCloud, de modo a importar e sincronizar os objetos (hosts vmware e guestsvm) para a console de gerenciamento da solução;
- 1.5.60. A solução deverá ser capaz de implementar as funcionalidades de Antimalware, Controle de Acesso a Sites Maliciosos, Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Windows através de um único agente;
- 1.5.61. A solução deverá ser capaz de implementar as funcionalidades de Antimalware, Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Linux através de um único agente;
- 1.5.62. A solução deverá ser capaz de implementar as funcionalidades de Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Solaris através de um único agente;
- 1.5.63. A solução deverá ser capaz de implementar as funcionalidades de Inspeção de Logs e Monitoramento de Integridade no sistema operacional AIX através de um único agente;
- 1.5.64. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;
- 1.5.65. Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;
- 1.5.66. A solução deve permitir a proteção contra códigos maliciosos através da

instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

- 1.5.67. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;
- 1.5.68. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;
- 1.5.69. A solução deve permitir proteção de antimalware em ambientes Linux (Ubuntu, CentOS, RedHat e SUSE) utilizando agentes;
- 1.5.70. A solução deverá permitir a proteção de antimalware em ambientes Windows;
- 1.5.71. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;
- 1.5.72. A solução deverá oferecer scanear processos em memória em busca de Malware;
- 1.5.73. O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;
- 1.5.74. O scan de arquivos comprimidos do tipo OLE deverá ser de no mínimo 20 camadas de compressão;
- 1.5.75. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;
- 1.5.76. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;
- 1.5.77. Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware.
- 1.5.78. Inspeção de Pacotes (HIPS/Virtual Patching):
- 1.5.79. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;
- 1.5.80. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;
- 1.5.81. A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;
- 1.5.82. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

- 1.5.83. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2008, 2012, 2016, 2019, 2022, Linux RedHat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Databa, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;
- 1.5.84. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;
- 1.5.85. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;
- 1.5.86. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instantMessaging;
- 1.5.87. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;
- 1.5.88. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;
- 1.5.89. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;
- 1.5.90. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);
- 1.5.91. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;
- 1.5.92. Deverá ser capaz de inspecionar tráfego criptografado de entrada;
- 1.5.93. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL Injection, Cross site script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double DecodingExploit;
- 1.5.94. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;
- 1.5.95. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;
- 1.5.96. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;
- 1.5.97. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;

- 1.5.98. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;
- 1.5.99. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;
- 1.5.100. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;
- 1.5.101. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVES;
- 1.5.102. As regras de IPS poderão ter sua capacidade de LOG desabilitado;
- 1.5.103. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;
- 1.5.104. As regras devem ser atualizadas automaticamente pelo fabricante;
- 1.5.105. Poderá atuar no modo em linha para proteção contra ataques ou modo escuta para monitoração e alertas;
- 1.5.106. Devem ser fornecidas 30 licenças da solução para proteção dos servidores (físicos e/ou virtuais) para a excelência da prestação do serviço.
- 1.5.107. Soluções de Segurança para Estações de Trabalho:
- 1.5.108. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:
 - 1.5.108.1. Windows 7 (x86/x64);
 - 1.5.108.2. Windows 8.1 (x86/x64);
 - 1.5.108.3. Windows 10 (x86/x64);
 - 1.5.108.4. Windows 11 (x64);
- 1.5.109. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;
- 1.5.110. Deve possuir capacidade nativa de integração com modulo da análise virtual para ameaças desconhecidas com suporte a sandbox do mesmo fabricante da solução ofertada;
- 1.5.111. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de Tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;
- 1.5.112. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:
- 1.5.113. Processos em execução em memória principal (RAM);
- 1.5.114. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

- 1.5.115. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip e exe;
- 1.5.116. Arquivos recebidos por meio de programas de comunicação instantânea (msnmessenger, yahoomessenger, google talk, icq, dentre outros).
- 1.5.117. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex;
- 1.5.118. Deve possuir detecção heurística de vírus desconhecidos;
- 1.5.119. Deve permitir configurar o consumo de cpu que será utilizada para uma varredura manual ou agendada;
- 1.5.120. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):
- 1.5.121. Em tempo real de arquivos acessados pelo usuário;
- 1.5.122. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;
- 1.5.123. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;
- 1.5.124. Automáticos do sistema com as seguintes opções:
- 1.5.125. Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;
- 1.5.126. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);
- 1.5.127. Frequência: horária, diária, semanal e mensal;
- 1.5.128. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados;
- 1.5.129. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;
- 1.5.130. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;
- 1.5.131. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;
- 1.5.132. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

- 1.5.133. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independente da maneira de como a URL está sendo acessada;
- 1.5.134. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;
- 1.5.135. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;
- 1.5.136. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;
- 1.5.137. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;
- 1.5.138. Funcionalidade de atualização:
- 1.5.139. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;
- 1.5.140. Deve permitir atualização incremental da lista de definições de vírus;
- 1.5.141. Deve permitir a atualização automática do engines do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;
- 1.5.142. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;
- 1.5.143. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;
- 1.5.144. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;
- 1.5.145. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;
- 1.5.146. Funcionalidade de administração:
- 1.5.147. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

- 1.5.148. Deve possibilitar instalação "silenciosa";
- 1.5.149. Deve permitir o bloqueio por nome de arquivo;
- 1.5.150. Deve permitir o travamento de pastas e diretórios;
- 1.5.151. Deve permitir o travamento de compartilhamentos;
- 1.5.152. Deve permitir o rastreamento e bloqueio de infecções;
- 1.5.153. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;
- 1.5.154. Quando on-premises, Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;
- 1.5.155. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;
- 1.5.156. Deve permitir a desinstalação através da console de gerenciamento da solução;
- 1.5.157. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;
- 1.5.158. Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;
- 1.5.159. Deve permitir a deleção dos arquivos quarentenados;
- 1.5.160. Deve permitir remoção automática de clientes inativos por determinado período de tempo;
- 1.5.161. Deve permitir integração com Active Directory para acesso a console de administração;
- 1.5.162. Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada;
- 1.5.163. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;
- 1.5.164. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
- 1.5.165. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP;
- 1.5.166. Deve permitir criação de subdomínios consecutivos dentro da árvore de

gerenciamento;

- 1.5.167. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
- 1.5.168. Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;
- 1.5.169. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;
- 1.5.170. Deve prover criptografia para as comunicações entre o servidor e os agentes de proteção;
- 1.5.171. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;
- 1.5.172. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;
- 1.5.173. Deve permitir a criação de usuários locais de administração da console de anti-malware;
- 1.5.174. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;
- 1.5.175. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;
- 1.5.176. Deve permitir a gerência de domínios separados para usuários previamente definidos;
- 1.5.177. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;
- 1.5.178. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.
- 1.5.179. Devem ser fornecidas 600 licenças da solução de proteção das estações de trabalho para a excelência da prestação do serviço.

2. Plano de transição com a contratação emergencial

A contratada elaborará Plano de Transição específico, a ser submetido à aprovação do NTI/ITERPA no prazo da Fase 1 do item 5.2 do Termo de Referência, contemplando:

- a) cronograma detalhado de substituição, em janela única ou em janelas sucessivas, dos equipamentos e serviços atualmente fornecidos no âmbito da contratação emergencial;

- b) operação simultânea da contratação emergencial e da nova solução durante a janela de transição, com convivência das políticas de segurança;
- c) procedimentos de retorno seguro à configuração anterior em caso de falha (rollback técnico), com pontos de verificação claramente definidos;
- d) plano de comunicação à equipe técnica do ITERPA e à empresa atualmente prestadora dos serviços emergenciais, para fins de coordenação;
- e) entrega, ao final da transição, de relatório consolidado de migração, atestando a integralidade da substituição e a estabilidade da nova solução.

3. Acordo de Nível de Serviço

3.1. Compromissos gerais

A contratada garantirá a operacionalidade da solução, com atuação proativa e reativa, mediante:

- a) suporte técnico disponível 24 horas por dia, 7 dias por semana;
- b) substituição de peças defeituosas no prazo máximo de 72 (setenta e duas) horas úteis após a notificação, admitida a manutenção de peças sobressalentes nas dependências do ITERPA;
- c) registro e tratamento de chamados por sistema web da contratada ou por central telefônica (0800 ou número local em Belém), disponível em regime ininterrupto, sem limite quantitativo durante a vigência.

3.2. Classificação de severidade e prazos máximos

Severidade Alta – proteção cibernética total ou parcialmente indisponível, ou incidente em curso. Prazo de resposta para início de diagnóstico remoto: 1 (uma) hora. Atendimento presencial, quando necessário: até 4 (quatro) horas.

Severidade Média – degradação de desempenho ou falha parcial de funcionalidade. Prazo de resposta para início de diagnóstico remoto: 4 (quatro) horas úteis. Atendimento presencial, quando necessário: até 8 (oito) horas.

Severidade Baixa – esclarecimentos ou solicitações não urgentes. Prazo de resposta para início de diagnóstico remoto: 24 (vinte e quatro) horas úteis. Atendimento presencial, quando necessário: agendamento em até 2 (dois) dias úteis.

Belém (PA), 17 de setembro de 2026.

Potyguara Prazeres de O. Ferreira

Coordenador do Núcleo de Tecnologia da Informação – NTI/ITERPA
Matrícula nº 54185591/7

Igor Alves Quadros

Analista de Sistemas do Núcleo de Tecnologia da Informação – NTI/ITERPA
Matrícula nº 5958069/1

APÊNDICE 2 – PLANILHA DE ITENS E QUANTITATIVOS

MAPA COMPARATIVO DE PREÇOS

Termo de Referência nº 03/2026 - ITERPA

Órgão/Entidade	Instituto de Terras do Pará — ITERPA (autarquia estadual)
Unidade Solicitante	Núcleo de Tecnologia da Informação — NTI
Processo (PAE)	2026/2933349
Identificação do TR	Termo de Referência nº 003/2026 — ITERPA
Objeto	Solução integrada de segurança de rede (NGFW, comutadores, pontos de acesso Wi-Fi 6 e EDR), com garantia e suporte por 36 meses
Vigência inicial	36 (trinta e seis) meses
Data da pesquisa	16/06/2026
Agentes responsáveis	Potyguara Prazeres de O. Ferreira — Coordenador do NTI (Mat. 54185591/7); Igor Alves Quadros — Analista de Sistemas do NTI (Mat. 5958069/1)
Fundamento normativo	Lei nº 14.133/2021, art. 23; Decreto Estadual nº 2.734/2022; IN SEGES/ME nº 65/2021 (subsidiária); Item 9 do TR nº 003/2026-ITERPA
Método matemático	Mediana das referências compatíveis após saneamento (art. 5º do Decreto Estadual nº 2.734/2022)
Índice de atualização	IPCA acumulado até junho de 2026 (art. 4º, § 3º, do Decreto Estadual nº 2.734/2022)
Ordem de prioridade das fontes	Art. 4º, § 1º, do Decreto Estadual nº 2.734/2022: SIMAS → PNCP → contratações similares → Pannel de Preços/outros
Observação	Não foi realizada consulta direta a fornecedores, em conformidade com a deliberação técnica do NTI

ESTRUTURA DO DOCUMENTO

Planilha 1	Item 1.1 — Firewall de Próxima Geração (NGFW)
Planilha 2	Item 1.2 — Comutador (switch) de acesso PoE+ de 48 portas Gigabit
Planilha 3	Item 1.3 — Comutador (switch) de núcleo de 24 portas de fibra óptica SFP+
Planilha 4	Item 1.4 — Ponto de acesso sem fio Wi-Fi 6 (IEEE 802.11ax)
Planilha 5	Item 1.5 — Serviço continuado de detecção e resposta nos computadores e servidores (EDR)
Planilha 6	Consolidação final do valor estimado definitivo

Item 1.1 — Firewall de Próxima Geração (NGFW)

Quantitativo: 2 Equipamento(s) — Período: 36 meses

Nº	Fonte	Órgão contratante	Identificação	Data	Valor original /uni. (R\$)	IPCA (%)	Valor atualizado (R\$)	Status	Justificativa do saneamento	Escopo/observações
1	PNCP	AGENCIA NACIONAL DE MINERACAO (ANM)	Contrato nº 00073/2025	21/11/2025	1.336.692,595	5,40	1.408.874,00	ACEITO	Compatível com o conjunto após saneamento estatístico.	Firewall Aplicação: Segurança Rede Computadores, Modelo: Apliance Ngfw, Suporte, Instalação, Garantia, licenças e operação
2	PNCP	TRIBUNAL SUPERIOR ELEITORAL (TSE)	Contrato nº 35/2026	10/07/2026	1.688.411,50	2,20	1.725.556,55	ACEITO	Compatível com o conjunto após saneamento estatístico.	Firewall Aplicação: Segurança Rede Computadores, Modelo: Apliance Ngfw, Suporte, Instalação, Garantia, licenças e operação
3	PNCP	INSTITUTO FEDERAL DE EDUCACAO, CIENCIA E TECNOLOGIA DO RIO GRANDE DO NORTE (IFRN).	EDITAL - PREGAO 204.2026	25/08/2026	972.624,98	2,20	994.022,73	ACEITO	Compatível com o conjunto após saneamento estatístico.	Firewall Aplicação: Segurança Rede Computadores, Modelo: Apliance Ngfw, Suporte, Instalação, Garantia, licenças e operação
4	igepps.pa.gov.br	IGEPREV	Contrato nº 59 / Pregão 025/2021	10/01/2022	1.209.250,00	23,50	1.493.423,75	ACEITO	Compatível com o conjunto após saneamento estatístico.	Firewall Aplicação: Segurança Rede Computadores, Modelo: Apliance Ngfw, Suporte, Instalação, Garantia, licenças e operação

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
 CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
 Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

MÉTODO MATEMÁTICO APLICADO	
Quantidade de referências válidas após saneamento	4 de 4 coletadas
Critério de saneamento (item 9.4 do TR / art. 5º, § 2º, Decreto Estadual nº 2.734/2022)	Descarte de preços > 25% acima da média e < 75% da média dos remanescentes
Atualização monetária aplicada (item 9.5 do TR / art. 4º, § 3º, Decreto Estadual nº 2.734/2022)	IPCA acumulado até junho de 2026
Método matemático adotado (item 9.3 do TR / art. 5º, Decreto Estadual nº 2.734/2022)	Mediana das referências compatíveis após saneamento
Mediana — valor unitário estimado definitivo (R\$)	1.451.148,88
Quantitativo	2 Equipamento(s)
Valor total estimado definitivo do componente (R\$)	2.902.297,76

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
 CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
 Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

Item 1.2 — Comutador (switch) de acesso PoE+ de 48 portas Gigabit

Quantitativo: 25 Equipamento(s) — Período: 36 meses

Nº	Fonte	Órgão contratante	Identificação	Data	Valor original (R\$)	IPCA (%)	Valor atualizado (R\$)	Status	Justificativa do saneamento	Escopo/observações
1	Gov.br	CONAB-COMPANHIA NACIONAL DE ABASTECIMENTO	PROCESSO N.º 21200.006578/2024-79	15/10/2025	43.639,88	5,40	45.996,43	ACEITO	Compatível com o conjunto após saneamento estatístico.	Switch PoE+ 48 portas com módulo de redundância, 60 meses
2	tjpi.jus.br	TJ-PI	Sei: 23.0.000083685-0 ata 6/2024/tj-pi Licitação: 72 / 2023	05/12/2023	56.300,00	16,90	65.793,70	ACEITO	Compatível com o conjunto após saneamento estatístico.	Switch PoE+ 48 portas Gigabit, gerenciável, 36 meses suporte
3	comprasnet.gov.br	COMANDO DA AERONÁUTICA (COMAER)	Pregão eletrônico nº 90005/2025	06/03/2025	24.266,40	5,40	25.576,79	ACEITO	Compatível com o conjunto após saneamento estatístico.	Switch PoE+ 48 portas, suporte 36 meses

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
 CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
 Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

MÉTODO MATEMÁTICO APLICADO

Quantidade de referências válidas após saneamento	3 de 3 coletadas
Critério de saneamento (item 9.4 do TR / art. 5º, § 2º, Decreto Estadual nº 2.734/2022)	Descarte de preços > 25% acima da média e < 75% da média dos remanescentes
Atualização monetária aplicada (item 9.5 do TR / art. 4º, § 3º, Decreto Estadual nº 2.734/2022)	IPCA acumulado até junho de 2026
Método matemático adotado (item 9.3 do TR / art. 5º, Decreto Estadual nº 2.734/2022)	Mediana das referências compatíveis após saneamento
Mediana — valor unitário estimado definitivo (R\$)	45.996,43
Quantitativo	25 Equipamento(s)
Valor total estimado definitivo do componente (R\$)	1.149.910,75

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
 CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
 Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

Item 1.3 — Comutador (switch) de núcleo de 24 portas de fibra óptica SFP+

Quantitativo: 2 Equipamento(s) — Período: 36 meses

Nº	Fonte	Órgão contratante	Identificação	Data	Valor original (R\$)	IPCA (%)	Valor atualizado (R\$)	Status	Justificativa do saneamento	Escopo/observações
1	PNCP	JUSTICA FEDERAL DE PRIMEIRA INSTANCIA	Editais nº 90001/2026	14/01/2026	248.000,00	2,20	253.456,00	ACEITO	Compatível com o conjunto após saneamento estatístico.	Switch 24p SFP+/QSFP28 100G, suporte 60 meses
2	PNCP	(UO) ESP-PRODESP-CIA.PROC DE DADOS EST. SP	Editais nº 90003/2025	14/02/2025	515.000,00	5,40	542.810,00	ACEITO	Compatível com o conjunto após saneamento estatístico.	Switch 24p SFP+ 10G, roteamento L3, 36 meses
3	PNCP	TRIBUNAL SUPERIOR DO TRABALHO	Editais nº 90007/2026	25/08/2026	495.732,91	2,20	506.639,03	ACEITO	Compatível com o conjunto após saneamento estatístico.	Switch núcleo 24p SFP+, OSPF/BGP, 36 meses

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
 CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
 Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

MÉTODO MATEMÁTICO APLICADO

Quantidade de referências válidas após saneamento	3 de 3 coletadas
Critério de saneamento (item 9.4 do TR / art. 5º, § 2º, Decreto Estadual nº 2.734/2022)	Descarte de preços > 25% acima da média e < 75% da média dos remanescentes
Atualização monetária aplicada (item 9.5 do TR / art. 4º, § 3º, Decreto Estadual nº 2.734/2022)	IPCA acumulado até junho de 2026
Método matemático adotado (item 9.3 do TR / art. 5º, Decreto Estadual nº 2.734/2022)	Mediana das referências compatíveis após saneamento
Mediana — valor unitário estimado definitivo (R\$)	506.639,03
Quantitativo	2 Equipamento(s)
Valor total estimado definitivo do componente (R\$)	1.013.278,06

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
 CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
 Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

Item 1.4 — Ponto de acesso sem fio Wi-Fi 6 (IEEE 802.11ax)

Quantitativo: 40 Equipamento(s) — Período: 36 meses

Nº	Fonte	Órgão contratante	Identificação	Data	Valor original (R\$)	IPCA (%)	Valor atualizado (R\$)	Status	Justificativa do saneamento	Escopo/observações
1	PNCP	MINISTERIO DA SAUDE	Edital nº 90120/2026	23/04/2026	5.860,00	2,20	5.988,92	ACEITO	Compatível com o conjunto após saneamento estatístico.	AP Wi-Fi 6, gerenciamento centralizado, 36 meses
2	PNCP	SECRETARIA DE ESTADO DA ADMINISTRACAO	Edital nº 525/2025	07/07/2025	8.081,665	5,40	8.518,07	ACEITO	Compatível com o conjunto após saneamento estatístico.	AP Wi-Fi 6 dual-band, controladora unificada, 36 meses
3	PNCP	INSTITUTO FEDERAL DE EDUCACAO, CIENCIA E TECNOLOGIA DE SAO PAULO	Edital nº 158/2026	13/08/2026	7.011,00	2,20	7.165,24	ACEITO	Compatível com o conjunto após saneamento estatístico.	AP Wi-Fi 6, WPA3, roaming inteligente, 36 meses
4	PNCP	ESTADO DE GOIAS	Edital nº 121642/2026	03/08/2026	9.527,20	2,20	9.736,80	ACEITO	Compatível com o conjunto após saneamento estatístico.	AP Wi-Fi 6 internos/externos, gerenciamento em nuvem privada, 36 meses

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
 CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
 Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

MÉTODO MATEMÁTICO APLICADO

Quantidade de referências válidas após saneamento	4 de 4 coletadas
Critério de saneamento (item 9.4 do TR / art. 5º, § 2º, Decreto Estadual nº 2.734/2022)	Descarte de preços > 25% acima da média e < 75% da média dos remanescentes
Atualização monetária aplicada (item 9.5 do TR / art. 4º, § 3º, Decreto Estadual nº 2.734/2022)	IPCA acumulado até junho de 2026
Método matemático adotado (item 9.3 do TR / art. 5º, Decreto Estadual nº 2.734/2022)	Mediana das referências compatíveis após saneamento
Mediana — valor unitário estimado definitivo (R\$)	7.841,66
Quantitativo	40 Equipamento(s)
Valor total estimado definitivo do componente (R\$)	313.666,40

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
 CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
 Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

Item 1.5 — Serviço continuado de detecção e resposta nos computadores e servidores (EDR)

Quantitativo: 36 Mês(s) — Período: 36 meses

Nº	Fonte	Órgão contratante	Identificação	Data	Valor original (R\$)	IPCA (%)	Valor atualizado (R\$)	Status	Justificativa do saneamento	Escopo/observações
1	PNCP	MINISTERIO DA CIENCIA, TECNOLOGIA E INOVACOES	Contrato nº 00009/2024	27/11/2024	30.325,00	11,50	33.812,38	ACEITO	Compatível com o conjunto após saneamento estatístico.	EDR para 300 endpoints, operação 24x7, mensalidade
2	PNCP	CONSELHO FEDERAL DE PSICOLOGIA	Edital nº 12/2026	01/07/2026	29.100,00	2,20	29.740,20	ACEITO	Compatível com o conjunto após saneamento estatístico.	EDR licenciamento por endpoint (~280 unid.), SOC 24x7, mensalidade
3	PNCP	MINISTERIO DA CIDADANIA	Edital nº 90005/2026	13/04/2026	39.107,64	2,20	39.968,01	ACEITO	Compatível com o conjunto após saneamento estatístico.	EDR/XDR gerenciado, ~320 endpoints, mensalidade

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
 CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
 Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

MÉTODO MATEMÁTICO APLICADO

Quantidade de referências válidas após saneamento	3 de 3 coletadas
Critério de saneamento (item 9.4 do TR / art. 5º, § 2º, Decreto Estadual nº 2.734/2022)	Descarte de preços > 25% acima da média e < 75% da média dos remanescentes
Atualização monetária aplicada (item 9.5 do TR / art. 4º, § 3º, Decreto Estadual nº 2.734/2022)	IPCA acumulado até junho de 2026
Método matemático adotado (item 9.3 do TR / art. 5º, Decreto Estadual nº 2.734/2022)	Mediana das referências compatíveis após saneamento
Mediana — valor unitário estimado definitivo (R\$)	33.812,38
Quantitativo	36 Mês(s)
Valor total estimado definitivo do componente (R\$)	1.217.245,68

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
 CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
 Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

CONSOLIDAÇÃO FINAL DO VALOR ESTIMADO DEFINITIVO

Composição a partir das medianas saneadas, por componente

Item	Descrição	Qtd.	Unidade	Valor unitário (R\$)	Valor total (R\$)
1.1	Firewall de Próxima Geração (NGFW)	2	Equipamento	1.451.148,88	2.902.297,76
1.2	Comutador (switch) de acesso PoE+ de 48 portas Gigabit	25	Equipamento	45.996,43	1.149.910,75
1.3	Comutador (switch) de núcleo de 24 portas de fibra óptica SFP+	2	Equipamento	506.639,03	1.013.278,06
1.4	Ponto de acesso sem fio Wi-Fi 6 (IEEE 802.11ax)	40	Equipamento	7.841,66	313.666,40
1.5	Serviço continuado de detecção e resposta nos computadores e servidores (EDR)	36	Mês	33.812,38	1.217.245,68
VALOR GLOBAL ESTIMADO DEFINITIVO (R\$)					6.596.398,75

OBSERVAÇÃO: O valor global estimado definitivo constituirá o preço máximo aceitável no certame, tanto no valor global quanto nos valores unitários por componente, na forma do item 9.8 do TR. Os critérios de exequibilidade observam o art. 59, § 4º, da Lei nº 14.133/2021.

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951

CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com

Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

METODOLOGIA APLICADA — PESQUISA DE PREÇOS DEFINITIVA

1. FONTES CONSULTADAS — ORDEM DE PRIORIDADE (ART. 4º DO DECRETO ESTADUAL Nº 2.734/2022)

Foram consultadas, na seguinte ordem de preferência:

- (a) Banco Referencial do SIMAS — consultado sem registros diretamente compatíveis com o objeto;
- (b) Portal Nacional de Compras Públicas — PNCP;
- (c) Contratações similares celebradas por órgãos e entidades da Administração Pública, localizadas em portais de transparência e atas de registro de preços vigentes;
- (d) Subsidiariamente, o Painel de Preços do Governo Federal.

Não foi realizada consulta direta a fornecedores (art. 4º, V, do Decreto Estadual nº 2.734/2022), em deliberação técnica do NTI.

2. PARÂMETROS TEMPORAIS

Observaram-se os prazos de validade do art. 4º do Decreto Estadual nº 2.734/2022: contratações similares e PNCP, até 1 (um) ano anterior; fontes subsidiárias, até 6 (seis) meses anteriores. Os preços de fontes mais antigas foram atualizados pelo IPCA, na forma do § 3º do mesmo artigo.

3. MÉTODO MATEMÁTICO — MEDIANA

Adotou-se a mediana das referências compatíveis após saneamento, com fundamento no art. 5º do Decreto Estadual nº 2.734/2022, em coerência com o item 9.3 do TR nº 003/2026-ITERPA. A escolha decorre da maior robustez estatística do indicador frente a valores extremos, sem sacrificar a economicidade.

4. ANÁLISE CRÍTICA E SANEAMENTO ESTATÍSTICO (ART. 5º, § 2º)

Aplicaram-se, cumulativamente:

- (a) descarte de preços superiores em mais de 25% à média do conjunto;
- (b) descarte de preços inferiores a 75% da média dos valores remanescentes, ressalvados os preços de atas e contratos firmados com o Poder Público;
- (c) documentação individual do saneamento, com indicação do critério aplicado, da fundamentação objetiva e do responsável pela decisão.

5. ATUALIZAÇÃO MONETÁRIA

Os preços de fontes históricas foram atualizados pelo IPCA acumulado até junho de 2026, conforme tabela de fatores aplicada no campo IPCA (%) de cada referência, em observância ao art. 4º, § 3º, do Decreto Estadual nº 2.734/2022.

6. MATERIALIZAÇÃO

A presente pesquisa materializa-se neste Mapa Comparativo de Preços, parte integrante do Apêndice II do Termo de Referência nº 003/2026-ITERPA, em cumprimento ao art. 2º do Decreto Estadual nº 2.734/2022.

APÊNDICE 3 - MEMÓRIA DE CÁLCULO DA PESQUISA DE PREÇOS

Termo de Referência nº 003/2026 – ITERPA

Órgão/Entidade	Instituto de Terras do Pará – ITERPA (autarquia estadual)
Unidade Solicitante	Núcleo de Tecnologia da Informação – NTI
Processo (PAE)	Nº 2026/2933349
Identificação do TR	Termo de Referência nº 003/2026 – ITERPA
Objeto	Solução integrada de segurança de rede (firewall NGFW, comutadores PoE+ e de fibra, pontos de acesso Wi-Fi 6 e serviço continuado de EDR), com garantia e suporte do fabricante por 36 meses
Fundamento normativo	Lei nº 14.133/2021, art. 23; Decreto Estadual nº 2.734/2022; Item 9 do TR nº 003/2026-ITERPA
Data da pesquisa	16 de junho de 2026

1. INTRODUÇÃO

A presente Memória de Cálculo documenta a pesquisa de preços definitiva realizada para a apuração do valor estimado da contratação tratada no Termo de Referência nº 003/2026-ITERPA, em observância ao art. 23 da Lei nº 14.133/2021, ao Decreto Estadual nº 2.734/2022 e à Instrução Normativa SEGES/ME nº 65/2021, aplicada subsidiariamente como referencial de boa prática administrativa. A peça materializa, de forma analítica, os parâmetros metodológicos previamente fixados no item 9 do referido Termo de Referência.

A pesquisa não contemplou consulta direta a fornecedores, em conformidade com a deliberação técnica do NTI/ITERPA. Privilegiaram-se, em coerência com a ordem de preferência do art. 4º, § 1º, do Decreto Estadual nº 2.734/2022, as fontes oficiais e os registros de contratações similares já materializados em portais públicos.

2. METODOLOGIA APLICADA

2.1. Fontes consultadas – ordem de preferência (art. 4º do Decreto Estadual nº 2.734/2022)

Foram consultadas, na seguinte ordem de prioridade:

- a) Banco Referencial do Sistema de Materiais e Serviços – SIMAS, mantido pela Administração Pública Estadual, com extrato negativo quanto à existência de registros diretamente compatíveis com o objeto;
- b) Portal Nacional de Compras Públicas – PNCP, base preponderante da pesquisa;
- c) contratações similares celebradas por órgãos e entidades da Administração Pública, localizadas em portais de transparência e em atas de registro de preços vigentes;

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951

CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com

Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

d) subsidiariamente, o Painel de Preços do Governo Federal.

Não se procedeu a consulta direta a fornecedores, possibilidade prevista no art. 4º, V, do Decreto Estadual nº 2.734/2022, em virtude da suficiência dos preços obtidos nas fontes prioritárias.

2.2. Parâmetros temporais

Observaram-se os prazos máximos de validade do art. 4º do Decreto Estadual nº 2.734/2022: contratações similares e PNCP, até 1 (um) ano anterior à data da pesquisa; fontes subsidiárias, até 6 (seis) meses anteriores à data de divulgação do edital. Preços obtidos em fontes mais antigas foram admitidos mediante atualização monetária pelo IPCA, na forma do § 3º do referido artigo.

2.3. Método matemático adotado

Adotou-se o método da mediana das referências compatíveis após saneamento, em coerência com o item 9.3 do TR e com fundamento no art. 5º do Decreto Estadual nº 2.734/2022, que autoriza a utilização da média, da mediana ou do menor dos valores obtidos. A mediana foi preferida por sua maior robustez estatística frente a valores extremos remanescentes, sem comprometimento da economicidade.

2.4. Análise crítica e saneamento estatístico

Aplicaram-se, cumulativamente, os seguintes critérios objetivos de saneamento, fundamentados no art. 5º, § 2º, do Decreto Estadual nº 2.734/2022:

- a) descarte de preços excessivamente elevados, superiores em mais de 25% à média do conjunto;
- b) descarte de preços inferiores a 75% da média dos valores remanescentes, ressalvados os preços de atas e contratos firmados com o Poder Público, cuja exequibilidade já foi demonstrada pela Administração;
- c) documentação individual do descarte, com indicação do preço, do critério aplicado e da fundamentação objetiva, no Mapa Comparativo de Preços Apêndice.

2.5. Atualização monetária – IPCA acumulado

Os preços de fontes históricas foram atualizados pelo Índice Nacional de Preços ao Consumidor Amplo – IPCA, na ausência de índice setorial específico, conforme art. 4º, § 3º, do Decreto Estadual nº 2.734/2022. Adotaram-se os seguintes fatores de atualização acumulados até junho de 2026:

Preços de 2022: 23,50%; de 2023: 16,90%; de 2024: 11,50%; de 2025: 5,40%; de 2026: 2,20%.

3. DETALHAMENTO DO CÁLCULO POR COMPONENTE

3.1. Item 1.1 – Firewall de Próxima Geração (NGFW)

Foram coletadas 4 (quatro) referências de preços de fontes distintas. A análise crítica resultou na aceitação de todas as 4 (quatro) referências coletadas, não havendo descarte por valor excessivo ou inexequível. Após a atualização monetária pelo IPCA, as referências geraram a mediana de R\$ 1.451.148,88 por unidade. Aplicado o quantitativo de 2 (dois) equipamentos, o valor total estimado para o componente é de R\$ 2.902.297,76.

3.2. Item 1.2 – Comutador (switch) de acesso PoE+ de 48 portas

Coletaram-se 3 (três) referências de preços. A análise crítica validou todas as 3 (três) referências após o saneamento estatístico. Após a atualização monetária, as referências geraram a mediana de R\$ 45.996,43 por unidade. Aplicado o quantitativo de 25 (vinte e cinco) equipamentos, o valor total estimado para o componente é de R\$ 1.149.910,75.

3.3. Item 1.3 – Comutador (switch) de núcleo de 24 portas de fibra

Coletaram-se 3 (três) referências de preços oriundas do PNCP e portais oficiais. A análise crítica validou as 3 (três) referências após o saneamento estatístico. As referências remanescentes geraram a mediana de R\$ 506.639,03 por unidade. Aplicado o quantitativo de 2 (dois) equipamentos, o valor total estimado é de R\$ 1.013.278,06.

3.4. Item 1.4 – Ponto de acesso sem fio Wi-Fi 6

Coletaram-se 4 (quatro) referências de fontes diversificadas. A análise crítica aceitou todas as 4 (quatro) referências válidas coletadas. As referências remanescentes geraram a mediana de R\$ 7.841,66 por unidade. Aplicado o quantitativo de 40 (quarenta) equipamentos, o valor total estimado é de R\$ 313.666,40.

3.5. Item 1.5 – Serviço continuado de EDR

Coletaram-se 3 (três) referências compatíveis com o escopo do objeto e o quantitativo aproximado. A análise crítica aceitou todas as referências válidas. As referências, após atualização monetária pelo IPCA, geraram a mediana de R\$ 33.812,38 por mês. Aplicado o quantitativo de 36 (trinta e seis) meses de vigência, o valor total estimado é de R\$ 1.217.245,68.

4. CONSOLIDAÇÃO DO VALOR ESTIMADO DEFINITIVO

Aplicando-se as medianas saneadas e atualizadas aos quantitativos do Apêndice I do TR, obtém-se o seguinte valor global estimado definitivo:

Item	Descrição	Qtd.	Unidade	Valor Unitário (R\$)	Valor Total (R\$)
------	-----------	------	---------	----------------------	-------------------

1.1	Firewall de Próxima Geração (NGFW)	2	Equipamento	1.451.148,88	2.902.297,76
1.2	Comutador (switch) de acesso PoE+ de 48 portas Gigabit	25	Equipamento	45.996,43	1.149.910,75
1.3	Comutador (switch) de núcleo de 24 portas de fibra óptica SFP+	2	Equipamento	506.639,03	1.013.278,06
1.4	Ponto de acesso sem fio Wi-Fi 6 (IEEE 802.11ax)	40	Equipamento	7.841,66	313.666,40
1.5	Serviço continuado de detecção e resposta nos computadores e servidores (EDR)	36	Mês	33.812,38	1.217.245,68
VALOR GLOBAL ESTIMADO DEFINITIVO (R\$)					6.596.398,75

O valor global de R\$ 6.596.398,75 constituirá o preço máximo aceitável no certame, observados, igualmente, os preços máximos unitários por componente, na forma do item 9.8 do TR. Os critérios de exequibilidade observam o parâmetro do art. 59, § 4º, da Lei nº 14.133/2021, com presunção relativa de inexecutabilidade para propostas inferiores a 75% do valor estimado, admitida elisão mediante demonstração objetiva da viabilidade técnica e econômica da execução.

5. REGIME DE PUBLICAÇÃO DO ORÇAMENTO ESTIMADO

Em conformidade com o item 9.7 do TR e com o art. 24 da Lei nº 14.133/2021, o orçamento estimado será divulgado juntamente com o instrumento convocatório, por opção institucional do ITERPA pela transparência ativa. Caso a Administração opte por preservar o sigilo até a conclusão da licitação, na forma do parágrafo único do mesmo artigo, os documentos de suporte à pesquisa serão classificados conforme o art. 10 da Lei nº 12.527/2011.

6. DECLARAÇÃO DE CONFORMIDADE

Os agentes públicos subscritores desta Memória declaram, sob a responsabilidade prevista no art. 4º, I, do Decreto Estadual nº 2.939/2023, que a presente pesquisa de preços observou integralmente: (i) a ordem de preferência das fontes do art. 4º, § 1º, do Decreto Estadual nº 2.734/2022; (ii) o quantitativo mínimo de três preços válidos por componente, exigido pelo art. 5º do mesmo Decreto; (iii) os parâmetros temporais aplicáveis a cada fonte consultada; (iv) o método matemático da mediana das referências compatíveis após saneamento; (v) a aplicação do IPCA como índice de atualização dos preços históricos; e (vi) o registro documental de cada descarte realizado, com indicação do critério, da fundamentação e do responsável.

A presente Memória, acompanhada do Mapa Comparativo de Preços, integra o Apêndice II do Termo de Referência nº 003/2026-ITERPA e os autos do Processo nº 2025/2472424, para todos os efeitos de controle interno e externo.

Belém (PA), 17 de setembro de 2026.

Potyguara Prazeres de O. Ferreira

Coordenador do Núcleo de Tecnologia da Informação – NTI/ITERPA
Matrícula nº 54185591/7

Igor Alves Quadros

Analista de Sistemas do Núcleo de Tecnologia da Informação – NTI/ITERPA
Matrícula nº 5958069/1

APÊNDICE 4 - JUSTIFICATIVA DA PESQUISA DE PREÇOS

Termo de Referência nº 003/2026 – ITERPA

Senhora Coordenadora,

Encaminha-se, para juntada aos autos do processo administrativo em epígrafe, o Mapa Comparativo de Preços e a respectiva Memória de Cálculo da pesquisa de preços definitiva conduzida com vistas à apuração do valor estimado da contratação pretendida – solução integrada de segurança de rede do Instituto de Terras do Pará –, em observância ao art. 23 da Lei nº 14.133/2021, ao Decreto Estadual nº 2.734/2022 e ao item 9 do Termo de Referência nº 003/2026-ITERPA.

A pesquisa observou a ordem de preferência das fontes prevista no art. 4º, § 1º, do Decreto Estadual nº 2.734/2022. Em razão da inexistência, no Banco Referencial do SIMAS, de registros diretamente compatíveis com o objeto, a apuração apoiou-se preponderantemente no Portal Nacional de Compras Públicas – PNCP, em contratações similares localizadas em portais de transparência de órgãos federais e estaduais e, subsidiariamente, no Painel de Preços do Governo Federal. Não se procedeu a consulta direta a fornecedores, na forma do art. 4º, V, do mesmo Decreto, em razão da suficiência de preços obtidos nas fontes prioritárias.

Para a maioria dos componentes da solução foram coletadas referências de preços em quantitativo compatível com o exigido pelo art. 5º do Decreto Estadual nº 2.734/2022. Os preços coletados foram submetidos a análise crítica documentada nos autos, com aplicação dos critérios objetivos de saneamento estatístico do § 2º do referido artigo – descarte de valores superiores em mais de 25% à média do conjunto e descarte de valores inferiores a 75% da média dos remanescentes –, com registro individual de cada descarte, do critério aplicado e da fundamentação objetiva no Mapa Comparativo.

Os preços de fontes históricas foram atualizados pelo Índice Nacional de Preços ao Consumidor Amplo – IPCA acumulado até junho de 2026, nos termos do art. 4º, § 3º, do Decreto Estadual nº 2.734/2022. Sobre as referências remanescentes após o saneamento, aplicou-se o método matemático da mediana, autorizado pelo art. 5º do mesmo Decreto e adotado em coerência com o item 9.3 do Termo de Referência.

Da composição das medianas saneadas e atualizadas, aplicadas aos quantitativos do Apêndice I do TR, resultou o valor global estimado definitivo de R\$ 6.596.398,75, que constituirá o preço máximo aceitável no certame, tanto no valor global quanto nos valores unitários por componente, na forma do item 9.8 do TR.

Os agentes responsáveis pela pesquisa, designados nos termos do art. 4º, I, do Decreto Estadual nº 2.939/2023, declaram, sob as penas da lei, que o procedimento observou

integralmente as exigências normativas aplicáveis, sendo a documentação juntada nos autos suficiente para a aferição pelo controle interno e externo.

À consideração superior, com o encaminhamento dos documentos anexos para integração ao processo administrativo e prosseguimento da fase preparatória, com a publicação do instrumento convocatório.

Belém (PA), 17 de setembro de 2026.

Potyguara Prazeres de O. Ferreira

Coordenador do NTI/ITERPA – Matrícula nº 54185591/7

Igor Alves Quadros

Analista de Sistemas do NTI/ITERPA – Matrícula nº 5958069/1

APÊNDICE 5 – MODELO DE TERMO DE VISTORIA

De acordo com o Termo de Referência nº 003/2026-ITERPA, elaborado pelo Núcleo de Tecnologia da Informação – NTI/ITERPA, declaro que a empresa _____, inscrita no CNPJ/MF sob o nº _____, por intermédio do(a) Sr.(a) _____, portador(a) da Cédula de Identidade nº _____, devidamente credenciado(a), realizou, nesta data, vistoria técnica às dependências do ITERPA, tomando ciência das condições e particularidades do local da prestação dos serviços.

A vistoria foi acompanhada pelo(a) servidor(a) _____, matrícula nº _____, lotado(a) no Núcleo de Tecnologia da Informação – NTI do ITERPA, designado(a) para este fim pela autoridade competente.

Belém (PA), ____ de _____ de 2026.

Razão Social da Proponente / Assinatura do Representante Legal

APÊNDICE 6 – MODELO DE TERMO DE DISPENSA DE VISTORIA

A empresa _____, CNPJ nº _____,
_____, por intermédio do(a) Sr.(a) _____,
_____, CPF nº _____,
declara conhecer as condições e particularidades do serviço a ser prestado, dispensando a
realização de vistoria técnica, por possuir informações suficientes para a elaboração da proposta,
renunciando, em consequência, a qualquer alegação futura de desconhecimento das instalações.

Belém (PA), ____ de _____ de 2026.

Razão Social da Proponente / Assinatura do Representante Legal

APÊNDICE 7 – TERMO DE CONFIDENCIALIDADE E SIGILO

A empresa _____, CNPJ nº _____, assume o compromisso de manter a confidencialidade e o sigilo sobre todas as informações jurídicas, técnicas, administrativas e pessoais obtidas junto ao Instituto de Terras do Pará em decorrência da execução contratual, inclusive sobre dados pessoais tratados na condição de operadora, nos termos da Lei nº 13.709/2018 (LGPD), obrigando-se a:

- a) não utilizar as informações acessadas para benefício próprio ou de terceiros;
- b) não efetuar gravação ou cópia de documentação confidencial, salvo mediante autorização prévia do ITERPA;
- c) não apropriar material confidencial ou de uso restrito;
- d) não transmitir o conhecimento das informações confidenciais a qualquer pessoa não autorizada, respondendo por todos os que venham a ter acesso por seu intermédio;
- e) adotar as medidas técnicas e administrativas aptas a proteger os dados pessoais acessados, na forma dos arts. 46 a 49 da Lei nº 13.709/2018.

A obrigação de confidencialidade persistirá enquanto a informação não se tornar de conhecimento público por outros meios, ou enquanto não houver autorização escrita do ITERPA para sua divulgação, subsistindo, em relação aos dados pessoais, pelo prazo previsto em lei.

Belém (PA), ____ de _____ de 2026.

Razão Social da Proponente / Assinatura do Representante Legal

APÊNDICE 8 – MODELO DE DECLARAÇÃO DE CONFORMIDADE TÉCNICA (DCT)

A Declaração de Conformidade Técnica – DCT é documento de apresentação obrigatória, juntamente com a proposta comercial, conforme item 8.5 deste Termo de Referência, e destina-se a demonstrar, de forma objetiva e em formato matricial, o atendimento a cada requisito técnico estabelecido neste instrumento e em seu Apêndice I.

A licitante apresentará matriz contendo, obrigatoriamente, as colunas: identificação do requisito; transcrição do requisito; declaração de atendimento (Sim/Não); marca/modelo ofertado; página da ficha técnica (datasheet); observações.

A licitante declara, ainda, ter pleno conhecimento de que: (a) a inexatidão, a omissão ou a falsidade de qualquer informação caracterizará comportamento inidôneo e ensejará as sanções previstas nos arts. 155 a 163 da Lei nº 14.133/2021; (b) a documentação técnica apresentada integra, para todos os efeitos, esta Declaração; (c) o ITERPA poderá exigir esclarecimentos adicionais ou proceder à diligência junto ao fabricante; (d) a aceitação da proposta fica condicionada à comprovação integral dos requisitos declarados.

Belém (PA), ____ de _____ de 2026.

Razão Social da Proponente / Assinatura do Representante Legal

ANEXO II – ESTUDO TÉCNICO PRELIMINAR Nº 003/2026 (ETP)

Órgão/Entidade	Instituto de Terras do Pará – ITERPA (autarquia estadual)
Unidade Solicitante	Núcleo de Tecnologia da Informação – NTI
Processo (PAE)	Nº 2026/2933349
Identificação do Estudo	Estudo Técnico Preliminar nº 003/2026 – ITERPA
Objeto	Contratação de solução integrada de segurança de rede – firewall de próxima geração (NGFW), switches PoE e de fibra, pontos de acesso Wi-Fi 6 e serviço de EDR –, com garantia e suporte do fabricante por 36 meses
Vigência inicial	36 (trinta e seis) meses, prorrogáveis até o limite decenal do art. 107 da Lei nº 14.133/2021

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO (ART. 18, §1º, I, DA LEI Nº 14.133/2021)

O presente Estudo Técnico Preliminar tem por objeto identificar e analisar as soluções disponíveis no mercado capazes de recompor, em bases tecnológicas adequadas ao estado atual da ameaça cibernética, a infraestrutura de segurança de rede do Instituto de Terras do Pará – ITERPA, demonstrando a viabilidade técnica, econômica e socioambiental das alternativas existentes e fornecendo as informações necessárias para subsidiar o processo de contratação, em alinhamento com o planejamento estratégico da instituição e com vistas ao atendimento das metas de Gestão Fundiária do Governo do Estado do Pará.

O ITERPA, autarquia estadual criada pela Lei Estadual nº 4.584/1975, é o órgão responsável pela gestão das terras públicas do Estado do Pará, tendo sua competência ampliada pela Lei Estadual nº 8.878/2019, que lhe atribuiu a Regularização Fundiária Urbana – REURB. A transição para o modelo digital, consolidada na implantação do Sistema de Cadastro Rural e Fundiário – SICARF, impõe à infraestrutura computacional do Instituto níveis crescentes de confidencialidade, integridade e disponibilidade dos dados tratados, o que torna a proteção cibernética requisito inafastável da operação.

Em seus servidores residem registros históricos de propriedades rurais, títulos expedidos em favor de milhares de famílias paraenses, bases georreferenciadas que sustentam a política estadual de

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951

CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com

Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

combate à grilagem e ao desmatamento ilegal e farto volume de dados pessoais alcançados pela Lei Geral de Proteção de Dados – LGPD (Lei Federal nº 13.709/2018). A proteção desse acervo encontra fundamento expresso no art. 46 da LGPD, que impõe ao controlador a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

O Contrato nº 08/2020, que assegurava o funcionamento dos serviços de segurança da informação do ITERPA – suporte técnico especializado presencial às soluções de segurança Fortinet, renovação de licenciamento de programas de proteção para o ambiente virtualizado, soluções antimalware para estações de trabalho e servidores, operação assistida e garantia do fabricante –, encerrou sua vigência em abril de 2025, ao atingir o limite temporal máximo então aplicável, sem possibilidade de nova prorrogação. Desde então, a instituição opera em situação de descobertura progressiva, conforme documentado no despacho lavrado pelo NTI no sequencial 32 do Processo nº 2025/2472424.

Naquele despacho, a unidade técnica descreveu o quadro com a transparência que a gravidade impunha: os dois firewalls FortiGate 500e seguem em operação sem licenças válidas, com assinaturas de proteção vencidas e vulnerabilidades conhecidas sem correção; aproximadamente trezentas estações de trabalho e servidores, físicos e virtuais, operam sem qualquer solução de antimalware atualizada; e o monitoramento especializado de tentativas de invasão foi descontinuado. Em síntese, o órgão opera sem visibilidade sobre o que circula em sua própria rede.

A persistência desse quadro projeta riscos concretos e mensuráveis. Os chamados ataques de sequestro de dados (ransomware), nos quais o invasor criptografa os arquivos da instituição e exige resgate em criptomoeda para devolver o acesso, têm tido órgãos públicos brasileiros como alvos prioritários, e o acervo fundiário do ITERPA, por sua valoração histórica e econômica, constitui alvo de manifesto interesse. A criptografia maliciosa de bases cartoriais ou georreferenciadas, sem cópias de segurança íntegras, pode tornar a recuperação inviável. Há, ainda, os ataques persistentes e silenciosos, em que o invasor mantém acesso prolongado e indetectado à rede para fins de espionagem ou adulteração de registros – risco cuja materialização comprometeria a própria segurança jurídica das titulações expedidas pelo Estado. A tudo isso soma-se a exposição do ente a sanções da Autoridade Nacional de Proteção de Dados – ANPD e a pretensões reparatórias dos titulares de dados pessoais, em decorrência do descumprimento dos deveres impostos pela LGPD.

Registra-se, neste ponto, o histórico de tentativas de equacionamento da demanda. O projeto de segurança da informação do ITERPA foi originalmente elaborado de forma abrangente, com o propósito de proteger, em arquitetura unificada, os ativos digitais, os dados sensíveis e os sistemas críticos da instituição, implementando controles de segurança eficazes para assegurar a confidencialidade, a integridade e a disponibilidade das informações, e ponderando a escalabilidade dos processos de regularização fundiária do SICARF e o crescimento do volume de dados que transitam na rede

computacional do Instituto. Tal projeto, contudo, não logrou ser licitado, por restrições orçamentárias e financeiras supervenientes ao planejamento.

Em razão dessa impossibilidade, e diante do encerramento do Contrato nº 08/2020, a Administração viabilizou contratação emergencial, com fundamento no art. 75, VIII, da Lei nº 14.133/2021, pelo prazo de doze meses e no valor estimado de R\$ 2.656.276,77, com o exclusivo propósito de manter, em padrões mínimos e pelo período estritamente necessário, os mesmos serviços anteriormente compreendidos no contrato encerrado, evitando que o Instituto permanecesse totalmente descoberto de proteção cibernética. A medida emergencial tem, portanto, natureza de contenção: dirige-se a interromper o estado de descobertura enquanto se conclui o planejamento estruturante.

A contratação ora estudada possui natureza diversa. Não substitui a emergencial nem com ela se confunde. Volta-se à recomposição definitiva da arquitetura de segurança de rede do Instituto, com solução integrada – firewall de próxima geração, switches PoE e de fibra, pontos de acesso Wi-Fi 6 e serviço continuado de EDR –, dimensionada para o triênio e ajustada à atual realidade orçamentária do ITERPA. Trata-se da segunda iteração do planejamento original, redesenhada para conciliar a integralidade da proteção pretendida com a capacidade financeira efetiva do órgão, em prevenção à perpetuação de soluções de contingência cujo custo total de propriedade cresce de modo desproporcional ao benefício.

Diante desse conjunto de fatores – encerramento do contrato anterior, exposição cibernética concreta do órgão, custódia de acervo crítico e inafastável, transitoriedade da medida emergencial em curso e necessidade de solução estruturante economicamente exequível –, o presente estudo busca identificar, dentre as soluções disponíveis no mercado, aquela que melhor equacione disponibilidade, segurança e escalabilidade da infraestrutura de proteção cibernética do ITERPA com as restrições orçamentárias e operacionais existentes, em consonância com o Documento de Formalização da Demanda anexado ao sequencial 02 do Processo nº 2025/2472424.

2. ALINHAMENTO COM O PLANEJAMENTO DA ADMINISTRAÇÃO (ART. 18, §1º, II)

O art. 18, §1º, II, da Lei nº 14.133/2021 exige que o ETP demonstre a previsão da contratação no Plano de Contratações Anual – PCA, “sempre que elaborado”, de modo a indicar o alinhamento da demanda com o planejamento da Administração.

O PCA do ITERPA para o exercício de 2025 encontra-se em fase de elaboração, não tendo sido concluído até a presente data. Essa circunstância, contudo, não constitui óbice à continuidade do processo de contratação, conforme se demonstra a seguir.

O próprio texto legal emprega a expressão “sempre que elaborado” (art. 18, caput, e §1º, II), admitindo, portanto, que a contratação prossiga quando o PCA ainda não estiver finalizado, desde que devidamente justificada a excepcionalidade. Nesse sentido, o Enunciado nº 38 do Simpósio de Licitações e Contratos da Justiça Federal é esclarecedor ao estabelecer que se permite,

excepcionalmente, a realização de contratação não constante do PCA, desde que devidamente justificada e condicionada à aprovação da autoridade competente, à demonstração de alinhamento com a estratégia institucional, à existência de lastro orçamentário e à posterior inclusão no PCA vigente para fins de monitoramento.

A presente contratação justifica-se como excepcional pelos seguintes fundamentos. Primeiro, trata-se de demanda crítica e inadiável: o Contrato nº 08/2020 encerrou sua vigência em abril de 2025, e desde então o Instituto opera em descobertura progressiva, mitigada apenas por contratação emergencial de prazo determinado, cuja postergação até a conclusão formal do PCA implicaria perpetuação do quadro de exposição. Segundo, há alinhamento com o planejamento estratégico de Tecnologia da Informação e Comunicação do ITERPA, com as metas de Governança Fundiária do Governo do Estado do Pará e com o Documento de Formalização da Demanda que originou este ETP. O dever de alinhamento das contratações ao planejamento estratégico e às leis orçamentárias, imposto pelo art. 11, parágrafo único, da Lei nº 14.133/2021, é atendido independentemente da conclusão formal do PCA. Terceiro, existe lastro orçamentário: a despesa está prevista na Lei Orçamentária Anual do Estado do Pará para o exercício de 2025, com dotação compatível com o valor estimado da contratação, distribuída entre os exercícios financeiros alcançados pela vigência do contrato.

Como providência correlata, determina-se que, tão logo concluído o PCA do ITERPA, a presente contratação seja nele incluída, para fins de transparência e monitoramento dos indicadores de desempenho, em conformidade com o Enunciado nº 38 do Simpósio de Licitações e Contratos da Justiça Federal e com as boas práticas de governança preconizadas pelo art. 12, VII, da Lei nº 14.133/2021 e pelo Decreto Estadual nº 2.227/2022.

3. REQUISITOS DA CONTRATAÇÃO (ART. 18, §1º, III)

3.1. Requisitos do objeto

O objeto qualifica-se como bem e serviço continuado de segurança de rede, compreendendo o fornecimento de equipamentos físicos (firewall de próxima geração; comutadores de rede com alimentação elétrica integrada e comutadores de fibra; pontos de acesso sem fio do padrão Wi-Fi 6) e a prestação continuada de serviço de detecção e resposta a ameaças nos computadores e servidores conectados à rede (EDR), todos com garantia técnica do fabricante e suporte por 36 meses.

3.1.1. Firewall de Próxima Geração (NGFW)

A solução deverá ir além da filtragem básica praticada pelos firewalls tradicionais, ofertando inspeção profunda do conteúdo do tráfego, detecção e prevenção de tentativas de invasão, controle granular de aplicações por identidade do usuário, análise de tráfego criptografado sem comprometimento da privacidade e integração com bases de inteligência de ameaças mantidas pelo fabricante. A operação será em arranjo de alta disponibilidade, com os dois equipamentos ativos

simultaneamente e replicação automática de configurações e do estado das conexões em curso, de modo a garantir continuidade do tráfego em caso de falha de um deles. As assinaturas de proteção serão atualizadas automaticamente, em intervalo não superior a 24 horas.

3.1.2. Comutadores de rede (switches)

Os comutadores de acesso, de 48 portas Gigabit com alimentação elétrica integrada (padrão PoE+), fornecerão conectividade e energia, pelo próprio cabo de rede, a estações de trabalho, telefones IP e câmeras, com suporte a segmentação lógica da rede, priorização do tráfego sensível (voz e vídeo) e protocolos de prevenção de laços lógicos. Os comutadores de fibra de 24 portas comporão a espinha dorsal da rede do Instituto, em arquitetura redundante, com capacidade de roteamento entre sub-redes e velocidades não inferiores a 10 Gigabits por segundo em cada porta. Ambos integrar-se-ão a uma única console de gerenciamento, em conjunto com o firewall e com os pontos de acesso sem fio.

3.1.3. Pontos de acesso sem fio (Wi-Fi 6)

Os pontos de acesso observarão o padrão Wi-Fi 6 (norma técnica IEEE 802.11ax), com suporte à coexistência de múltiplas redes sem fio em um mesmo equipamento, separação lógica entre a rede interna e a rede para visitantes, criptografia no padrão atual mais robusto (WPA3), balanceamento inteligente das conexões dos usuários e continuidade da conexão durante a mobilidade dentro do ambiente. O gerenciamento será centralizado, por equipamento dedicado ou em ambiente computacional restrito do fabricante, com integração à console unificada da solução.

3.1.4. Serviço continuado de EDR

O serviço de detecção e resposta a ameaças em computadores e servidores (EDR) abrangerá monitoramento contínuo dos equipamentos conectados à rede, identificação de comportamentos suspeitos típicos de ameaças avançadas (ransomware, ataques persistentes e exploração de falhas ainda sem correção pública), resposta automatizada (isolamento do equipamento comprometido, encerramento de processos maliciosos e remoção de artefatos), análise técnica pós-incidente para identificação da origem e da extensão do ataque, e integração com o firewall para aplicação coordenada de bloqueios. A contratada operará o serviço em regime ininterrupto (24 horas por dia, 7 dias por semana), com prazos máximos de detecção e de resposta a serem detalhados no Termo de Referência. O licenciamento será dimensionado pelo parque atual de equipamentos (aproximadamente 300), com previsão de margem para crescimento.

3.1.5. Segurança e proteção de dados

A solução deverá observar criptografia robusta para os dados armazenados (padrão AES-256) e para os dados em trânsito (protocolo TLS 1.2 ou superior), autenticação em dois fatores para todo o

acesso administrativo, registro de eventos de auditoria com retenção mínima de doze meses e gestão de vulnerabilidades com aplicação tempestiva de correções críticas, em atendimento ao art. 46 da Lei nº 13.709/2018.

3.1.6. Reversibilidade e portabilidade

Ao término da vigência contratual, a contratada deverá entregar ao ITERPA, em formatos abertos e não proprietários, as configurações, políticas, registros de eventos (logs) e bases de inteligência específicas do Instituto, sem custos adicionais, em prevenção ao aprisionamento tecnológico, na esteira da orientação do TCU consolidada no Acórdão nº 1.739/2015-Plenário.

3.2. Requisitos da contratada

A empresa a ser contratada deverá demonstrar capacidade técnico-operacional para o fornecimento e a operação de solução integrada de segurança de rede em ambiente de Administração Pública, mediante apresentação de atestado(s) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) a execução satisfatória de serviços compatíveis com o objeto, observado o limite de 50% das parcelas de maior relevância técnica, nos termos do art. 67, caput, §§ 1º e 2º, da Lei nº 14.133/2021.

Justifica-se a exigência pela natureza crítica do objeto: a falha na operação da solução compromete diretamente a continuidade do serviço público de regularização fundiária e a integridade do acervo digital sob custódia do Instituto. A exigência é proporcional e indispensável à garantia do cumprimento das obrigações (art. 37, XXI, parte final, da CF/88).

A contratada indicará preposto como ponto focal de contato com o ITERPA durante a execução contratual, sem necessidade de dedicação exclusiva presencial, podendo as atividades de relacionamento ser exercidas remotamente, com disponibilidade para reuniões presenciais quando solicitado.

3.2.1. Avaliação quanto à exigência de certificações de sistemas de gestão

No planejamento da contratação, avaliou-se a pertinência de exigir, como condição de habilitação, certificações institucionais de sistemas de gestão, notadamente ISO/IEC 20000-1, ISO/IEC 27001 e ISO/IEC 27701.

O art. 17, § 6º, III, da Lei nº 14.133/2021 admite que a Administração exija certificação por organização independente acreditada pelo INMETRO em relação a material e corpo técnico apresentados para fins de habilitação. Trata-se, contudo, de faculdade administrativa, e não de requisito obrigatório de contratação, devendo sua adoção ser examinada à luz das características concretas do objeto e dos princípios da motivação, razoabilidade, competitividade e proporcionalidade previstos no art. 5º da mesma Lei.

Essa faculdade deve ser compatibilizada, ainda, com o art. 9º, I, “a” e “c”, da Lei nº 14.133/2021, que veda a inclusão de condições capazes de comprometer, restringir ou frustrar o caráter competitivo do processo licitatório, bem como de exigências impertinentes ou irrelevantes para o objeto específico do contrato; com o art. 11, I e II, que estabelece como objetivos do processo licitatório a seleção da proposta apta a gerar o resultado mais vantajoso para a Administração e a garantia de tratamento isonômico e justa competição; e, sobretudo, com o art. 37, XXI, da Constituição Federal, segundo o qual somente podem ser estabelecidas exigências de qualificação técnica e econômica indispensáveis à garantia do cumprimento das obrigações.

A jurisprudência do Tribunal de Contas da União recomenda que essa avaliação seja realizada de maneira concreta e fundamentada. No Acórdão nº 2.129/2021-Plenário, Rel. Min. Benjamin Zymler, a Corte assentou ser irregular a exigência de normas técnicas, certificações, laudos e certificados de conformidade sem demonstração de sua essencialidade para garantir a qualidade e o desempenho suficientes do objeto contratado. O entendimento evidencia que a existência de certificação reconhecida no mercado, isoladamente considerada, não torna necessária sua transformação em requisito eliminatório de acesso ao certame.

Em precedente específico sobre certificações ISO, o Acórdão nº 1.085/2011-Plenário, Rel. Min. José Múcio Monteiro, registrou que a certificação de sistemas de gestão não assegura, por si só, que o produto ou serviço de empresa certificada seja superior ao de fornecedor não certificado, destacando que o afastamento de participantes não certificados pode reduzir a possibilidade de obtenção da melhor proposta pela Administração. A decisão ressaltou, ainda, que a simples existência da exigência pode desestimular a participação de fornecedores aptos, circunstância que nem sempre se revela pela quantidade final de propostas apresentadas no certame.

Naquela oportunidade, o TCU também reproduziu entendimento doutrinário de Marçal Justen Filho no sentido de que a certificação formal não deve se sobrepor à demonstração material da capacidade de satisfação do interesse público: o aspecto essencial é a presença dos requisitos necessários à adequada execução do objeto, e não apenas a titularidade formal de determinado certificado. Embora formulada sob o regime legislativo anterior, essa premissa permanece pertinente como orientação quanto à proporcionalidade das exigências, especialmente quando conjugada com os arts. 5º, 9º e 11 da Lei nº 14.133/2021 e com o art. 37, XXI, da Constituição Federal. (JUSTEN FILHO, Marçal. Comentários à Lei de Licitações e Contratos Administrativos, 8ª ed., Dialética, 2001, p. 349, conforme citado no Acórdão nº 1.085/2011-TCU-Plenário).

Registra-se que o Acórdão nº 1.091/2025-Plenário, também de relatoria do Ministro Benjamin Zymler, reconheceu, já sob a vigência da Lei nº 14.133/2021, a possibilidade jurídica de utilização de certificações ISO como requisito de habilitação, com fundamento no art. 17, § 6º, III. A decisão, entretanto, não estabeleceu obrigatoriedade de adoção dessas certificações em contratações de tecnologia, tendo examinado as justificativas apresentadas pelo DNIT no caso concreto e reconhecido

que sua adoção se encontrava dentro do espaço de discricionariedade administrativa. O próprio julgado ponderou que deslocar a exigência para momento posterior poderia ampliar a competitividade, embora, naquela contratação específica, tenham prevalecido razões relacionadas ao prazo necessário à obtenção das certificações e à continuidade dos serviços.

Mais recentemente, o Acórdão nº 1.093/2026-Plenário, Rel. Min.-Subst. Augusto Sherman, voltou a enfrentar o tema e considerou regular a utilização de certificações ISO e PBQP-H para fins de pontuação técnica, mas não como requisito de habilitação, desde que sua ausência não possa produzir, direta ou indiretamente, a desclassificação da proposta. O precedente reforça a necessidade de cautela quando a certificação deixa de representar elemento de diferenciação e passa a constituir barreira de ingresso na competição.

Nesse contexto jurídico e jurisprudencial, examinadas as características específicas desta contratação, não se identificou demonstração suficiente de que a posse cumulativa das certificações ISO/IEC 20000-1, ISO/IEC 27001 e ISO/IEC 27701 pela própria licitante constitua condição indispensável à execução satisfatória do objeto ou requisito sem o qual não seja possível assegurar a qualidade, a segurança, a disponibilidade ou a continuidade dos serviços pretendidos.

Ao contrário, o planejamento da contratação já estabelece mecanismos diretamente vinculados à capacidade de execução e aos resultados pretendidos pelo ITERPA, compreendendo comprovação de experiência anterior compatível, requisitos de qualificação técnico-operacional, qualificação da equipe, especificações detalhadas dos componentes da solução, obrigações de segurança da informação e proteção de dados, níveis mínimos de disponibilidade, suporte e manutenção, monitoramento da execução, critérios objetivos de recebimento, fiscalização, glosas e demais mecanismos de responsabilização contratual.

Tais instrumentos incidem diretamente sobre a aptidão da empresa para executar o objeto e sobre o desempenho que deverá ser efetivamente entregue durante a vigência contratual. Nesse cenário, a imposição adicional de três certificações institucionais cumulativas não se mostrou necessária para suprir deficiência ou risco que já não esteja adequadamente tratado pelos requisitos técnicos e mecanismos de controle previstos na contratação.

A exigência cumulativa poderia, entretanto, produzir efeito competitivo relevante, restringindo o universo de participantes previamente aptos a disputar o certame e afastando empresas que possuam experiência comprovada, estrutura operacional, profissionais qualificados e solução tecnicamente aderente às necessidades do ITERPA, mas que não tenham submetido seus processos internos aos três procedimentos formais de certificação considerados.

Há, ainda, risco de se estabelecer diferenciação entre fornecedores a partir de atributo de governança institucional que, embora possa representar boa prática organizacional, não se confunde necessariamente com a capacidade concreta de executar o objeto nas condições técnicas, operacionais e

de desempenho estabelecidas pela Administração. Nessa hipótese, a exigência pode favorecer agentes econômicos previamente certificados em detrimento de outros fornecedores igualmente aptos, sem que dessa restrição resulte ganho proporcional e demonstrável para o ITERPA.

Sob a perspectiva econômica, toda restrição ao universo de potenciais participantes deve corresponder a benefício objetivo que a justifique. A diminuição da concorrência reduz a pressão competitiva sobre os preços e as condições ofertadas e pode afastar soluções técnica e economicamente vantajosas, contrariando os objetivos estabelecidos pelo art. 11, I e II, da Lei nº 14.133/2021. A Administração não deve, portanto, restringir previamente a disputa quando os resultados e padrões de qualidade pretendidos podem ser assegurados por requisitos diretamente relacionados ao próprio objeto.

Também se considerou que certificações dessa natureza envolvem procedimentos de auditoria, estruturação organizacional, manutenção de sistemas de gestão e custos próprios. Condicionar a participação à prévia conclusão desses processos, quando não demonstrada sua imprescindibilidade para esta contratação específica, poderia converter instrumento voluntário de governança empresarial em barreira indireta de ingresso no certame, sem correspondência necessária com a qualidade do resultado que será entregue ao ITERPA.

Assim, a opção pela não exigência não representa redução dos padrões de segurança, qualidade ou governança da contratação. Representa, ao contrário, a adoção de mecanismo de qualificação mais diretamente relacionado ao objeto e aos riscos efetivamente identificados, mantendo-se integralmente os requisitos técnicos, operacionais, profissionais, de segurança, desempenho, fiscalização e responsabilização estabelecidos neste Estudo e no Termo de Referência.

Diante da ausência de demonstração de imprescindibilidade das certificações; da existência de mecanismos mais diretamente relacionados à comprovação da capacidade técnico-operacional; da suficiência dos requisitos estabelecidos para proteção dos interesses do ITERPA; do risco de restrição desproporcional à competitividade; da possibilidade de exclusão de fornecedores tecnicamente aptos; do potencial favorecimento indireto de empresas previamente certificadas; da inexistência de benefício adicional proporcional à restrição produzida; e da necessidade de preservar a maior disputa possível pela proposta efetivamente mais vantajosa, opta-se por não exigir as certificações ISO/IEC 20000-1, ISO/IEC 27001 e ISO/IEC 27701 como condição de habilitação ou participação no certame.

A decisão preserva os padrões técnicos e de segurança definidos para o objeto e, simultaneamente, prestigia a isonomia, a proporcionalidade, a ampla competitividade e a justa competição, ampliando o universo de potenciais fornecedores sem flexibilizar qualquer requisito material necessário à adequada execução contratual e favorecendo a obtenção da proposta mais vantajosa para o ITERPA.

3.3. Necessidade de treinamento

Deverá a contratada prover treinamento operacional à equipe técnica do NTI/ITERPA para as ferramentas de gestão, monitoramento e resposta a incidentes da solução contratada, com carga horária mínima de 40 (quarenta) horas, a ser detalhada no Termo de Referência. A capacitação é indispensável à fiscalização contratual e à autonomia operacional do Instituto, na forma do art. 18, §1º, X, da Lei nº 14.133/2021. A omissão dessa providência implicaria subutilização da solução e fragilização da gestão do contrato.

4. ESTIMATIVA DAS QUANTIDADES (ART. 18, §1º, IV)

Os quantitativos foram dimensionados a partir do inventário do parque ativo de equipamentos de rede e dos computadores e servidores do ITERPA (aproximadamente trezentos equipamentos, entre físicos e virtuais), da projeção de expansão da força de trabalho e dos pontos de presença para o triênio (crescimento médio anual de 10%) e da cobertura física das instalações da Sede. A metodologia detalhada, com fórmulas e justificação por componente, consta do Apêndice II – Memória de Cálculo deste ETP, em atendimento ao art. 18, §1º, IV, da Lei nº 14.133/2021.

Síntese dos quantitativos:

Item	Descrição	Unidade	Qtd.
1.1	Firewall de Próxima Geração (NGFW), em arranjo de alta disponibilidade, com garantia e suporte do fabricante por 36 meses	Equipamento	2
1.2	Switch de acesso PoE+ de 48 portas Gigabit, com garantia e suporte do fabricante por 36 meses	Equipamento	25
1.3	Switch de núcleo/distribuição de fibra de 24 portas SFP+, com garantia e suporte do fabricante por 36 meses	Equipamento	2
1.4	Ponto de acesso Wi-Fi 6 (IEEE 802.11ax), com gerenciamento centralizado, garantia e suporte do fabricante por 36 meses	Equipamento	40
1.5	Serviço continuado de detecção e resposta a ameaças em computadores e servidores (EDR), com licenciamento por equipamento e operação assistida	Mês	36

5. LEVANTAMENTO DE MERCADO (ART. 18, §1º, V)

5.1. Critérios de avaliação

A análise das soluções disponíveis no mercado foi conduzida a partir de quatro objetivos: atualidade tecnológica da proteção cibernética do perímetro da rede e dos computadores e servidores conectados; viabilidade orçamentária frente à capacidade financeira do Instituto; preservação da soberania dos dados sob custódia do órgão; e unicidade da responsabilização técnica e contratual. Como parâmetros complementares, foram considerados o risco de obsolescência, a escalabilidade, a aderência à LGPD e a compatibilidade com o cronograma de transição com a contratação emergencial em curso.

5.2. Fontes de pesquisa

O levantamento utilizou as seguintes fontes, observada a ordem de prioridade estabelecida no art. 4º, §1º, do Decreto Estadual nº 2.734/2022: Banco Referencial do Sistema de Materiais e Serviços – SIMAS, consultado sem registros diretamente compatíveis com o objeto; Portal Nacional de Compras Públicas – PNCP; e contratações similares celebradas por órgãos e entidades da Administração Pública, localizadas em portais de transparência e em atas de registro de preços vigentes, que constituíram a base preponderante da estimativa. Subsidiariamente, foram consultados o Painel de Preços do Governo Federal e o Portal Compras.gov.br, nos termos do art. 4º, IV, do referido Decreto. As referências constam do Apêndice I.

5.3. Cenários analisados

5.3.1. Cenário A – Renovação isolada das licenças do parque legado

Consiste na renovação das licenças e do suporte dos firewalls FortiGate 500e existentes, mantendo-se a arquitetura legada. O investimento estimado para 36 meses totaliza aproximadamente R\$ 2,1 milhões. O cenário foi descartado porque a arquitetura legada, embora financeiramente atraente, não comporta os recursos exigidos pelo atual estado das ameaças – designadamente, a inspeção de tráfego criptografado em larga escala, a detecção comportamental nativa, a integração com inteligência de ameaças modernas e o suporte ao padrão Wi-Fi 6. Acresce-se a inexistência, no parque legado, de pontos de acesso Wi-Fi 6 e de solução de EDR, componentes considerados indispensáveis pela unidade técnica. Esta alternativa, portanto, atende parcialmente ao problema, sendo tecnicamente insuficiente.

5.3.2. Cenário B – Aquisição fragmentada (multifabricante)

Contempla a aquisição de cada componente junto a fabricantes distintos, escolhidos isoladamente pelo menor preço, com integração técnica a cargo do ITERPA. O custo estimado para 36

meses é de aproximadamente R\$ 7,3 milhões, superior ao da solução integrada em razão da inexistência de economias de escala na negociação. Transfere ao Instituto o ônus técnico e contratual da integração entre fabricantes diversos, com risco elevado de incompatibilidades, dispersão da responsabilização em caso de incidente e dificuldade na manutenção de prazos uniformes de atendimento. Esta alternativa pode atender ao problema, porém com custo superior e complexidade operacional crítica.

5.3.3. Cenário C – Solução integrada de fornecedor único

Consiste na contratação de solução integrada de segurança de rede, fornecida por um único fornecedor, abrangendo firewall de próxima geração (NGFW), comutadores de rede com alimentação elétrica integrada e comutadores de fibra, pontos de acesso sem fio do padrão Wi-Fi 6 e serviço continuado de detecção e resposta nos computadores e servidores (EDR), com garantia e suporte do fabricante por 36 meses e responsabilização técnica unificada. **O custo estimado para 36 meses é de R\$ 6.021.958,62** (seis milhões, vinte e um mil, novecentos e cinquenta e oito reais e sessenta e dois centavos). Este cenário atende aos quatro objetivos definidos: atualidade tecnológica assegurada pela natureza atual dos componentes; viabilidade orçamentária compatível com a capacidade financeira do Instituto; preservação da soberania dos dados, que permanecem em equipamentos instalados nas dependências do Instituto; e responsabilização unificada do fornecedor pelo conjunto da solução.

5.3.4. Cenário D – Segurança contratada como serviço em nuvem

Consiste na contratação de proteção cibernética em modelo de serviço gerenciado em nuvem, com firewall virtual, detecção de ameaças nos computadores e servidores conectados à rede e console de gestão operados a partir de centros de dados do provedor. O custo estimado para 36 meses é de aproximadamente R\$ 8,4 milhões. Esta alternativa foi descartada pelos seguintes motivos: (i) a dependência de conectividade de internet de alta disponibilidade entre Belém e os centros de dados dos provedores, localizados fora da Região Norte, introduz risco de latência e indisponibilidade incompatível com a operação do firewall de perímetro; (ii) a transferência da inspeção de tráfego ao provedor compromete a soberania dos dados sob custódia do ITERPA, em arranjo cujo enquadramento à LGPD demandaria contrato de transferência internacional de dados, com obstáculos adicionais; e (iii) o custo total no horizonte de 36 meses supera o da solução instalada nas dependências do Instituto. Registre-se que a LGPD não veda, por si só, o uso de soluções em nuvem, mas exige a adoção de medidas de segurança adequadas (art. 46); a descartação não se fundamenta em vedação genérica, mas nos fatores concretos acima descritos.

5.4. Análise comparativa

Critério	Cenário A – Renovação do legado	Cenário B – Aquisição fragmentada	Cenário C – Solução integrada	Cenário D – Segurança contratada como serviço em nuvem
Atualidade tecnológica da solução	Insuficiente	Adequada	Plena	Plena
Integração entre componentes	Limitada (parque legado)	Risco elevado (multifabricante)	Nativa	Dependente do provedor
Responsabilização contratual	Fornecedor único	Dispersa	Unificada	Unificada (cloud)
Soberania dos dados	Plena (equipamentos no Instituto)	Plena (equipamentos no Instituto)	Plena (equipamentos no Instituto)	Reduzida (provedor)
Custo estimado (36 meses)	R\$ 2,1 mi (insuficiente)	R\$ 7,3 mi	R\$ 6,0 mi	R\$ 8,4 mi
Viabilidade	Inviável	Crítica	Compatível	Inviável (latência/LGPD)

5.5. Conclusão do levantamento de mercado

O Cenário C – solução integrada de fornecedor único – constitui a alternativa mais vantajosa para o ITERPA. A escolha decorre de quatro fatores: plena atualidade tecnológica da proteção cibernética ofertada; viabilidade orçamentária comprovada (R\$ 6,0 milhões em 36 meses, contra R\$ 7,3 milhões do Cenário B e R\$ 8,4 milhões do Cenário D); preservação da soberania dos dados, que permanecem em equipamentos instalados nas dependências do Instituto; e responsabilização técnica e contratual unificada, com ponto único de contato para níveis de serviço, suporte e gestão de incidentes.

6. ESTIMATIVA DO VALOR DA CONTRATAÇÃO (ART. 18, §1º, VI)

O valor estimado da contratação é de **R\$ 6.021.958,62** (seis milhões, vinte e um mil, novecentos e cinquenta e oito reais e sessenta e dois centavos) para o período de 36 (trinta e seis) meses, obtido a partir de contratações similares da Administração Pública, consulta ao Portal Nacional de Compras Públicas, ao Pannel de Preços do Governo Federal, a portais de transparência e a atas de registro de preços vigentes, em observância ao art. 23 da Lei nº 14.133/2021 e ao Decreto Estadual nº 2.734/2022.

O valor tem caráter preliminar. A pesquisa de preços definitiva será realizada na fase de elaboração do Termo de Referência, com atualização dos valores na forma do art. 4º, §3º, do Decreto Estadual nº 2.734/2022. As referências utilizadas, com indicação das fontes, constam do Apêndice I. As memórias de cálculo que fundamentam a estimativa encontram-se detalhadas no Apêndice II – Memória de Cálculo, conforme exigência do art. 18, §1º, VI, da Lei nº 14.133/2021.

Os critérios de aceitabilidade de preços unitários e global, bem como o procedimento de avaliação de exequibilidade, serão definidos e motivados na fase de elaboração do Termo de Referência, nos termos do art. 59, III e IV, da Lei nº 14.133/2021. Adota-se, como diretriz, a fixação dos valores estimados unitários e global como preços máximos de aceitabilidade.

Composição do valor global estimado:

Item	Descrição	Qtd.	Valor Unitário (R\$)	Valor Total (R\$)
1.1	Firewall NGFW (36 meses)	2	1.272.971,30	2.545.942,60
1.2	Switch PoE+ 48 portas (36 meses)	25	43.639,88	1.090.997,00
1.3	Switch de fibra 24 portas (36 meses)	2	495.732,91	991.465,82
1.4	Ponto de acesso Wi-Fi 6 (36 meses)	40	7.546,33	301.853,20
1.5	Serviço de EDR (mensalidade)	36	30.325,00	1.091.700,00
Valor global estimado (36 meses) – R\$				6.021.958,62

7. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO (ART. 18, §1º, VII)

A solução consiste no fornecimento, pela contratada, de arranjo integrado de equipamentos e serviço continuado de segurança de rede, instalados nas dependências do ITERPA e operados sob garantia e suporte do fabricante por 36 meses. A contratada será responsável pela entrega, instalação, configuração inicial, integração entre os componentes, operação assistida do serviço de EDR e

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951

CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com

Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

manutenção preventiva e corretiva durante toda a vigência contratual, em ponto único de responsabilização técnica e administrativa.

A contratação será realizada mediante licitação na modalidade Pregão Eletrônico, do tipo menor preço global por grupo único, por se tratar de bem e serviço comum (art. 6º, XIII, da Lei nº 14.133/2021), cujas especificações técnicas são usualmente encontradas no mercado e podem ser objetivamente definidas no edital. O contrato terá vigência inicial de 36 (trinta e seis) meses, admitida prorrogação por períodos sucessivos, observado o limite máximo total de 10 (dez) anos – computada a vigência inicial –, nos termos do art. 107 da Lei nº 14.133/2021, por se tratar de serviço de natureza continuada (art. 6º, XV), desde que haja previsão em edital e que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração.

Cabe ao ITERPA a gestão da infraestrutura física local (energia, climatização, cabeamento estruturado) e a fiscalização contratual, incluindo acompanhamento dos níveis de serviço pactuados (disponibilidade, tempos de detecção e resposta a incidentes), verificação do cumprimento dos requisitos de segurança da informação e das cláusulas de transição e reversibilidade. As especificações técnicas detalhadas serão definidas no Termo de Referência.

8. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO (ART. 18, §1º, VIII)

A regra geral em licitações é o parcelamento do objeto, conforme art. 40, §2º, da Lei nº 14.133/2021 e Súmula 247 do TCU. Todavia, o §3º do mesmo artigo prevê que o parcelamento não será adotado quando o objeto configurar sistema único e integrado e houver risco ao conjunto pretendido, ou quando a economia de escala recomendar a contratação pelo mesmo fornecedor. O objeto da presente contratação enquadra-se nessas exceções, pelos motivos a seguir.

Interdependência técnica: os componentes da solução (firewall, comutadores de rede, pontos de acesso sem fio e serviço de detecção e resposta a ameaças) configuram sistema único e integrado, cuja operação coordenada depende da interoperabilidade entre os elementos. A separação em lotes distintos exigiria compatibilização entre equipamentos de diferentes fabricantes e versões de programas embarcados, com risco concreto de conflitos de configuração que comprometeriam a aplicação coordenada de políticas de segurança e a correlação de eventos. Em caso de incidente, haveria transferência de responsabilidade entre fornecedores, inviabilizando o cumprimento dos prazos de atendimento pactuados.

Inviabilidade econômica do parcelamento: o levantamento de mercado, sintetizado no item 5, demonstrou que a aquisição fragmentada (Cenário B) é aproximadamente 17,7% mais onerosa que a solução integrada (Cenário C), em razão da inexistência de economia de escala na negociação multilateral e do custo administrativo adicional de gestão de múltiplos contratos.

Natureza unitária do modelo de serviço: o objeto é a recomposição integral da arquitetura de segurança de rede, não a aquisição de componentes individuais. O fornecedor assume a responsabilidade pela operação coordenada do conjunto, em arranjo cuja fragmentação equivaleria a desnaturar o próprio objeto.

Registre-se que o TCU, no Acórdão nº 1.972/2018-Plenário, reafirmou que a justificativa para o não parcelamento deve ser substancial e fundamentada em estudo técnico, não bastando afirmações genéricas de conveniência. A presente justificativa atende a esse parâmetro ao demonstrar, com base no levantamento de mercado constante do item 5, a interdependência técnica concreta, a inviabilidade econômica mensurada e a natureza unitária do modelo de serviço.

9. RESULTADOS PRETENDIDOS (ART. 18, §1º, IX)

A contratação pretende alcançar resultados mensuráveis em quatro planos:

Economicidade: o modelo integrado apresenta custo aproximadamente 16% inferior ao da aquisição fragmentada (Cenário B) e 28% inferior à contratação em modelo de serviço em nuvem (Cenário D), preservando-se a soberania dos dados. A diluição do investimento em 36 meses, com licenciamento e suporte incluídos no preço global, evita o comprometimento de recursos extraordinários e estabiliza o fluxo orçamentário.

Continuidade operacional: a recomposição da arquitetura de segurança assegura a continuidade da operação dos sistemas finalísticos do Instituto, particularmente do SICARF, com restabelecimento da capacidade de detecção e resposta a incidentes em padrões compatíveis com a criticidade do acervo custodiado.

Aproveitamento de recursos humanos: a equipe técnica do NTI/ITERPA, atualmente empregada em esforços extraordinários de mitigação manual da descobertura, será liberada para atividades estratégicas, com ganho estimado de pelo menos dois técnicos em dedicação integral, à medida que o monitoramento e a resposta a incidentes passem a ser desempenhados, em grande parte, pela contratada e pelas ferramentas adquiridas.

Conformidade legal: aderência plena à LGPD, com criptografia, autenticação multifator, controle de acesso, logs de auditoria e capacidade de resposta a incidentes documentada, reduzindo o risco de sanções administrativas pela ANPD e de pretensões reparatórias dos titulares de dados.

10. PROVIDÊNCIAS PRÉVIAS À CONTRATAÇÃO (ART. 18, §1º, X)

Para o pleno sucesso da contratação, deverão ser adotadas as seguintes providências:

Inclusão no PCA: tão logo concluído o Plano de Contratações Anual do ITERPA, a presente contratação será nele incluída, na forma do item 2 deste Estudo.

Reserva orçamentária: indicação formal do programa de trabalho, da fonte de recursos e do elemento de despesa, com cobertura distribuída entre os exercícios financeiros alcançados pela vigência do contrato.

Designação e capacitação dos fiscais: designação formal dos fiscais técnico e administrativo do contrato, com treinamento prévio em gestão e fiscalização de contratos de TIC, nos termos do art. 18, §1º, X, da Lei nº 14.133/2021, e capacitação operacional da equipe do NTI sobre as ferramentas da solução, conforme item 3.3.

Plano de transição com a contratação emergencial: elaboração de cronograma de migração da contratação emergencial em curso (art. 75, VIII, da Lei nº 14.133/2021) para a nova solução, com operação simultânea durante a janela de transição e procedimentos de retorno seguro à configuração anterior em caso de falha, de modo a preservar a continuidade da proteção.

Infraestrutura física: verificação das condições de energia elétrica, climatização e cabeamento estruturado da sala técnica do ITERPA, conforme inspeção já realizada pela equipe do NTI, que atestou compatibilidade com os equipamentos a serem instalados, dispensando adequações estruturais.

11. CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES (ART. 18, §1º, XI)

Identificam-se as seguintes contratações correlatas, que devem ser monitoradas para garantir a plena fruição do objeto:

Link de dados corporativo: a operação do firewall NGFW e do serviço de EDR depende de conectividade de internet estável e com largura de banda adequada. Recomenda-se verificar a vigência e a adequação do contrato de link de dados do ITERPA.

Manutenção do sistema de climatização e energia: a operação dos equipamentos exige ambiente climatizado e fornecimento de energia elétrica estável, devendo ser assegurada a regularidade das contratações de manutenção predial correspondentes.

Contratação emergencial em curso: a transição da contratação emergencial fundada no art. 75, VIII, da Lei nº 14.133/2021 para a presente solução estrutural deverá observar cronograma específico, conforme detalhado no item 10 (Providências prévias à contratação) deste Estudo, com operação simultânea das duas soluções durante a janela de migração.

12. IMPACTOS AMBIENTAIS E MEDIDAS DE MITIGAÇÃO (ART. 18, §1º, XII)

Em atenção ao art. 18, §1º, XII, da Lei nº 14.133/2021, ao Decreto Estadual nº 4.193/2024, ao Guia Nacional de Contratações Sustentáveis da AGU (7ª edição, 2024, Item 40 – Tecnologia da Informação e Comunicação, p. 273-281), à IN SGD/ME nº 94/2022 (art. 16, I, “g”) e à Portaria SGD/MGI nº 2.751/2023, identificam-se os seguintes impactos ambientais e respectivas medidas mitigadoras:

12.1. Segurança, compatibilidade eletromagnética e eficiência energética dos equipamentos

A contratação envolve a instalação e operação de equipamentos de informática (firewall, switches e pontos de acesso) nas dependências do ITERPA. O Termo de Referência deverá exigir que os equipamentos atendam aos requisitos de segurança para o usuário e instalações, compatibilidade eletromagnética e eficiência energética, conforme parâmetros estabelecidos na Portaria INMETRO nº 170/2012. Por tratar-se de certificação voluntária, admitir-se-á a comprovação por certificado do fabricante, laudo pericial, ficha técnica (datasheet) ou outro meio válido de prova, nos termos do art. 42, §1º, da Lei nº 14.133/2021 e do Guia da AGU (p. 280-281).

12.2. Substâncias perigosas – Diretiva RoHS

Os equipamentos fornecidos não poderão conter substâncias perigosas em concentração acima da recomendada pela diretiva RoHS (Restriction of Certain Hazardous Substances), conforme art. 5º, IV, da IN SLTI/MPOG nº 01/2010, a saber: mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenilas polibromadas (PBBs) e éteres difenílicos polibromados (PBDEs). A comprovação poderá ser feita mediante certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova que ateste o cumprimento da exigência, nos termos do art. 5º, §1º, da IN SLTI/MPOG nº 01/2010 e do Guia da AGU (p. 275-277).

12.3. Resíduos eletroeletrônicos e logística reversa

Os equipamentos do parque legado, substituídos em razão desta contratação, deverão ter destinação ambientalmente adequada, em conformidade com a Lei nº 12.305/2010 (Política Nacional de Resíduos Sólidos), com o Decreto nº 10.936/2022 e com o Decreto nº 10.240/2020. Caberá à contratada a obrigação de recolhimento dos equipamentos substituídos e seu encaminhamento a entidades recicladoras credenciadas, com apresentação de declaração de destinação ambientalmente adequada ao Instituto. A obrigação será detalhada no Termo de Referência.

12.4. Cadastro Técnico Federal de Atividades Potencialmente Poluidoras (CTF/APP)

Os fabricantes dos equipamentos fornecidos deverão estar registrados no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais (CTF/APP), instituído pela Lei nº 6.938/1981 e regulamentado pela IN IBAMA nº 6/2013, na categoria “Indústria de Material Elétrico, Eletrônico e Comunicações” (código 5-2). A comprovação do registro será exigida no Termo de Referência.

12.5. Sustentabilidade institucional

A contratada adotará as boas práticas de sustentabilidade ambiental previstas no Decreto Estadual nº 4.193/2024 (arts. 5º e 22), incluindo a utilização de tecnologias menos agressivas ao meio

ambiente, a destinação ambientalmente adequada dos resíduos gerados na execução do contrato (peças substituídas, embalagens) e, quando aplicável, a elaboração de Plano de Gerenciamento de Resíduos Sólidos.

13. POSICIONAMENTO CONCLUSIVO (ART. 18, §1º, XIII)

Considerando os estudos acima dispostos, declara-se viável a contratação de solução integrada de segurança de rede para o ITERPA, pelos seguintes fundamentos:

Viabilidade técnica: a solução atende aos requisitos de proteção do perímetro da rede, conectividade interna, controle de autenticação e detecção e resposta a ameaças nos computadores e servidores do Instituto, em padrões compatíveis com o cenário atual de ameaças cibernéticas e com a criticidade do acervo digital sob custódia do órgão, em especial do SICARF.

Viabilidade econômica: o modelo integrado apresenta custo inferior ao das alternativas de aquisição fragmentada (16% inferior) e de contratação em nuvem (28% inferior), respeitando o princípio da economicidade (art. 5º da Lei nº 14.133/2021) e a capacidade orçamentária efetiva do ITERPA, demonstrada na lei orçamentária do exercício.

Viabilidade jurídica: a contratação observa os princípios da eficiência (art. 37, caput, da CF/88) e da continuidade do serviço público, encontra amparo nos arts. 6º (XV), 18, 40 (§2º) e 107 da Lei nº 14.133/2021, e assegura conformidade com a LGPD.

Viabilidade socioambiental: a solução incorpora práticas de sustentabilidade (Decreto Estadual nº 4.193/2024, Guia Nacional da AGU, Lei nº 12.305/2010), com logística reversa do parque legado e equipamentos com eficiência energética superior à do parque atual.

A não contratação resultaria na perpetuação da descobertura cibernética, mitigada apenas pela contratação emergencial em curso, cuja vigência é limitada por imposição legal (art. 75, §6º, da Lei nº 14.133/2021), e cuja expiração sem solução estrutural conduziria o Instituto a novo estado de exposição, com risco concreto ao acervo fundiário do Estado do Pará e à segurança jurídica das titulações já expedidas.

Belém (PA), 17 de setembro de 2026.

Potyguara Prazeres de O. Ferreira

Coordenador do Núcleo de Tecnologia da Informação – NTI/ITERPA

Matrícula nº 54185591/7

Igor Alves Quadros

Analista de Sistemas do Núcleo de Tecnologia da Informação – NTI/ITERPA

Matrícula nº 5958069/1

APÊNDICE 1 – REFERÊNCIAS DE PREÇOS E FONTES DE CONSULTA

1. Metodologia de atualização de valores

Para atualização dos preços históricos (2022-2024), aplicou-se o IPCA acumulado, nos termos do art. 4º, §3º, do Decreto Estadual nº 2.734/2022, que admite o emprego de índice de atualização de preços correspondente. Para componentes cujas exigências técnicas não existiam nos editais de referência – especialmente firewalls com capacidade de inspecionar tráfego criptografado nos protocolos mais recentes e pontos de acesso sem fio do padrão Wi-Fi 6 com gerenciamento centralizado em ambiente computacional restrito do fabricante –, aplicou-se margem adicional de 5% a 8% sobre os valores atualizados, mediante justificativa técnica fundamentada, conforme permitido pelo art. 5º, §1º, do referido Decreto.

2. Tabela de referências

Componente	Órgão	Edital/Contrato	Valor Referência /uni. (R\$)	Fonte
Firewall NGFW	AGENCIA NACIONAL DE MINERACAO (ANM)	Contrato nº00073/2025	1.336.692,595	PNCP
Firewall NGFW	TRIBUNAL SUPERIOR ELEITORAL (TSE)	Contrato nº 35/2026	1.688.411,50	PNCP
Firewall NGFW	INSTITUTO FEDERAL DE EDUCACAO, CIENCIA E TECNOLOGIA DO RIO GRANDE DO NORTE (IFRN).	EDITAL - PREGAO 204.2026	972.624,98	PNCP
Firewall NGFW	IGEPREV	Contrato nº59/Pregão025/2021	1.209.250,00	igepps.pa.gov.br
Switch PoE+	CONAB-COMPANHIA NACIONAL DE ABASTECIMENTO	PROCESSO N.º 21200.006578/2024-79	43.639,88	Gov.br
Switch PoE+	TJ-PI	Sei: 23.0.000083685-0 ata 6/2024/tj-pi Licitação: 72 / 2023	56.300,00	tjpi.jus.br
Switch PoE+				

	COMANDO DA AERONÁUTICA (COMAER)	Pregão eletrônico nº 90005/2025	24.266,40	comprasnet.gov.br
Switch de fibra	JUSTICA FEDERAL DE PRIMEIRA INSTANCIA	Edital nº 90001/2026	248.000,00	PNCP
Switch de fibra	(UO) ESP-PRODESP-CIA.PROC DE DADOS EST. SP	Edital nº 90003/2025	515.000,00	PNCP
Switch de fibra	TRIBUNAL SUPERIOR DO TRABALHO	Edital nº 90007/2026	495.732,91	PNCP
Ponto de acesso Wi-Fi 6	MINISTERIO DA SAUDE	Edital nº 90120/2026	5.860,00	PNCP
Ponto de acesso Wi-Fi 6	SECRETARIA DE ESTADO DA ADMINISTRACAO	Edital nº 525/2025	8.081,665	PNCP
Ponto de acesso Wi-Fi 6	INSTITUTO FEDERAL DE EDUCACAO, CIENCIA E TECNOLOGIA DE SAO PAULO	Edital nº 158/2026	7.011,00	PNCP
Ponto de acesso Wi-Fi 6	ESTADO DE GOIAS	Edital nº 121642/2026	9.527,20	PNCP
Serviço de EDR	MINISTERIO DA CIENCIA, TECNOLOGIA E INOVACOES	Contrato nº 00009/2024	30.325,00	PNCP
Serviço de EDR	CONSELHO FEDERAL DE PSICOLOGIA	Edital nº 12/2026	29.100,00	PNCP
Serviço de EDR	MINISTERIO DA CIDADANIA	Edital nº 90005/2026	39.107,64	PNCP

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951

CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com

Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

3. Metodologia de cálculo da estimativa

A pesquisa de preços baseou-se, em ordem de prioridade (art. 4º, §1º, do Decreto Estadual nº 2.734/2022): (a) Banco Referencial do SIMAS, sem registros diretamente compatíveis com o objeto; (b) Portal Nacional de Compras Públicas – PNCP; (c) contratações similares da Administração Pública, em portais de transparência e atas de registro de preços vigentes, que constituíram a base preponderante. Subsidiariamente, consultaram-se o Painel de Preços do Governo Federal e o Portal Compras.gov.br.

Adotou-se, para obtenção do preço estimado, o método da mediana dos valores compatíveis para cada componente, atualizados conforme item 1 deste Anexo, com fundamento no art. 5º do Decreto Estadual nº 2.734/2022, que autoriza a utilização da média, da mediana ou do menor dos valores obtidos na pesquisa. A escolha da mediana decorre da maior robustez estatística do indicador frente a valores extremos, sem sacrificar a economicidade.

Nesta fase do Estudo Técnico Preliminar não se realizou análise estatística formal da dispersão dos valores coletados nem descarte fundamentado de preços inexequíveis. A análise crítica formal da amostra, com aplicação dos critérios previstos no art. 5º, §2º, do Decreto Estadual nº 2.734/2022, será realizada na fase de elaboração do Termo de Referência.

4. Links das fontes para consulta direta

Item 1. - Firewall de Próxima Geração (NGFW)

Nº	Fonte	Órgão Contratante	Identificação	Data	Valor original (R\$)	Escopo e observações	Situação	Link de Acesso ao Pregão
01	PNCP	SEPLAD	PE nº 90002/2026 https://pncp.gov.br/app/editais/35747782000101/2026/2	29.01.2026	603.280,06	Firewall Aplicação: Segurança Rede Computadores, Modelo: Apliance Ngfw, Suporte, Instalação, Garantia, licenças e operação.	Em andamento.	https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra?compra=92784305900022026
02	PNCP	AGENCIA NACIONAL DE MINERACAO (ANM)	Contrato nº 00073/2025 https://pncp.gov.br/app/contratos/29406625000130/2025/94	21/11/2025	1.408.874,00	Firewall Aplicação: Segurança Rede Computadores, Modelo: Apliance Ngfw, Suporte, Instalação, Garantia, licenças e operação	Aceite.	https://pncp.gov.br/app/editais/29406625000130/2025/78
03	PNCP	TRIBUNAL SUPERIOR ELEITORAL (TSE)	Contrato nº 35/2026 https://pncp.gov.br/app/contratos/00509018000113/2026/2317	10/07/2026	1.725.556,55	Firewall Aplicação: Segurança Rede Computadores, Modelo: Apliance Ngfw, Suporte, Instalação, Garantia, licenças e operação	Aceite.	https://pncp.gov.br/app/editais/00509018000113/2026/1287
04	PNCP	IFRN	EDITAL - PREGAO 204.2026 https://pncp.gov.br/app/editais/10877412000168/2026/222	25/08/2026	994.022,73	Firewall Aplicação: Segurança Rede Computadores, Modelo: Apliance Ngfw, Suporte, Instalação, Garantia, licenças e operação	Em andamento.	https://pncp.gov.br/app/editais/10877412000168/2026/222
05	igepps.pa.gov.br	IGEPREV	Contrato nº 59 / Pregão 025/2021 https://www.igepps.pa.gov.br/sites/default/files/CONTRATO%20ADMINISTRATIVO%20N%C2%BA%20059.2021%20-%20IT%20PROTECT%20-%20EQUIPAMENTOS%20DE%2	10/01/2022	1.493.423,75	Firewall Aplicação: Segurança Rede Computadores, Modelo: Apliance Ngfw, Suporte, Instalação, Garantia, licenças e operação	Concluído.	https://www.igepps.pa.gov.br/contratos-administrativos-2021

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
 CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
 Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

Nº	Fonte	Órgão Contratante	Identificação	Data	Valor original (R\$)	Escopo e observações	Situação	Link de Acesso ao Pregão
			0INFORM%C3%81TICA_compresed.pdf					

Item 2. - Comutador de acesso PoE+ de 48 portas Gigabit

Nº	Fonte	Órgão Contratante	Identificação	Data	Valor original (R\$)	Situação	Escopo e observações	Portal de Consulta
01	Gov.br	CONAB - COMPANHIA NACIONAL DE ABASTECIMENTO	PROCESSO N.º 21200.006578/2024- 79	15/10/2025	43.639,88	Concluído	Aquisição de Switch acesso 48 portas PoE+	https://www.gov.br/conab/pt-br/aceso-a-informacao/licitacoes-e-contratos/licitacoes/matriz/edital-de-pregao-eletronico-srp-conab-matriz-no-90-017-2025-ativos-de-rede-switches/edital-de-pregao-eletronico-srp-conab-matriz-no-90-017-2025-ativos-de-rede-switches
02	tjpi.jus.br	TJ-PI	SEI: 23.0.000083685- 0 ATA 6/2024/TJ-PI Licitação: 72 / 2023	05/12/2023	56.300,00	homologado	Aquisição de Switch acesso 48 portas PoE+	https://www.tjpi.jus.br/transparencia/licitacoes/860
03	comprasnet.gov.br	Comando da Aeronáutica (COMAER)	Pregão Eletrônico Nº 90005/2025	06/03/2025	24.266,40	Concluído	Aquisição de Switch acesso 48 portas PoE+	https://www.comprasnet.gov.br/aceso.asp?url=/edital-120071-5-90005-2025

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

Item 3. - Comutador de núcleo de 24 portas de fibra óptica SFP+

Nº	Fonte	Órgão Contratante	Identificação	Data	Valor original (R\$)	Situação	Escopo e observações	Portal de Consulta
01	PNCP	JUSTICA FEDERAL DE PRIMEIRA INSTANCIA	Edital nº 90001/2026 https://pncp.gov.br/app/editais/00508903000188/2026/72	14/01/2026	248.000,00	Concluído	SWITCH 24 PORTA SFP+	https://pncp.gov.br/app/editais/00508903000188/2026/72
02	PNCP	(UO) ESP-PRODESP-CIA.PROC DE DADOS EST. SP	Edital nº 90003/2025 https://pncp.gov.br/app/editais/62577929000135/2025/5	14/02/2025	515.000,00	Concluído	SWITCH 24 PORTA SFP+ para Datacenter	https://pncp.gov.br/app/editais/62577929000135/2025/5
03	PNCP	TRIBUNAL SUPERIOR DO TRABALHO	Edital nº 90007/2026 https://pncp.gov.br/app/editais/00509968000148/2026/999	25/08/2026	495.732,91	Concluído	SWITCH CORE 100G 4 BAIAS. Datacenter	https://pncp.gov.br/app/editais/00509968000148/2026/999

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

Item 4. - Ponto de acesso sem fio Wi-Fi 6

Nº	Fonte	Órgão Contratante	Identificação	Data	Valor original (R\$)	Situação	Escopo e observações	Portal de Consulta
01	PNCB	MINISTERIO DA SAUDE	Edital nº 90120/2026 https://pncp.gov.br/app/editais/00394544000185/2026/729	23/04/2026	5.860,00	Concluído	Ponto De Acesso Tipo: Wi-Fi 6, Dual Band Simultâneo, Padrão: Ieee 802.11 Ax/Ac/N/G/B/A, Características Adicionais: Múltiplos Ssids; Autenticação Em Wpa3, Porta Uplink, Velocidade Wireless: 5ghz: 1000 Mbps E 2.4ghz :500MBPS, Frequencia Nominal: 2.4 E 5.0GHZ.	https://pncp.gov.br/app/editais/00394544000185/2026/729
02	PNCB	SECRETARIA DE ESTADO DA ADMINISTRACAO	Edital nº 525/2025 https://pncp.gov.br/app/editais/82951351000142/2025/518	07/07/2025	8.081,665	Concluído	PONTO DE ACESSO PONTO DE ACESSO - À REDE SEM FIO Ponto de Acesso Sem Fio Indoor Wi-Fi6	https://pncp.gov.br/app/editais/82951351000142/2025/518
03	PNCB	INSTITUTO FEDERAL DE EDUCACAO, CIENCIA E TECNOLOGIA DE SAO PAULO	Edital nº 158/2026 https://pncp.gov.br/app/editais/10882594000165/2026/424	13/08/2026	7.011,00	Andamento	Ponto De Acesso tipo: wi-fi 6, dual band simultâneo, padrão: ieee 802.11 ax/ac/n/g/b/a, características adicionais: múltiplos ssids; autenticação em wpa3, porta uplink, velocidade wireless: 5ghz: 1000 mbps e 2.4ghz :500, frequencia nominal: 2.4 e 5.0 FortiAP FAP-231K + FortiCare 60 meses (SKU: FAP-231K + FC-10-P231K-247-02-60)	https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra?compra=15815405001582026
04	PNCB	ESTADO DE GOIAS	Edital nº 121642/2026 https://pncp.gov.br/app/editais/01409580000138/2026/1188	03/08/2026	9.527,20	Andamento	Access Point (Ponto de Acesso), WI-FI 6, com acessórios, cabos e softwares necessários para funcionamento do equipamento.	https://pncp.gov.br/app/editais/01409580000138/2026/1188

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
 CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
 Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

Item 5. - Serviço continuado de detecção e resposta (EDR)

Nº	Fonte	Órgão Contratante	Identificação	Data	Valor original (R\$)	Situação	Escopo e observações	Link de Acesso ao Pregão
01	PNCP	MINISTERIO DA CIENCIA, TECNOLOGIA E INOVACOES	Contrato nº 00009/2024 https://pncp.gov.br/app/contratos/01263896000164/2024/472	27/11/2024	30.325,00	Aceite	licenças de solução de segurança com detecção e resposta (EDR- Endpoint Detection and Response) para servidores, laptops e desktops Windows, Linux e macOS, com gerenciamento centralizado. Serviço de instalação do agente da solução EDR nos endpoints Windows, Linux e macOS. Serviço de implantação do ambiente da central de gerência, administração e monitoramento. Serviço de suporte para a solução de EDR. Serviço de Treinamento para a solução de EDR.	https://pncp.gov.br/app/editais/01263896000164/2024/850
02	PNCP	CONSELHO FEDERAL DE PSICOLOGIA	Edital nº 12/2026 https://pncp.gov.br/app/editais/00393272000107/2026/19	01/07/2026	29.100,00	Em andamento	Central Managed Detection and Response Complete (MDR) for Users com agentes de proteção EDR e XDR. Instalação e Configuração	https://pncp.gov.br/app/editais/00393272000107/2026/19
03	PNCP	MINISTERIO DA CIDADANIA	Edital nº 90005/2026 https://pncp.gov.br/app/editais/05526783000165/2026/19	13/04/2026	39.107,64	ACEITE	Licenciamento de Proteção de Endpoints (EDR) para estações de trabalho, incluindo telemetria, análise comportamental, detecção de ameaças avançadas, resposta remota e integração com XDR. Licenciamento de Proteção de Servidores Windows e Linux (EDR/XDR Server), incluindo monitoramento de integridade, mitigação automática e proteção de workloads físicos/virtuais.	https://pncp.gov.br/app/editais/05526783000165/2026/19

Painel de Preços Federal: <https://paineldeprecos.planejamento.gov.br>.

Portal Nacional de Compras Públicas: <https://pncp.gov.br>.

Portal de Compras Governamentais: <https://www.gov.br/compras>.

Transparência TJ-PA: <https://www.tjpa.jus.br/PortalTransparencia>.

Sistema SIMAS: <https://www.compraspara.pa.gov.br/simas>.

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951
CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com
Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

APÊNDICE 2 – MEMÓRIA DE CÁLCULO

1. Introdução

O presente documento demonstra a metodologia e os cálculos utilizados para a definição dos quantitativos do ETP nº 003/2025-ITERPA, em atendimento ao art. 18, §1º, IV, da Lei nº 14.133/2021. Os quantitativos foram derivados do inventário do parque ativo, das projeções de crescimento da força de trabalho do Instituto e dos parâmetros técnicos de cobertura física das instalações.

2. Dados de referência do ambiente atual

Estações de trabalho ativas: 280 unidades. Servidores físicos e virtuais: 20 unidades. Total de equipamentos a serem protegidos: aproximadamente 300. Pontos de presença física: Sede em Belém, estruturada em 4 blocos administrativos (sendo o quarto bloco com três andares). Taxa média de crescimento projetada da força de trabalho: 10% ao ano. Horizonte de planejamento: 36 meses (vigência inicial da contratação).

3. Dimensionamento dos itens

3.1. Firewall NGFW (quantidade: 2)

A operação em arranjo de alta disponibilidade, com ambos os equipamentos ativos simultaneamente, é requisito técnico definido no item 3.1.1 deste ETP e exige no mínimo 2 (dois) equipamentos físicos, com replicação automática de configurações e do estado das conexões em curso, de modo que a falha de um deles não interrompa o tráfego perimetral. Esta é a configuração mínima recomendada pelos fabricantes do segmento para ambientes que tratam dados sensíveis sob a LGPD.

3.2. Switch PoE+ de 48 portas (quantidade: 25)

Estações ativas: 280. Acréscimo para telefonia IP, câmeras e demais dispositivos PoE: 160. Total de portas de acesso necessárias: 440. Margem de expansão para crescimento projetado (10% ao ano $\times$ 3 anos): aproximadamente 36%, elevando a 598 portas. Capacidade por switch: 48 portas úteis. Cálculo: $598 \div 48 = 12,5$ switches. Reserva técnica para substituição emergencial (6 unidades) e redundância em pontos críticos (6 unidades): 12 unidades. Total: 24,5 arredondado para 25 switches.

3.3. Switch de fibra de 24 portas (quantidade: 2)

A espinha dorsal da rede (backbone) em arranjo redundante, com ambos os equipamentos ativos, exige no mínimo 2 (dois) switches de núcleo, conectados entre si, de modo a preservar a operação em caso de falha de um deles. As 24 portas SFP+ por switch acomodam 12 conexões com os switches

de acesso, 6 conexões para servidores críticos, 2 conexões para o par de firewalls, 2 portas de empilhamento entre os switches e 2 portas de reserva técnica.

3.4. Ponto de acesso Wi-Fi 6 (quantidade: 40)

Cobertura da Sede (distribuída entre os 4 blocos administrativos, contemplando os 3 andares do quarto bloco): 24 unidades. Áreas de alta densidade (auditório, sala de reuniões, recepção): 6 unidades adicionais. Cobertura externa (estacionamento e áreas de circulação): 4 unidades. Reserva técnica e expansão projetada: 6 unidades. Total: 40 pontos de acesso.

3.5. Serviço de EDR (quantidade: 36 meses)

A métrica “mês” reflete a natureza continuada do serviço, cuja vigência é dimensionada pela vigência inicial do contrato (36 meses). O licenciamento será proporcional ao parque atual de equipamentos a proteger (aproximadamente 300, entre computadores e servidores), com previsão de margem para crescimento. O detalhamento individualizado do licenciamento por equipamento será objeto do Termo de Referência.

4. Documentos de suporte

Inventário do parque ativo do NTI/ITERPA (data-base abril/2025); Planta arquitetônica da Sede e das unidades regionais; Relatório de utilização de banda do link corporativo (referência 2024); Despacho do NTI no sequencial 32 do PAE nº 2025/2472424; Documento de Formalização da Demanda (sequencial 02 do mesmo PAE).

5. Conclusão

Os quantitativos foram obtidos mediante metodologia objetiva e reproduzível, considerando o cenário atual e as projeções de crescimento para o horizonte de 36 meses. Os dados de entrada são auditáveis e estão documentados nos relatórios técnicos referenciados, integrando os autos do PAE nº 2025/2472424.

Belém (PA), 17 de setembro de 2026.

Potyguara Prazeres de O. Ferreira

Coordenador do Núcleo de Tecnologia da Informação – NTI/ITERPA

Matrícula nº 54185591/7

Igor Alves Quadros

Analista de Sistemas do Núcleo de Tecnologia da Informação – NTI/ITERPA

Matrícula nº 5958069/1

Instituto de Terras do Pará -ITERPA

Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000 – Tel.: 91 3284-9900 /9951

CNPJ: 05.089495/0001-90 – Site: www.iterpa.pa.gov.br – e-mail: ca.iterpa@gmail.com

Horário de Funcionamento: segunda a sexta-feira, 08 às 17 horas

ANEXO III - MODELO DE DECLARAÇÃO DE ÍNDICES DE LIQUIDEZ

Pregão Eletrônico Nº 90002/2026/ITERPA.

PROCESSO Nº: E-2026/2650481

RAZÃO SOCIAL: _____ **CNPJ:** _____

ANO DE REFERÊNCIA: _____

Ativo Circulante = R\$ 0,00

Realizável a Longo Prazo = R\$ 0,00

Passivo Circulante = R\$ 0,00

Passivo Não Circulante = R\$ 0,00

Ativo Total = R\$ 0,00

ILG = $\frac{\text{Ativo Circulante} + \text{Realizável a Longo Prazo}}$

ILG =

$\frac{\text{Passivo Circulante} + \text{Exigível a Longo Prazo}}$

ILC = $\frac{\text{Ativo Circulante}}$

ILG =

$\frac{\text{Passivo Circulante}}$

ISG = $\frac{\text{Ativo Total}}$

ISG =

$\frac{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$

PL = R\$ 0,00

Cidade (UF), ____/____/____

Nome e assinatura do Representante

Legal da Empresa

ANEXO IV DO EDITAL

DECLARAÇÃO DE NÃO OCORRÊNCIA DE REGISTRO DE OPORTUNIDADE

A empresa _____, inscrita no CNPJ sob o nº _____, por intermédio de seu representante legal, Sr(a) _____, **DECLARA** que para a apresentação de proposta ao Pregão Eletrônico nº 90002/2026-ITERPA, cujo objeto é a **Contratação de empresa especializada na prestação de serviço de outsourcing de Data Center, englobando o fornecimento, a instalação, a configuração, a operação e a manutenção de infraestrutura de Tecnologia da Informação e Comunicação – TIC, na modalidade de serviço gerenciado, destinado a suportar os sistemas e dados institucionais do Instituto de Terras do Pará – ITERPA**, NÃO HOUVE ocorrência de “Registro de Oportunidade”, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública, conforme disposto no Anexo I da Instrução Normativa SGD/ME Nº 94 de 23 de dezembro de 2022 e art. 5º da Lei nº 14.133, de 2021:

“1.7. O órgão ou entidade deverá exigir das empresas licitantes declaração que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio da competitividade, conforme o disposto no art. 5º da Lei nº 14.133, de 2021.”

DECLARA, ainda, estar ciente das **SANÇÕES** sujeitará o licitante às sanções previstas na [Lei nº 14.133, de 2021](#), e no Edital.

Cidade (UF), ____/____/____

Nome e assinatura do Representante

Legal da Empresa

ANEXO V – MINUTA DE TERMO DE CONTRATO
PREGÃO ELETRÔNICO Nº XXXX/2026/ITERPA
CONTRATO ITERPA Nº XXX/2026
PAE nº 2026/2933349

RESUMO



CONTRATANTE

Estado do Pará | Instituto de Terras do Pará – ITERPA
CNPJ nº 05.089.495/0001-90

CONTRATADO

Nome da pessoa jurídica
CNPJ nº xxx.xxx.xxx-xx.



OBJETO

Contratação de empresa especializada para o fornecimento de solução integrada de segurança de rede, abrangendo a entrega, a instalação, a configuração, a integração e a operação dos equipamentos a seguir, acompanhada do serviço continuado de detecção e resposta a ameaças nos computadores e servidores do Instituto de Terras do Pará – ITERPA, conforme quantidades, condições e especificações constantes no Termo de Referência.



LOCAL DE PRESTAÇÃO DO SERVIÇO

O serviço será prestado na sede do órgão, localizado no End. Rod. Augusto Montenegro, km 09 s/n- Bairro: Parque Guajará - Icoaraci – CEP: 66.821-000



VALOR TOTAL

R\$ xxx.xxx,xx.

REAJUSTE

Índice

☒ IPCA

☐ INPC

☐ INCC

☐
IGPM

Período

A cada **12 meses**, a contar de **dd/mm/aaaa** (data do orçamento estimado).

PAGAMENTO

Forma

Ordem bancária.

Prazo

20 dias úteis, 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 xxx.xxx.xxx-xx, matrícula nº nnnn, lotado no [inserir setor]. (Esses dados devem ser inseridos por ocasião da assinatura do contrato).



VIGÊNCIA

Prazo

36 meses.

Início

dd/mm/aaaa (a data deve ser especificada na assinatura do contrato).

Fim

dd/mm/aaaa (a data deve ser especificada na assinatura do contrato).

CLÁUSULAS CONTRATUAIS

CLÁUSULA 1

Partes

Este contrato tem como PARTES:

CONTRATANTE

ESTADO DO PARÁ, por intermédio do INSTITUTO DE TERRAS DO PARÁ-ITERPA, Autarquia, Pessoa Jurídica de Direito Público da Administração Indireta do Estado do Pará, inscrito no CNPJ nº 05.089.495/0001-90, com sede à Rod. Augusto Montenegro, SN, km 09, Bairro Parque Guajará, Distrito – Icoaraci, CEP: 66.821-000, Belém-PA, neste ato representada pelo Presidente do Órgão, Sr. **FLÁVIO RICARDO ALBUQUERQUE AZEVEDO**, CPF: 727.811.222-20.

CONTRATADO

NOME DA RAZÃO SOCIAL DA PESSOA JURÍDICA, CNPJ nº XX.XXX.XXX/XXXX-XX, com sede na [inserir endereço], neste ato representado por [NOME DO REPRESENTANTE DA PJ], RG nº XXXXX, CPF nº XXX.XXX.XXX-XX, com domicílio na [inserir endereço].

CLÁUSULA 2

Fundamento legal

O presente contrato é oriundo do **Pregão Eletrônico nº XXX/2026** constante no PAE nº 2026/2933349 e é regido pela Lei Federal nº 14.133/21.

CLÁUSULA 3

Objeto

3.1 O objeto é a **contratação de empresa especializada para o fornecimento de solução integrada de segurança de rede**, abrangendo a entrega, a instalação, a configuração, a integração e a operação dos equipamentos a seguir, acompanhada do serviço continuado de detecção e resposta a ameaças nos computadores e servidores do Instituto de Terras do Pará – ITERPA, conforme descrito 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 ÚNICO						
Item	Descrição	Qtd	Und	Valor Unitário	Vlr. Unt. (Mensal)	Vlr. Total Anual
1	Firewall NGFW (36 meses)	2	Equipamento			
2	Switch PoE+ 48 portas (36 meses)	25	Equipamento			
3	Switch de fibra 24 portas (36 meses)	2	Equipamento			
4	Ponto de acesso Wi-Fi 6 (36 meses)	40	Equipamento			
5	Serviço de EDR (mensalidade)	36	Mês			
VALOR ESTIMADO MENSAL						
VALOR ESTIMADO ANUAL						

3.4. Vinculam esta contratação, independentemente de transcrição:

3.4.1. O TERMO DE REFERÊNCIA;

3.4.2. O EDITAL DA LICITAÇÃO;

3.4.3. A PROPOSTA DO CONTRATADO; e

3.4.4. Eventuais anexos dos documentos supracitados.

CLÁUSULA 4

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 demais, previstos no Edital do Pregão Eletrônico Nº xxxx/2026/ITERPA, que originou este contrato.

CLÁUSULA 5

Preço

5.1 O valor global do contrato é **R\$ xxx.xxx,xx** 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 6

Dotação orçamentária

6.1 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:

Gestão/Unidade: 560201/56000 - ITERPA
Ação: 295.604
Proj./Ativ.: 21.122.1297.8338 – Operacionalização das ações administrativas
Fonte: 02.756.0000.23
01.756.0000.23
Detalhamento: 000000
Elemento de Despesa: 449040
P.I.: 411.000.8338E

CLÁUSULA 7

Reajuste

7.1 Em estrita observância ao art. 25, §7º, combinado com o art. 92, inciso V, da Lei nº 14.133/2021, fixa-se como índice de reajustamento monetário o Índice Nacional de Preços ao Consumidor Amplo (IPCA), apurado pelo Instituto Brasileiro de Geografia e Estatística (IBGE).

7.2 O reajuste será devido unicamente a cada período de **12 (doze) meses**, contados a partir da data de apresentação da proposta ou da data do orçamento estimado pela Administração, incidindo exclusivamente sobre o saldo contratual remanescente.

7.3 O reajuste se *restringirá* ao valor do *saldo contratual* existente na data em que aquele for devido.

7.4 O reajuste será realizado *de ofício* pelo CONTRATANTE mediante a aplicação do índice de correção monetária mencionado na Cláusula 7.1 na base de cálculo do item 7.3.

7.5 O reajuste será automático e independará de requerimento do CONTRATADO.

7.6 O reajuste será realizado por *simples apostila*.

7.7 No caso de atraso ou não divulgação do índice do item 7.1, o **CONTRATANTE** utilizará a sua última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

7.8 Caso o índice do item 7.1 venha a ser extinto ou não possa mais ser utilizado, as **PARTES** elegerão novo índice, fixando-o por meio de termo aditivo.

7.9 Não será devido reajuste quando o atraso na entrega do bem for atribuível ao **CONTRATADO**.

CLÁUSULA 8

Pagamento

8.1 O pagamento será realizado em **20 dias úteis**, a contar do recebimento da nota fiscal ou fatura atestada pelo fiscal do contrato.

8.2 A forma de medição e pagamento do serviço prestado, será realizado nos termos estabelecidos no TERMO DE REFERÊNCIA, e demais, previstos no Edital (anexo I) do Pregão Eletrônico Nº XXXX/2026/ITERPA, que originou este contrato.

8.3 O pagamento será efetuado por ordem bancária para conta de titularidade da **CONTRATADO**, cujos dados são:

Banco Banpará.

Agência XXXX-X.

Conta XXXXXX-X.

8.3 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.

8.4 Na hipótese do item 8.3, o prazo para pagamento começará a correr depois da comprovação da regularização da pendência, sem ônus à **CONTRATANTE**.

8.5 A data do efetivo pagamento será considerada aquela que constar da ordem bancária emitida para quitação da nota fiscal ou fatura.

8.6 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.

8.7 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.

8.8 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**.

8.9 A instauração do procedimento de inexecução contratual não impede o pagamento do serviço que já foi prestado.

8.10 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.

8.11 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.

8.12 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.

8.13 O **CONTRATANTE** efetuará a retenção tributária prevista na legislação aplicável por ocasião do pagamento.

8.14 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 123/06.

CLÁUSULA 9

Garantia de cumprimento contratual

☒ **9.1** 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, a ser apresentada no prazo de até **10 (dez)** dias úteis contados da assinatura do contrato.

9.2 A garantia corresponderá a **5%** (de acordo com o Termo de Referência) do **valor atualizado** do contrato.

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

Banco	Banpará.
Agência	XXXX-X.
Conta	XXXXXX-X.

9.4 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**.

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

9.6 Se a garantia for utilizada em pagamento de qualquer obrigação, o **CONTRATADO** fica obrigado a recompor o que tiver sido usado no prazo de **10 dias úteis**, a contar de sua notificação.

9.7 O **CONTRATANTE** executará a garantia na forma prevista na legislação.

9.8 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**.

9.9 Quando a garantia for em dinheiro, o valor a ser devolvido, nos termos do item 9.8, será corrigido monetariamente.

9.10 Além da garantia de que tratam os arts. 96 e seguintes da Lei nº 14.133/21, a presente contratação possui previsão de garantia contratual dos bens e dos serviços a serem fornecidos, conforme condições estabelecidas no TERMO DE REFERÊNCIA, e demais, previstos no Edital (anexo I) do Pregão Eletrônico Nº XXXX/2026/ITERPA, que originou este contrato.

CLÁUSULA 10

Obrigações das partes

10.1 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 seja substituído, reparado ou corrigido às suas expensas.
- d.** Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações do **CONTRATADO**.
- e.** Efetuar o pagamento do objeto fornecido no prazo, forma e condições aqui estabelecidos.

- f.** Aplicar ao **CONTRATADO** as sanções decorrentes da inexecução total ou parcial do contrato.
- g.** 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.
- h.** Solicitar à contratada todas as providências necessárias ao bom andamento dos serviços;
- i.** Rejeitar, no todo ou em parte, os serviços executados em desacordo com as respectivas especificações;
- j.** Solicitar a substituição do empregado que não estiver desempenhando suas atividades a contento, de acordo com o estabelecido neste Termo de Referência;
- k.** Notificar a Contratada, por escrito, sobre imperfeições, falhas ou irregularidades constatadas nos serviços prestados, para que sejam adotadas as medidas corretivas necessárias.

10.2 O CONTRATADO tem a obrigação de:

10.2.2 Executar os serviços objeto desta licitação, em total conformidade com o estabelecido a seguir:

- a.** Executar o objeto conforme Termo de Referência.
- b.** Aceitar acréscimos ou supressões unilaterais impostas pelo **CONTRATANTE** de até **25%** do valor atualizado do contrato nas mesmas condições pactuadas inicialmente.
- c.** 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.
- d.** 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.
- e.** Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior e prestar esclarecimentos ou informações por eles solicitados.
- f.** 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.
- g.** 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.

- h.** 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.
- i.** Responsabilizar-se pelo cumprimento das obrigações previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao **CONTRATANTE**.
- j.** Comunicar ao fiscal do contrato, no prazo de **24 horas**, qualquer ocorrência anormal que se verifique no local da execução do objeto contratual.
- k.** Manter durante a vigência do contrato todas as condições exigidas para habilitação na licitação ou para qualificação, na contratação direta.
- l.** Cumprir durante todo o período de execução do contrato a reserva de cargos para pessoa com deficiência, reabilitado da Previdência Social, aprendiz e outras reservas de cargos previstas na legislação.
- m.** Comprovar o cumprimento da alínea acima no prazo fixado pelo fiscal do contrato, indicando os empregados que preencheram as referidas vagas.
- n.** 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.
- o.** Cumprir as normas de segurança do **CONTRATANTE**, além da legislação vigente em âmbito federal, estadual e municipal.
- p.** As obrigações estabelecidas nesta cláusula **não se restringem** às aqui descritas, **abrangendo igualmente todas aquelas previstas, delimitadas e especificadas no TERMO DE REFERÊNCIA, e demais, previstos no edital (anexo I), o qual integra** o presente contrato para todos os fins de direito, devendo ser observado em sua integralidade pelo **CONTRATANTE** e pelo **CONTRATADO**, conforme suas respectivas atribuições.

CLÁUSULA 11

Responsabilidade por danos

11.1 A responsabilidade pelos danos causados por ato do **CONTRATADO**, de seus empregados, prepostos ou subordinado, é exclusivamente do **CONTRATADO**.

11.2 A responsabilidade pelos compromissos assumidos pelo **CONTRATADO** com terceiros é exclusivamente sua.

11.3 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 12

Infrações e sanções administrativas

12.1 Constituem infrações administrativas do **CONTRATADO** a serem punidas com as seguintes sanções:

Infração	Penalidade
	Advertência*
a. Dar causa à inexecução parcial do contrato.	* 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.	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> ”.
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.

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**

12.2 Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

12.2.1 Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

12.2.2 Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c”, “d”, “e” e “f” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

12.2.3 Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “g”, “h”, “i”, “j” e “k” do subitem acima deste Contrato, bem como nas alíneas “b”, “c”, “d”, “e” e “f”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

12.3 O atraso superior a **30 dias corridos** autoriza a rescisão do contrato por seu descumprimento, nos termos do art. 137, I, da Lei Federal nº 14.133/21.

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

12.5 As sanções podem ser *cumuladas* com as seguintes multas:

Multa

Moratória

Compensatória

- a. **0,5% (meio por cento) ao dia, até o máximo de 10% (dez por cento)** sobre o valor da parcela inadimplida por dia de atraso injustificado até o limite de **30 dias corridos**.
- b. **0,5% (meio por cento) ao dia, até o máximo de 10% (dez 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.

12.5.1 Multa:

1. **Compensatória**, para as infrações descritas nas alíneas “g” a “k” do subitem 12.1, de 10% a 20% do valor do Contrato.
2. **Compensatória**, para a inexecução total do contrato prevista na alínea “c” do subitem 12.1, de 10% a 20% do valor do Contrato.
3. Para infração descrita na alínea “b” do subitem 12.1, a multa será de 10% a 20% do valor do Contrato.
4. Para infrações descritas na alínea “f” do subitem 12.1, a multa será de 0,5% a 10% do valor do Contrato.
5. Para a infração descrita na alínea “a” do subitem 12.1, a multa será de 0,5% a 10% do valor do Contrato.

12.6 Antes da aplicação das sanções, o **CONTRATADO** será notificado para apresentar defesa no prazo de **15 dias úteis**, contado de sua intimação.

12.7 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.

12.8 Antes do ajuizamento da cobrança, a multa poderá ser recolhida administrativamente em até **15 dias úteis**, a contar do trânsito em julgado da decisão administrativa.

12.9 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.

12.10 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**.
- e.** A implantação ou aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.11 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.

12.12 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.

12.13 No prazo de **15 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.

12.14 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.

12.15 Constatada irregularidade no procedimento licitatório ou na execução contratual, caso não seja possível o saneamento, a decisão sobre a suspensão da execução ou sobre a declaração de nulidade do contrato somente será adotada na hipótese em que se revelar medida de interesse público, com avaliação dos aspectos indicados no art. 147 da Lei Federal nº 14.133/2021.

CLÁUSULA 13

Alterações do contrato

13.1 As alterações contratuais serão disciplinadas pelo art. 124 e seguintes da Lei Federal nº 14.133/21.

13.2 Caso haja interesse público, o **CONTRATANTE** pode alterar unilateralmente o contrato para impor acréscimos ou supressões de até **25%** do valor atualizado do contrato, mantidas as mesmas condições pactuadas inicialmente.

13.3 As PARTES podem acordar suprimir o objeto do contrato em percentual superior a 25% do valor inicial atualizado do contrato.

13.4 Os acréscimos ou supressões não podem transfigurar o objeto da contratação.

13.5 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 14

Da Subcontratação

14.1 A presente contratação admite subcontratação parcial do objeto, limitada a 30% (trinta por cento) do valor total do contrato, mediante autorização prévia do ITERPA, e será realizado nos termos e condições estabelecidos no TERMO DE REFERÊNCIA, e demais, previstos no Edital (anexo I) do Pregão Eletrônico Nº XXXXX/2026/ITERPA, que originou este contrato.

CLÁUSULA 15

Da Execução e Gestão do Contrato

15.1 Os serviços contratados serão realizados no **regime de serviços continuados, sem dedicação exclusiva de mão de obra**, relacionados ao fornecimento de solução integrada de segurança de rede, estando a licitante obrigada a fornecer solução composta por equipamentos, programas e serviços, na **modalidade de serviço gerenciado**, sendo responsável pela instalação, configuração, integração, operação, administração, monitoramento e manutenção durante toda a vigência do contrato. A solução deverá ser funcional e pronta para uso, observadas, no mínimo, as especificações do TERMO DE REFERÊNCIA, e demais, previstos no Edital (anexo I) do Pregão Eletrônico Nº XXXX/2026/ITERPA;

15.2 O prazo máximo para a execução dos serviços contratados será de **36 (trinta e seis) meses**, sendo que a empresa deverá iniciar os trabalhos a partir da data de assinatura do contrato com o ITERPA e com o aval da supervisão geral da coordenadoria administrativa.

15.3 Demais modelos de gestão e de execução contratual, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no TERMO DE REFERÊNCIA, e demais, previstos no Edital (anexo I) do Pregão Eletrônico Nº XXXXX/2026/ITERPA, que originou este contrato.

CLÁUSULA 16

Extinção do contrato

16.1 O contrato se extingue quando todas as obrigações de ambas as PARTES forem cumpridas, ainda que isso ocorra antes do prazo estipulado.

16.2 Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que o **CONTRATANTE** deverá providenciar a readequação do cronograma fixado para cumprimento do contrato.

16.3 Se a não conclusão do contrato decorrer de culpa do **CONTRATADO**, ele ficará constituído em mora, devendo ser instaurado procedimento de inexecução contratual para a aplicação das sanções administrativas cabíveis.

16.4 Na hipótese do item 17.3, o **CONTRATANTE** poderá optar, ainda, pela extinção do contrato e adotar as medidas previstas em lei para a continuidade da execução do objeto.

CLÁUSULA 17

Fiscalização

17.1 O cumprimento do contrato será fiscalizado pelo servidor **NOME DO SERVIDOR**, CPF nº xxx.xxx.xxx-xx, matrícula nº nnnn, lotado no [inserir setor], conforme ato a ser publicado no Diário Oficial do Estado.

CLÁUSULA 18

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 19

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 121/19.

CLÁUSULA 20

Obrigações Pertinentes à LGPD

20.1 Da Proteção de Dados Pessoais. A CONTRATADA, na qualidade de operadora de dados pessoais, obriga-se a tratar os dados a que tiver acesso em razão deste contrato exclusivamente para o cumprimento de seu objeto e segundo as instruções documentadas do CONTRATANTE, na forma dos arts. 39 e 46 a 49 da Lei nº 13.709/2018, adotando medidas técnicas e administrativas de segurança, entre as quais a criptografia dos dados em repouso e em trânsito, a autenticação multifator para acessos administrativos e a manutenção de registros de auditoria.

§1º A CONTRATADA comunicará ao CONTRATANTE, no prazo máximo de 24 (vinte e quatro) horas, qualquer incidente de segurança que possa acarretar risco ou dano aos titulares, cooperando na comunicação à Autoridade Nacional de Proteção de Dados e aos titulares afetados, nos termos do art. 48 da referida Lei.

§2º Extinto o contrato, a CONTRATADA, conforme instrução do CONTRATANTE, eliminará ou devolverá os dados pessoais tratados, ressalvada a conservação exigida por obrigação legal, vedado o compartilhamento com terceiros sem autorização expressa.

§3º A CONTRATADA responderá pelos danos decorrentes de tratamento realizado em desconformidade com a legislação de proteção de dados, sem prejuízo das sanções contratuais cabíveis.”

20.2 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.

20.3 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.

20.4 É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

20.5 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.

20.6 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.

20.7 É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

20.8 O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

20.9 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.

20.10 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.

20.11 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.

20.12 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 21

Divulgação e publicação

21.1 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**.

21.2 Os prazos contidos no item 21.1 são contados da data da assinatura do contrato.

CLÁUSULA 22

Vigência

22.1 O contrato terá vigência de **36 meses**, a contar da assinatura do contrato, podendo ser prorrogado sucessivamente, respeitada a vigência máxima decenal (10 anos), na forma do artigo 107 da Lei 14.133 de 2021.

22.2 Quando o objeto não for concluído no período acima fixado, o prazo de vigência do contrato será *automaticamente prorrogado*, sem prejuízo da aplicação dos itens 16.3 e 16.4, quando a não conclusão decorrer de culpa do **CONTRATADO**.

22.3 Antes da prorrogação da vigência do contrato, o **CONTRATANTE** deverá verificar a regularidade fiscal do **CONTRATADO**, consultar o CEIS e o CNEP, emitir as certidões negativas de inidoneidade, de impedimento e de débitos trabalhistas e juntá-las ao respectivo processo.

CLÁUSULA 23

Foro

23.1 As PARTES elegem o foro da **Comarca de Belém, Estado do Pará** para resolver os litígios oriundos deste contrato, observado o disposto na **Cláusula 19**.

Cidade (PA), 30 de setembro de 2026.

FLÁVIO RICARDO ALBUQUERQUE

AZEVEDO

Presidente do ITERPA

Contratante

NOME DO CONTRATADO

Nome do representante, se não for PF

Contratado

NOME DA TESTEMUNHA

RG: xxxxxxxx PC/UF

CPF: xxx.xxx.xxx-xx

Testemunha

NOME DA TESTEMUNHA

RG: xxxxxxxx PC/UF

CPF: xxx.xxx.xxx-xx

Testemunha