

PREGÃO ELETRÔNICO Nº 90016/2025/ADEPARÁ
PAE nº 2025/3141716

RESUMO



PROMOTOR

Agência de Defesa Agropecuária do Estado do Pará (ADEPARÁ)
CNPJ nº 05.470.347/0001-11.



OBJETO

Empresa especializada para na Prestação de Serviços de Atividade de Execução Continuada, pelo período de 12 meses, compreendendo:

- Solução de Firewall de próxima Geração;
- Solução SD-WAN;
- Serviço de Proteção das Estações de Trabalho e Servidores de Rede (antivírus)
- Serviço de Gestão de Backups;
- Serviço de Conectividade Wifi;
- Serviços Técnicos Especializados.



MÉTODO DE DISPUTA

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



CRITÉRIO DE JULGAMENTO

- ☒ Menor preço
- ☐ Maior desconto



ENTREGA

Forma Em parcela única.

Prazo **30 dias corridos** após a emissão da nota de empenho.

Local Sede administrativa da ADEPARÁ: Tv. da Estrella, 1184
- Pedreira, Belém - PA, 66080-008.

VALOR TOTAL

R\$ 1.445.670,96



REAJUSTE

Índice ☐ IPCA ☐ INCC ☐ Outro: (sigla)
☐ INPC ☒ IGPM

Período A cada **12 meses**, a contar de XX/XX/XX (data do orçamento estimado).

PAGAMENTO

Forma Ordem bancária.

Prazo **30 dias corridos**, a contar do recebimento da nota fiscal ou fatura atestada pelo fiscal do contrato.



ABERTURA DA SESSÃO PÚBLICA

Data 05/12/2025.

Hora 10:00 hrs.

SUMÁRIO

CLÁUSULA 1	
Promotor do pregão	4
CLÁUSULA 2	
Fundamento legal	4
CLÁUSULA 3	
Objeto	4
CLÁUSULA 4	
Condições para participar da licitação	6
CLÁUSULA 5	
Fases da licitação, apresentação da proposta e documentos de habilitação	8
CLÁUSULA 6	
Preenchimento da proposta	11
CLÁUSULA 7	
Abertura da sessão, classificação das propostas e formulação de lances	12
CLÁUSULA 8	
Julgamento das propostas	17
CLÁUSULA 9	
Habilitação	20
CLÁUSULA 10	
Adjudicação e homologação	24
CLÁUSULA 11	
Recursos	24
CLÁUSULA 12	
Infrações e sanções administrativas	25
CLÁUSULA 13	
Impugnação ao edital	28
CLÁUSULA 14	
Disposições finais	29

REGULAMENTO DA COMPETIÇÃO

CLÁUSULA 1

Promotor do pregão

O PROMOTOR deste pregão é o **AGÊNCIA DE DEFESA AGROPECUÁRIA DO ESTADO DO PARÁ** (ADEPARÁ), CNPJ nº 05.470.347/0001-11, com sede na Travessa Estrella 1184, neste ato representado pelo JAMIR JUNIOR PARAGUASSU MACEDO, Diretor Geral.

CLÁUSULA 2

Fundamento legal

A presente licitação será realizada por meio de **PREGÃO ELETRÔNICO** e observará a Lei Federal nº 14.133/21, Decreto Estadual nº Decreto Estadual nº 2.939/23, o Decreto Estadual nº 3.037, de 25 de abril de 2023, Lei Complementar Federal nº 123/06, Portaria nº 77/2024 – ADEPARA de 25 de janeiro de 2024, que designam Agentes de Contratação, 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 na Prestação de Serviços de Atividade de Execução Continuada, pelo período de 12 meses, compreendendo:** ▪ **Serviço de Firewall de próxima geração;** ▪ **Solução SD-WAN;** ▪ **Serviço de Proteção das Estações de Trabalho e Servidores de Rede (antivírus)** ▪ **Serviço de Gestão de Backups;** ▪ **Serviço de Conectividade Wifi; Serviços Técnicos Especializados.**

3.1.1 A especificação técnica dos materiais no arquivo PDF a ser baixada juntamente com o Edital no Comprasnet (Relação de Itens) geralmente é obtida a partir de aproximações do CATMAT/CATSER, não sendo editável, em alguns casos, pelo órgão promotor do certame. Portanto, sempre que tal especificação não corresponder à descrição do Termo de Referência – TR, prevalecerá a que consta do TR.

3.2 Os serviços a serem licitados são os seguintes itens descritos no TR:

Lote	Item	Descrição	Und	Qtd	Valor unitário	Total
1	1	Serviço de Firewall de próxima geração	Meses	12	R\$ 31.100,04	R\$ 373.200,48

	2	Serviço SD-WAN	Meses	12	R\$ 41.429,19	R\$ 497.150,28
	3	Serviços de Proteção das Estações de Trabalho e Servidores de Rede (Antivírus)	Meses	12	R\$ 10.506,70	R\$ 126.080,40
	4	Serviço de Gestão de Backups	Meses	12	R\$ 3.954,25	R\$ 47.451,00
	5	Serviço de Conectividade Wifi	Meses	12	R\$ 13.711,15	R\$ 164.533,80
	6	Serviços Técnicos Especializados	Meses	12	R\$ 19.771,25	R\$ 237.255,00
				VALOR TOTAL ESTIMADO	R\$ 1.445.670,96	

3.3 A licitação observará o seguinte:

- ☒ **Lote único**, formados por 6 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, excluía 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. Será concedido tratamento favorecido para as MEs, EPPs, para as sociedades cooperativas mencionadas no artigo 16 da Lei Federal nº 14.133/21, para o agricultor familiar, o produtor rural pessoa física e para o Microempreendedor Individual (MEI), nos limites previstos da Lei Complementar Federal nº 123/06 e na Lei Estadual nº 8.417/16.

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 abertura da sessão pública.

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 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.

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

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

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

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

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

5.10 O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser

alterado pelo LICITANTE durante a fase de disputa, sendo proibido:

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

5.11 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.

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

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

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 global do lote.
- 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 90 (noventa) dias, a contar da data de sua apresentação.

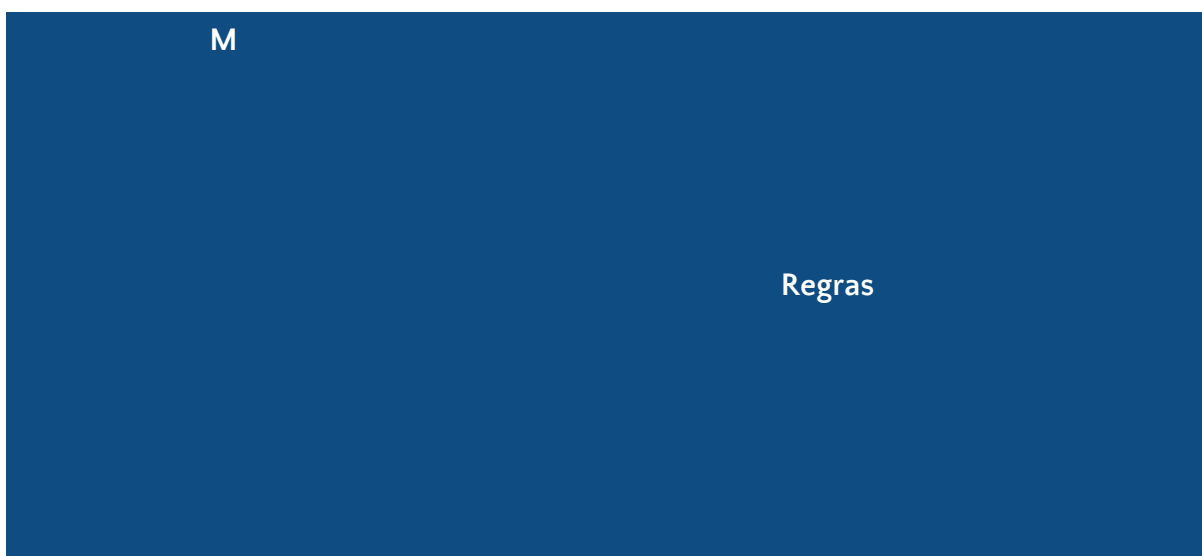
6.9 Os LICITANTES devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas:

- 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

- 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:
- 7.9.1** O lance deverá ser ofertado pelo valor do grupo.
- 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 será de R\$0,10 (dez centavos).
- 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 inexecutável.

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



- 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*.

7.15 Após o término dos prazos estabelecidos no [item 7.14](#), o sistema ordenará e divulgará os lances segundo a ordem *A ordem será crescente* 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:

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

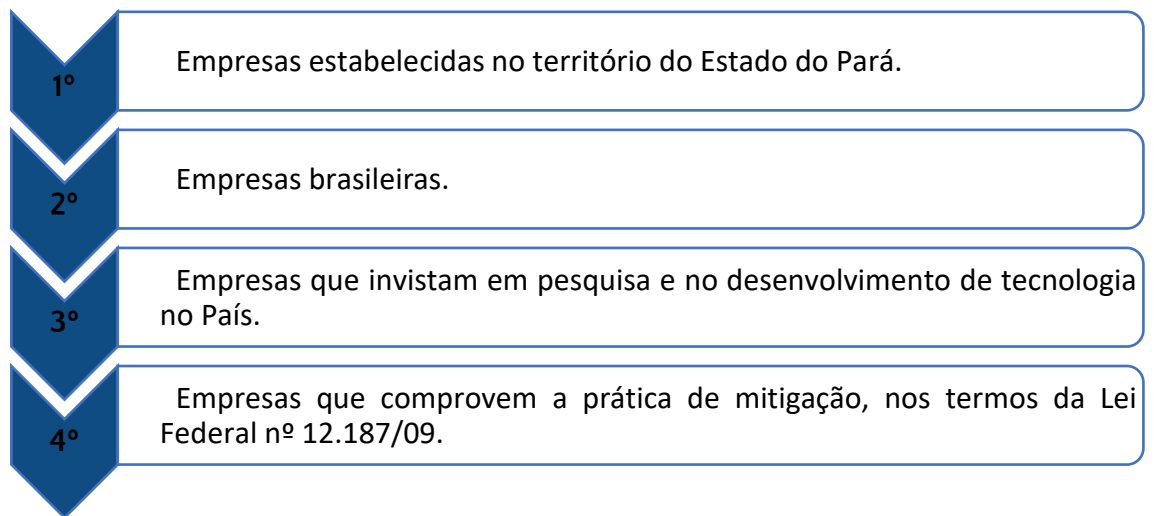
Desenvolvimento de ações de equidade entre homens e mulheres no ambiente de trabalho

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 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 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 da empresa LICITANTE e de seu sócio majoritário, considerando a proibição do art. 12 da Lei Federal nº 8.429/92.

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 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.

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

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

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

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

8.13 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.

CLÁUSULA 9

Habilitação

9.1 Os documentos previstos no TR serão exigidos para habilitação do LICITANTE.

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.

9.2.1 – A habilitação jurídica visa a demonstrar a capacidade de o licitante exercer direitos e assumir obrigações, e a documentação a ser apresentada por ele limita-se à comprovação de existência jurídica da pessoa e, quando cabível, de autorização para o exercício da atividade a ser contratada art. 66 da Lei nº 14.133/2021.

9.2.2 As habilitações Fiscal (Federal, Estadual e Municipal), social e Trabalhista serão aferidas mediante a verificação dos requisitos dispostos no art. 68 da Lei nº 14.133/2021, conforme a seguir a seguir:

9.2.2.1 A inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ);

9.2.2.2 A inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.2.2.3 A regularidade perante a Fazenda Federal, Estadual e/ou Municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

9.2.2.4 A regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

9.2.2.5 A regularidade perante a Justiça do Trabalho;

9.2.2.6 O cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal.

9.2.3. Para fins de demonstração da habilitação Econômico-Financeira, o licitante vencedor deverá apresentar (art. 69 da Lei nº 14.133/2021):

9.2.3.1 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;

9.2.3.2 As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e ficarão autorizadas a substituir os demonstrativos contábeis pelo Balanço de Abertura.

9.2.3.3. A comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um) resultantes da aplicação das fórmulas:

$$LG = (\text{Ativo Circulante} + \text{Realizável a Longo Prazo}) / (\text{Passivo Circulante} + \text{Passivo Não Circulante});$$
$$SG = (\text{Ativo Total}) / (\text{Passivo Circulante} + \text{Passivo não Circulante})$$
$$\text{e } LC = (\text{Ativo Circulante}) / (\text{Passivo Circulante}).$$

9.2.3.4. O Licitante que apresentar resultado igual ou menor que 1 (um), em qualquer dos índices citados no item acima, quando da habilitação, deverá comprovar, considerados os riscos para a ADEPARA, o Capital ou Patrimônio Líquido mínimo equivalente a 10% (dez por cento) do valor estimado para a contratação (§ 4º do art. 69 da Lei nº 14.133/2021).

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

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

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 Em caso 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.

9.12 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.

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 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.

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

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

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, deve-se observar o seguinte:

- a. A intenção de recorrer deverá ser manifestada imediatamente, sob pena de não ser possível apresentar o recurso; e
- b. 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

Infrações e sanções administrativas

12.1 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 manter a proposta, em especial quando:	Impedimento de licitar e contratar*
1. Não enviar a proposta adequada ao último lance ofertado ou após a negociação;	* Exceto quando se justificar a imposição de penalidade mais grave, ocasião em que poderá ser aplicada a sanção de “Declaração de

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;	<i>inidoneidade para licitar e contratar”.</i>
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;	Multa 15% a 30% do valor do contrato licitado. <i>e</i> Declaração de inidoneidade para licitar e contratar

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

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

12.3. As sanções previstas no [item 12.1](#) não excluem as responsabilidades civil e criminal dos envolvidos.

12.4 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.

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

12.6 As sanções poderão ser aplicadas cumulativamente ou não com a penalidade de multa.

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

12.9 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.

12.10 A duração da sanção de declaração de inidoneidade para licitar ou contratar observará o prazo previsto no art. 156, § 5º, da Lei Federal nº 14.133/21.

12.11 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 do item 12.1](#), caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do PROMOTOR.

12.12 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.

12.13 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.

12.14 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.

12.15 O recurso a que se refere o [item 12.13](#) deverá ser decidido no prazo máximo de 20 dias úteis, contado do seu recebimento.

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

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

CLÁUSULA 13

Impugnação ao edital

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

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

13.3 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.

13.4 A impugnação e a solicitação de esclarecimento poderão ser realizadas por meio eletrônico, através do e-mail: licitacao@adepara.pa.gov.br.

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

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

13.7 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 14

Disposições finais

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

14.2 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.

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

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

14.5 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.

14.6 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.

- 14.7** Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento.
- 14.8** Só se iniciam e vencem os prazos em dias de expediente na Administração.
- 14.9** 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.
- 14.10** Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerão as deste Edital.
- 14.11** O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas e no Portal ComprasPará.
- 14.12** Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

ANEXO I – Termo de Referência

Apêndice do ANEXO I – Estudo Técnico Preliminar

ANEXO II – Minuta de Termo de Contrato

Cidade (PA), 24 de outubro de 2025.

(Assinatura)

JAMIR JUNIOR PARAGUASSU MACEDO
Diretor Geral

TERMO DE REFERÊNCIA DE BENS COMUNS

PAE nº 2025/3141716

O QUE SERÁ CONTRATADO?							
Lote*	Item	Descrição	Código SIMAS	Und	Qtd	Valor Unitário Estimado	Total**
1	1	Serviço de Firewall de próxima geração	24288-8	Mês	12	R\$ 31.100,04	R\$ 373.200,48
	2	Serviço SD-WAN	24288-8	Mês	12	R\$ 41.429,19	R\$ 497.150,28
	3	Serviços de Proteção das Estações de Trabalho e Servidores de Rede (Antivírus)	24288-8	Mês	12	R\$ 10.506,70	R\$ 126.080,40
	4	Serviço de Gestão de Backups	24288-8	Mês	12	R\$ 3.954,25	R\$ 47.451,00
	5	Serviço de Conectividade Wifi	24288-8	Mês	12	R\$ 13.711,15	R\$ 164.533,80
	6	Serviços Técnicos Especializados	24288-8	Mês	12	R\$ 19.771,25	R\$ 237.255,00
				VALOR GLOBAL ESTIMADO**		R\$ 1.445.670,96	
JUSTIFICATIVA DO AGRUPAMENTO EM LOTES*							
Não se pode simplesmente optar por determinada possibilidade sem antes avaliar uma série de elementos condicionantes ou viáveis sob as mais diversas óticas. Não é recomendável que se adote o parcelamento com vistas a economia de escala, em detrimento de uma eventual redução de custos de gestão de contratos ou a maior vantagem na contratação, quando a análise realizada recomendar a compra do item do mesmo fornecedor, quanto o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido ou quando o processo de padronização ou de escolha de marca levar a fornecedor exclusivo. Para se deflagrar a análise que permitirá ou não o parcelamento, deve-se observar a responsabilidade técnica, os custos para a Administração de vários contratos frente às vantagens da redução de custos, com divisão do objeto em itens, devendo sempre buscar a ampliação da competição e de evitar a concentração de mercado, conforme dito.							

Além dessa legislação, temos ainda a Súmula nº 247 do TCU que trata desse mesmo assunto:

"É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade"

Essa questão é pacificada junto àquele Tribunal, o que pode ser observado junto ao Acórdão n. 3140/2006:

"Cabe considerar, porém, que o modelo para a contratação parcelada adotado nesse parecer utilizou uma excessiva pulverização dos serviços ... Esta exagerada divisão de objeto pode maximizar a influência de fatores que contribuem para tornar mais dispendiosa a contratação (...) embora as estimativas numéricas não mostrem consistência, não há nos autos nenhuma evidência no sentido oposto, de que o parcelamento seria mais vantajoso para a Administração. Ao contrário, os indícios são coincidentes em considerar a licitação global mais econômica"

Assim, definidos os pressupostos a serem observados, passaremos a tratar da análise quanto a viabilidade ou não.

A análise quanto ao parcelamento consiste em verificar a possibilidade de unificar os itens em um objeto único ou separá-los, mas desde que alguns critérios sejam observados, especialmente buscando atender requisitos, necessidades e elementos que permitem atender o interesse público envolvido.

Um aspecto preponderante está justamente na integração e nos aspectos legais que envolvem o modelo de contratação. O primeiro ponto é o principal: viabilidade técnica. Ela consiste em avaliar se o objeto consegue alcançar os mesmos resultados se estiver sendo fornecido por empresas distintas. O escopo do objeto consiste em operação de infraestrutura e atendimento a usuários, governança de dados com foco na segurança da informação. O elemento focal está na segurança, integridade, preservação e confidencialidade das informações manuseadas e processadas.

Para tal decisão foram analisados diversos aspectos buscando minimizar riscos. O parcelamento, como dito, afeta não somente a segurança, mas atinge diretamente a eficiência operacional, sendo prejudicial ao conjunto do objeto.

Dado que todas as etapas envolvidas no ciclo de vida do serviço abrangem o escopo do fornecimento, na situação em questão, concluímos que dividir a contratação em múltiplos itens compromete a integração do serviço em relação aos seus elementos essenciais e à qualidade.

Sob a ótica da fiscalização, gestão e administração do contrato, também temos elementos a serem consi-

derados. Por tratar de itens de mesma característica e que foram licitados pelo Órgão Gerenciador em lote único, o parcelamento afeta dois aspectos: Onerosidade e maior esforço de fiscalização. Quanto a onerosidade, essa questão eu fala de custos comuns de administração de contratos, a integração do objeto retira essa duplicação de custos. Quanto ao esforço de fiscalização, ele aumenta as obrigações dos servidores públicos envolvidos, tendo em vista que cada execução deve ter seu acompanhamento individualizado.

Ao analisar as características do objeto em questão neste estudo, concluímos que reunir todas as demandas contratuais é viável tanto do ponto de vista técnico quanto econômico. Dividir o objeto poderia prejudicar a integridade do todo, além de gerar custos adicionais relacionados à coexistência de múltiplos contratos, aumentando os riscos e as dificuldades na gestão técnica e administrativa de uma variedade de contratos independentes.

Portanto, mesmo que a solução teoricamente possa ser dividida, existe um interesse técnico na sua manutenção como uma entidade única. Além disso, consideramos que a decisão não se baseia apenas na aplicação da regra geral, mas sim na sua viabilidade técnica. Nesse sentido, a avaliação técnica precede a avaliação econômica, uma vez que não se trata apenas de contratar o serviço pelo menor preço. Em nossa análise, a manutenção da unicidade do aspecto técnico garante os benefícios da solução, tornando conveniente para a Administração licitá-la dessa forma.

DESCRIÇÃO DA SOLUÇÃO	
QUAL O MOTIVO DA CONTRATAÇÃO?	<i>O objeto consiste na contratação de empresa especializada na prestação de serviços de atividades de execução continuada, pelo período de 12 meses.</i>
NATUREZA DO BEM	
NATUREZA	Serviço comum de natureza continuada.
HAVERÁ GARANTIA DO SERVIÇO?	☒ Sim. De acordo com o estudo técnico preliminar, o contratado deverá prestar garantia pelos serviços prestados de, no mínimo, 12 meses, após a sua conclusão. ☐ Não.
PROVA DE QUALIDADE, RENDIMENTO, DURABILIDADE E SEGURANÇA DO BEM	
HAVERÁ PROVA DE QUALIDADE?	☐ Sim. Justificativa: (A prova de qualidade deve ser sempre justificada e deverá ser comprovada por certificação de instituição credenciada pelo CONMETRO). ☒ Não.
O EDITAL EXIGIRÁ AMOSTRA?	☐ Sim. Justificativa: (A exigência de amostra deve ser justificada). ☒ Não.

HAVERÁ GARANTIA DO BEM?	☒ Sim. De acordo com o estudo técnico preliminar, o contratado deverá prestar garantia dos bens indicados nos itens 1 a 6 por, no mínimo, 12 meses, a partir do seu recebimento pela contratante. ☐ Não.
HAVERÁ ASSISTÊNCIA TÉCNICA?	☐ Sim. De acordo com o estudo técnico preliminar, o contratado prestará assistência técnica em relação aos bens indicados nos itens X e Y , durante N meses, a partir do seu recebimento pela contratante, <i>por meio de empresa credenciada contratada por ele</i> , sem custo para a administração pública. ☒ Sim. De acordo com o estudo técnico preliminar, o contratado prestará assistência técnica em relação aos bens indicados nos itens 1 a 6 , durante 12 meses, a partir do seu recebimento pela contratante, <i>por meios próprios</i> , sem custo para a administração pública. ☐ Não será prestada assistência técnica em relação aos itens X e Y .
CRITÉRIOS DE SELEÇÃO	
FORMA DE CONTRATAÇÃO	☐ Inexigibilidade de licitação, com fundamento no art. 74, Y , da Lei Federal nº 14.133/21. ☐ Dispensa de licitação em razão do valor* , com fundamento no art. 75, II, da Lei Federal nº 14.133/21. * Nesta hipótese, deve-se utilizar preferencialmente a dispensa eletrônica. ☐ Dispensa de licitação, com fundamento no art. 75, Y , da Lei Federal nº 14.133/21. ☒ Pregão eletrônico.
CRITÉRIO DE JULGAMENTO	☒ Menor preço. ☐ Maior desconto.
O ORÇAMENTO ESTIMADO É SIGILOSO?	☐ Sim. Justificativa: <i>(Indicar o motivo da escolha do orçamento sigiloso para a contratação).</i> ☒ Não.
CRITÉRIO PARA A PROPOSTA SER ACEITA	A proposta deve observar os valores unitários e global máximos aceitáveis conforme planilha de composição de preços do orçamento estimado*.

	* Se o orçamento estimado for <i>sigiloso</i>, o licitante não saberá os valores unitários e global máximos, razão pela qual o critério de aceitabilidade do preço também será considerado “<i>sigiloso</i>” para todos os fins.
HÁ ITENS COM PARTICIPAÇÃO EXCLUSIVA PARA MICROEMPRESAS E EMPRESA DE PEQUENO PORTE?	☐ Sim. Indicar os itens: (Indicar os itens).
	☒ Não.
REQUISITOS DA CONTRATADA	
SERÁ EXIGIDA HABILITAÇÃO TÉCNICA?	Solução de SD-WAN Atestados ou declarações de capacidade técnica devem comprovar aptidão para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto de que trata o processo licitatório, contendo, no mínimo as seguintes características: – Comprovar entrega ou fornecimento de pelo menos 50% do quantitativo exigido para cada item. Qual? A exigência de atestado de capacidade técnica é uma prática essencial para garantir a qualidade e a adequação dos serviços ou produtos a serem contratados. Este requisito visa assegurar que a empresa licitante possui a experiência e a competência técnica necessárias para a execução do objeto do contrato, refletindo diretamente na eficiência e na segurança da execução contratual. <i>Diante da complexidade do objeto em termos de segurança da informação, torna-se necessário prever tal comprovação, mitigando riscos de contratação de empresas que não detém conhecimento técnico e nem expertise mínima necessária.</i> Por quê? <i>O atestado de capacidade técnica é um documento formal emitido por entidades contratantes anteriores e que comprova que o licitante executou serviços ou forneceu produtos semelhantes ao objeto da licitação, dentro dos padrões estabelecidos e com êxito comprovado. Sua exigência está fundamentada na necessidade de verificar a conformidade técnica e a habilidade operacional do</i>

	<i>licitante, assegurando que este possui a experiência prática necessária para o cumprimento das obrigações contratuais.</i> <i>No contexto da presente licitação, a demanda por um atestado de capacidade técnica é justificada pela complexidade e especificidade do objeto contratado. Serviços ou produtos que envolvem tecnologia avançada, sistemas críticos ou processos especializados requerem um nível elevado de expertise e histórico comprovado para garantir que o fornecedor possa atender aos requisitos técnicos com a devida eficiência. O atestado de capacidade técnica serve, portanto, como uma ferramenta de mitigação de riscos, ao assegurar que a empresa licitante tem a experiência prática para lidar com as exigências e desafios do projeto.</i> <i>Além disso, a exigência deste atestado contribui para a competitividade leal entre os participantes da licitação. Ao estabelecer um critério técnico claro e objetivo, evita-se a participação de empresas que, apesar de terem potencial financeiro, não possuem a experiência prática necessária para a execução adequada do contrato. Isso promove a seleção de fornecedores realmente capacitados e aumenta a probabilidade de sucesso e eficiência na execução do contrato.</i> <i>Em suma, a exigência de atestado de capacidade técnica é um requisito fundamental que assegura a qualidade e a eficácia dos serviços ou produtos contratados. Este procedimento não apenas valida a experiência prática dos licitantes, mas também protege os interesses da administração pública e contribui para a execução bem-sucedida dos contratos, garantindo o cumprimento das metas e a satisfação das necessidades institucionais.</i> ☐ Não.
QUALIFICAÇÕES TÉCNICAS EXIGIDAS	☐ Declaração de ciência das informações necessárias para o cumprimento da futura obrigação contratual. Justificativa: <i>(Justificar o motivo da exigência, indicando a legislação aplicável, se for o caso).</i>

☐ Registro na entidade profissional competente.

Justificativa: *(Justificar o motivo da exigência, indicando a legislação aplicável, se for o caso).*

☐ Indicação de pessoal técnico, instalações e aparelhamento para o cumprimento da futura obrigação contratual com a comprovação de qualificação técnica de cada membro da equipe técnica responsável pela execução dos trabalhos.

Justificativa: *(Justificar o motivo da exigência, indicando a legislação aplicável, se for o caso).*

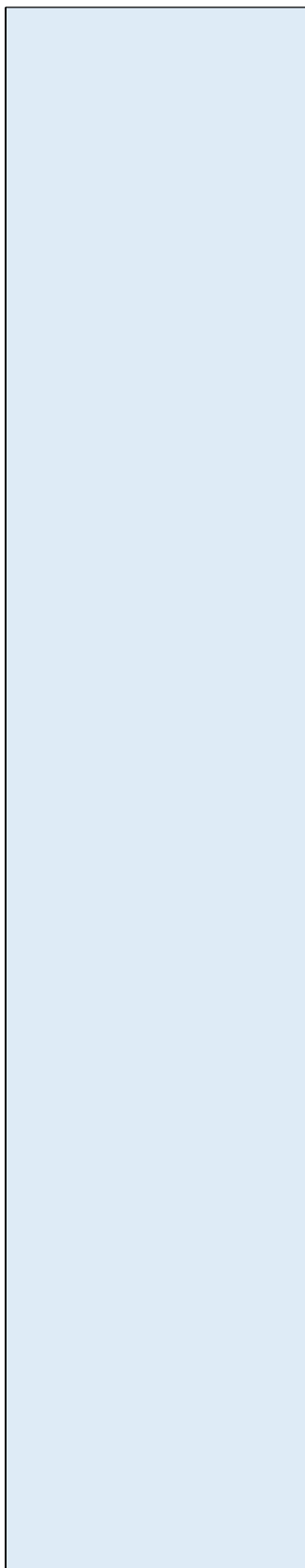
Diante da complexidade do objeto em termos de segurança da informação, torna-se necessário prever comprovação, mitigando riscos de contratação de empresas que não detém conhecimento técnico e nem expertise mínima necessária.

☒ Outro previsto em lei especial.

Especificar: Atestado de capacidade, relativo à qualificação técnico operacional.

O atestado de capacidade técnica é um documento formal emitido por entidades contratantes anteriores e que comprova que o licitante executou serviços ou forneceu produtos semelhantes ao objeto da licitação, dentro dos padrões estabelecidos e com êxito comprovado. Sua exigência está fundamentada na necessidade de verificar a conformidade técnica e a habilidade operacional do licitante, assegurando que este possui a experiência prática necessária para o cumprimento das obrigações contratuais.

No contexto da presente licitação, a demanda por um atestado de capacidade técnica é justificada pela complexidade e especificidade do objeto contratado. Serviços ou produtos que envolvem tecnologia avançada, sistemas críticos ou processos especializados requerem um



nível elevado de expertise e histórico comprovado para garantir que o fornecedor possa atender aos requisitos técnicos com a devida eficiência. O atestado de capacidade técnica serve, portanto, como uma ferramenta de mitigação de riscos, ao assegurar que a empresa licitante tem a experiência prática para lidar com as exigências e desafios do projeto.

Além disso, a exigência deste atestado contribui para a competitividade leal entre os participantes da licitação. Ao estabelecer um critério técnico claro e objetivo, evita-se a participação de empresas que, apesar de terem potencial financeiro, não possuem a experiência prática necessária para a execução adequada do contrato. Isso promove a seleção de fornecedores realmente capacitados e aumenta a probabilidade de sucesso e eficiência na execução do contrato.

Em suma, a exigência de atestado de capacidade técnica é um requisito fundamental que assegura a qualidade e a eficácia dos serviços ou produtos contratados. Este procedimento não apenas valida a experiência prática dos licitantes, mas também protege os interesses da administração pública e contribui para a execução bem-sucedida dos contratos, garantindo o cumprimento das metas e a satisfação das necessidades institucionais.

	☐ Não será exigida prova de qualificação técnica em razão da baixa complexidade da contratação.
HÁ CRITÉRIO DE SUSTENTABILIDADE?	☐ Sim. Especificar: <i>(Indicar o critério).</i> ☒ Não.
HÁ RISCOS A SEREM ASSUMIDOS PELA CONTRATADA?	Especificar: <i>(Somente é possível definir os riscos se a análise de risco tiver sido realizada. Nessa hipótese, os riscos devem ser especificados neste campo).</i> ☐ Sim. ☒ Não.
FORMA DE PRESTAÇÃO DO SERVIÇO	
COMO O SERVIÇO SERÁ PRESTADO?	☐ O serviço terá início imediato a partir da assinatura do contrato, contudo a prestação poderá estar sujeita à emissão de ordem de serviço pelo fiscal do contrato. ☒ O serviço terá início imediato a partir da assinatura do contrato com prestação de serviço continuada.
LOCAL E HORA DA PRESTAÇÃO DO SERVIÇO	O serviço deve ser prestado na sede administrativa da ADEPARÁ, localizada na Tv. Mariz e Barros, 1184 - Pedreira, Belém - PA, 66080-008.
PRAZO, FORMA DE PAGAMENTO E GARANTIA DO CONTRATO	
PRAZO DO CONTRATO	12 meses.
HAVERÁ POSSIBILIDADE DE PRORROGAÇÃO?	☒ Sim, conforme o art. 107 da Lei Federal nº 14.133/21, que dispõe que contratos de serviços e fornecimentos contínuos poderão ser prorrogados sucessivamente, desde que respeitada a vigência decenal. ☐ Não.
FORMA DE PAGAMENTO	Meio Ordem bancária. Onde? Conta corrente da contratada no Banco do Estado do Pará. Qual o prazo? Até 30 dias corridos, a contar do recebimento da nota fiscal (ou fatura) com o comprovante de regularidade fiscal da contratada.

	A regularidade fiscal pode ser provada: Prova da regularidade fiscal 1. Por consulta ao SICAF ou Cadastramento Unificado de Licitante. <i>ou</i> 2. Pela apresentação dos documentos constantes no art. 68 da Lei Federal nº 14.133/21, quando não for possível consultar aos sistemas oficiais.
QUAL A GARANTIA DO CONTRATO?	☒ 5% do valor inicial do contrato. Justificativa: A exigência da garantia de 5% é justificada pelo art. 96, §1º, da Lei 14.133/2021, considerando a complexidade e o alto risco do contrato de cibersegurança. O objeto envolve proteção de dados sensíveis e sistemas críticos, cuja falha pode gerar graves prejuízos à Administração. Assim, o percentual máximo mostra-se proporcional e necessário para assegurar a plena execução contratual e resguardar o interesse público.
PREVISÃO ORÇAMENTÁRIA	
DADOS ORÇAMENTÁRIOS DA CONTRATAÇÃO	20.122.1297–8338 Funcional Programática: (Operacionalização das Ações Administrativas) Elemento de Despesa: 339040 Fonte do Recurso: 01501.000061 Obs: Esses dados estão sujeitos à revisão por ocasião da emissão do atestado de disponibilidade orçamentária.

Cidade (PA), 05 de novembro de 2025.

(Assinatura)

Emerson Ribeiro

Gerente de Tecnologia e Informação – GTI

Agência de Defesa Agropecuária do Estado do Pará – ADEPARÁ

ANEXO I – ESPECIFICAÇÕES TÉCNICAS

1. DESCRIÇÃO DO OBJETO

- 1.1. A Licitante deverá fornecer uma solução composta por hardware, softwares e serviços na modalidade de serviço, sendo responsável por sua instalação, configuração, integração, operação, administração, monitoramento, gerenciamento e manutenção durante toda a vigência do contrato.
- 1.2. A Licitante deverá fornecer uma solução funcional e pronta para uso, contendo no mínimo as especificações deste edital, caso seja necessário o fornecimento de itens, acessórios ou quantidades acima do mínimo requerido para fins de atendimento a requisitos específicos da solução a ser fornecida, estes custos devem estar contemplados na proposta da licitante.

2. DETALHAMENTO DOS ITENS

2.1. Características Gerais para os Itens 1 e 2.

- 2.1.1. 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.
- 2.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 2.1.3. 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;
- 2.1.4. 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;
- 2.1.5. 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;
- 2.1.6. Deverá possuir e estar licenciado pelo período de **12 (doze) 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.

2.1.7. FUNCIONALIDADES DE REDE E FIREWALL

- 2.1.8. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 2.1.9. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
- 2.1.10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM- SM e PIM-DM);
- 2.1.11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;
- 2.1.12. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- 2.1.13. 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;
- 2.1.14. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

- 2.1.15. Deverá suportar sFlow ou Netflow;
- 2.1.16. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
- 2.1.17. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
- 2.1.18. Deve suportar o protocolo padrão da indústria VXLAN;
- 2.1.19. Deve implementar o protocolo ECMP;
- 2.1.20. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- 2.1.21. Enviar log para sistemas de monitoração externos;
- 2.1.22. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
- 2.1.23. Deve possuir mecanismos de proteção anti-spoofing;
- 2.1.24. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);
- 2.1.25. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- 2.1.26. Suportar OSPF graceful restart;
- 2.1.27. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 2.1.28. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- 2.1.29. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 2.1.30. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- 2.1.31. 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;
- 2.1.32. 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;
- 2.1.33. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;
- 2.1.34. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
- 2.1.35. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
- 2.1.36. 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;
- 2.1.37. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- 2.1.38. Deverá suportar controle por zonas de segurança;
- 2.1.39. Deverá suportar controles de políticas por porta e protocolo;
- 2.1.40. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
- 2.1.41. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

- 2.1.42. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
- 2.1.43. Controle, inspeção e descryptografia de SSL por política para tráfego de saída (Outbound);
- 2.1.44. Deve descryptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
- 2.1.45. 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;
- 2.1.46. Suporte a objetos e regras IPV6;
- 2.1.47. Suporte a objetos e regras multicast;
- 2.1.48. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
- 2.1.49. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES**
- 2.1.50. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- 2.1.51. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- 2.1.52. 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;
- 2.1.53. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
- 2.1.54. 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;
- 2.1.55. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
- 2.1.56. 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;
- 2.1.57. Para tráfego criptografado SSL, deve descryptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 2.1.58. 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;
- 2.1.59. Identificar o uso de táticas evasivas via comunicações criptografadas;
- 2.1.60. Atualizar a base de assinaturas de aplicações automaticamente;
- 2.1.61. 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;
- 2.1.62. 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;
- 2.1.63. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo

menos checagem de assinaturas e decodificação de protocolos;

- 2.1.64. 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;
- 2.1.65. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 2.1.66. Deve alertar o usuário quando uma aplicação for bloqueada;
- 2.1.67. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
- 2.1.68. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
- 2.1.69. 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;
- 2.1.70. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
- 2.1.71. 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);
- 2.1.72. 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;
- 2.1.73. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- 2.1.74. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

2.1.75. FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

- 2.1.76. 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;
- 2.1.77. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 2.1.78. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
- 2.1.79. 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;
- 2.1.80. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- 2.1.81. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 2.1.82. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
- 2.1.83. 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;
- 2.1.84. Deve permitir o bloqueio de vulnerabilidades;
- 2.1.85. Deve permitir o bloqueio de exploits conhecidos;

- 2.1.86. Deve incluir proteção contra-ataques de negação de serviços;
- 2.1.87. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
- 2.1.88. Detectar e bloquear a origem de portscans;
- 2.1.89. Bloquear ataques efetuados por worms conhecidos;
- 2.1.90. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- 2.1.91. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 2.1.92. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 2.1.93. 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;
- 2.1.94. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 2.1.95. Identificar e bloquear comunicação com botnets;
- 2.1.96. 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;
- 2.1.97. Os eventos devem identificar o país de onde partiu a ameaça;
- 2.1.98. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- 2.1.99. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- 2.1.100. 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.
- 2.1.101. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante
- 2.1.102. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
- 2.1.103. 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;
- 2.1.104. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS**
- 2.1.105. 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);
- 2.1.106. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
- 2.1.107. 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;
- 2.1.108. 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;

- 2.1.109. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 2.1.110. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
- 2.1.111. Possuir pelo menos 70 (setenta) categorias de URLs;
- 2.1.112. Deve possuir a função de exclusão de URLs do bloqueio;
- 2.1.113. Permitir a customização de página de bloqueio;
- 2.1.114. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;
- 2.1.115. 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;
- 2.1.116. 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;
- 2.1.117. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

2.1.118. FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

- 2.1.119. 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;
- 2.1.120. 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;
- 2.1.121. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;
- 2.1.122. 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;
- 2.1.123. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 2.1.124. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 2.1.125. 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);
- 2.1.126. 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;
- 2.1.127. Deve suportar o envio e recebimento de credenciais via RADIUS;
- 2.1.128. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

2.1.129. FUNCIONALIDADE DE FILTRO DE DADOS

- 2.1.130. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
- 2.1.131. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 2.1.132. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 2.1.133. 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.

2.1.134. FUNCIONALIDADE DE GEOLOCALIZAÇÃO

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

2.1.137. FUNCIONALIDADE DE VPN

- 2.1.138. Suportar VPN Site-to-Site e Cliente-To-Site;
- 2.1.139. Suportar IPSec VPN;
- 2.1.140. Suportar SSL VPN;
- 2.1.141. A VPN IPSEC deve suportar 3DES;
- 2.1.142. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
- 2.1.143. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- 2.1.144. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 2.1.145. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 2.1.146. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI
- 2.1.147. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 2.1.148. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
- 2.1.149. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 2.1.150. 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;
- 2.1.151. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- 2.1.152. 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;
- 2.1.153. Atribuição de DNS nos clientes remotos de VPN;
- 2.1.154. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

- 2.1.155. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
- 2.1.156. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 2.1.157. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- 2.1.158. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
- 2.1.159. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
- 2.1.160. Deverá manter uma conexão segura com o portal durante a sessão;
- 2.1.161. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 10 (64 bit) e Mac OS X (version 13);
- 2.1.162. FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO**
- 2.1.163. 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;
- 2.1.164. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
- 2.1.165. Endereço de origem;
- 2.1.166. Endereço de destino;
- 2.1.167. Usuário e grupo;
 - 2.1.167.1. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
 - 2.1.167.2. Por porta;
- 2.1.168. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
- 2.1.169. 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;
- 2.1.170. O QoS deve possibilitar a definição de fila de prioridade;
- 2.1.171. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
- 2.1.172. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
- 2.1.173. Suportar modificação de valores DSCP para o Diffserv;
- 2.1.174. Suportar priorização de tráfego usando informação de ToS (Type of Service);
- 2.1.175. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
- 2.1.176. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;
- 2.1.177. Deve possibilitar a definição de bandas distintas para download e upload;
- 2.1.178. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS**
- 2.1.179. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

- 2.1.180. A solução deve ser capaz de agregar vários links em uma interface virtual;
- 2.1.181. 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);
- 2.1.182. 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;
- 2.1.183. 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;
- 2.1.184. 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);
- 2.1.185. 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).
- 2.1.186. 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:
- 2.1.187. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.
- 2.1.188. 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;
- 2.1.189. 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;
- 2.1.190. 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;
- 2.1.191. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;
- 2.1.192. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);
- 2.1.193. 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);
- 2.1.194. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
- 2.1.195. 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;

- 2.1.196. 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;
- 2.1.197. 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;
- 2.1.198. 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;
- 2.1.199. A solução deve suportar nativamente conectores com clouds públicas;
- 2.1.200. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;
- 2.1.201. 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);
- 2.1.202. Deve implementar balanceamento de link por hash do IP de origem;
- 2.1.203. Deve implementar balanceamento de link por hash do IP de origem e destino;
- 2.1.204. 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;
- 2.1.205. 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;
- 2.1.206. 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.

2.2. ITEM 01 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW)

- 2.2.1. Deve suportar, no mínimo, 11 (onze) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
- 2.2.2. Deve suportar, no mínimo, 3 (três) milhões de conexões simultâneas;
- 2.2.3. Deve suportar, no mínimo, 250.000 (duzentos e cinquenta mil) novas conexões por segundo;
- 2.2.4. Deve Suportar, no mínimo, 10 (dez) Gbps de throughput VPN IPsec;
- 2.2.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 1.000 (mil) túneis de VPN IPSEC Site-to-Site simultâneos;
- 2.2.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 10.000 (dez mil) túneis de clientes VPN IPSEC simultâneos;
- 2.2.7. Deve suportar, no mínimo, 2 (dois) Gbps de throughput de VPN SSL;
- 2.2.8. Deve suportar, no mínimo, 500 (quinhentos) clientes de VPN SSL simultâneos;
- 2.2.9. Deve suportar, no mínimo, 4 (quatro) Gbps de throughput de IPS;
- 2.2.10. Deve suportar, no mínimo, 4 (quatro) Gbps de throughput de Inspeção SSL;
- 2.2.11. Deve suportar, no mínimo, 3 (três) 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.

- 2.2.12. Deve possuir, pelo menos, 16 (dezesseis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
- 2.2.13. Deve possuir, pelo menos, 8 (oito) interfaces com suporte a conectores SFP de 1 Gigabit Ethernet;
- 2.2.14. Deve possuir, pelo menos, 4 (quatro) interfaces com suporte a conectores SFP+ de 10 Gigabit Ethernet e SFP de 1 Gigabit Ethernet;
- 2.2.15. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;
- 2.2.16. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para Alta-Disponibilidade;
- 2.2.17. Deve possuir fonte de alimentação AC redundante e HotSwap;
- 2.2.18. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;
- 2.2.19. A solução deverá operar em cluter de no mínimo 02 equipamentos.

2.3. ITEM 02 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DOS APPLIANCES SD-WAN

- 2.3.1. Deve suportar, no mínimo, 5 (cinco) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
- 2.3.2. Deve suportar, no mínimo, 1 (um) milhões de conexões simultâneas;
- 2.3.3. Deve suportar, no mínimo, 30.000 (trinta mil) novas conexões por segundo;
- 2.3.4. Deve Suportar, no mínimo, 5 (cinco) Gbps de throughput VPN IPsec;
- 2.3.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos;
- 2.3.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 500 (quinhentos) túneis de clientes VPN IPSEC simultâneos;
- 2.3.7. Deve suportar, no mínimo, 400 (quatrocentos) Mbps de throughput de VPN SSL;
- 2.3.8. Deve suportar, no mínimo, 200 (duzentos) clientes de VPN SSL simultâneos;
- 2.3.9. Deve suportar, no mínimo, 1 (um) Gbps de throughput de IPS;
- 2.3.10. Deve suportar, no mínimo, 700 (setecentos) Mbps de throughput de Inspeção SSL;
- 2.3.11. Deve suportar, no mínimo, 700 (setecentos) 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.
- 2.3.12. Deve possuir, pelo menos, 10 (dez) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
- 2.3.13. Deverão ser fornecidos 10 equipamentos.

2.4. ITEM 03 - Serviços de Proteção das Estações de Trabalho e Servidores de Rede com garantia e suporte por 12 meses

- 2.4.1. Deverão ser fornecidas 400 licenças.
- 2.4.2. A Solução EDR deve apresentar modelo cliente/servidor, com uma gerência centralizada e hierarquizada.

- 2.4.3.** A solução de administração deve ser fornecida pela licitante vencedora e contemplar todos os softwares e respectivas licenças necessárias ou adicionais para a instalação, configuração e funcionamento da solução de proteção.
- 2.4.4.** Todas as licenças de software, principalmente as de sistemas operacionais, banco de dados, agentes locais, em nuvem ou eventuais componentes necessários ao pleno funcionamento da solução deverão ser fornecidas integralmente às expensas da contratada.
- 2.4.5.** A instalação, configuração e funcionamento da solução a ser contratada não poderão exigir aquisição extra ou aluguel de outras licenças de software ou hardware além das ofertadas na proposta e contrato.
- 2.4.6.** A solução de proteção deve ser oferecida na última versão disponibilizada pelo fabricante. Na data da proposta, nenhum dos softwares componentes da solução de proteção ofertados poderão estar listados pelo fabricante com data definida para fim de suporte ("end of support") ou fim de vendas ("end of sale").
- 2.4.7.** Toda a Solução EDR deve ser fornecida por um único fabricante de modo que tanto o suporte da solução quanto suas funcionalidades sejam integrados e interoperáveis, com o objetivo de otimizar e facilitar o gerenciamento.
- 2.4.8.** A solução EDR deve contemplar uma plataforma do nível "Enterprise" para atender, adequadamente, a proteção e gerência dos ativos da ADEPARA.
- 2.4.9.** Todas as licenças de software deverão ser perpétuas, ou seja, expirado o período de validade, deverão permanecer funcionais para a proteção contra códigos maliciosos, excetuando-se as atualizações, usando as versões dos softwares e base de assinaturas que a CONTRATANTE possua ao final do período de validade. Portanto, serão aceitas reduções nas funcionalidades de detecção de novos códigos maliciosos após expiração das licenças, contanto que essa proteção e o gerenciamento da solução continuem ativos.
- 2.4.10. Do módulo de proteção de endpoint.**
- 2.4.11.** A solução proposta deverá proteger os sistemas operacionais abaixo:
- 2.4.11.1. Windows 7
 - 2.4.11.2. Windows 8
 - 2.4.11.3. Windows 8.1
 - 2.4.11.4. Windows 10
 - 2.4.11.5. Windows 11
 - 2.4.11.6. Windows Server 2012 R2, 2016, 2019 e 2022
 - 2.4.11.7. Amazon Linux 2.
 - 2.4.11.8. CentOS Stream 8.
 - 2.4.11.9. CentOS Stream 9.
 - 2.4.11.10. Debian GNU/Linux 12.0 e posterior.
 - 2.4.11.11. Linux Mint 21.1 e posterior.
 - 2.4.11.12. openSUSE Leap 15.0 e posterior.
 - 2.4.11.13. Oracle Linux 7.3 e posterior.
 - 2.4.11.14. Oracle Linux 8.0 e posterior.
 - 2.4.11.15. Oracle Linux 9.0 e posterior.
 - 2.4.11.16. Red Hat Enterprise Linux 7.2 e posterior.

- 2.4.11.17. Red Hat Enterprise Linux 8.0 e posterior.
- 2.4.11.18. Red Hat Enterprise Linux 9.0 e posterior.
- 2.4.11.19. Rocky Linux 8.5 e posterior.
- 2.4.11.20. Rocky Linux 9.1.
- 2.4.11.21. SUSE Linux Enterprise Server 15 ou posterior.
- 2.4.11.22. Ubuntu 22.04 LTS.
- 2.4.11.23. Ubuntu 24.04 LTS.
- 2.4.11.24. Sistemas operacionais Arm de 64 bits:
- 2.4.11.25. CentOS Stream 9.
- 2.4.11.26.** SUSE Linux Enterprise Server 15.

2.4.12. Do módulo de gerenciamento avançado

2.4.13. A solução proposta deve suportar arquitetura cloud-native e on-premise;

2.4.14. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:

- 2.4.14.1. Amazon Web Services
- 2.4.14.2. Microsoft Azure

2.4.14.3. Google Cloud

2.4.15. A solução proposta deve incluir as seguintes opções de integração SIEM:

- 2.4.15.1. HP (Microfoco) ArcSight
- 2.4.15.2. IBM QRadar
- 2.4.15.3. Splunk

2.4.15.4. Kaspersky KUMA

2.4.16. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

2.4.17. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

2.4.18. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

2.4.19. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

2.4.20. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

2.4.21. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

2.4.22. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

2.4.23. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

2.4.24. A solução proposta deve incluir Role Based Access Control (RBAC) com funções

predefinidas personalizáveis.

2.4.25. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

2.4.26. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

2.4.26.1. Status do dispositivo

2.4.26.2. Tag

2.4.26.3. Diretório ativo

2.4.26.4. Proprietários de dispositivos

2.4.26.5. Hardware

2.4.27. A solução proposta deve suportar os seguintes canais de entrega de notificação:

2.4.27.1. E-mail

2.4.27.2. Registro de sistema

2.4.27.3. SMS

2.4.28. A solução proposta deve ter a capacidade de etiquetar/marcas computadores com base em:

2.4.28.1. Atributos de rede

2.4.28.2. Nome

2.4.28.3. Domínio e/ou Sufixo de Domínio

2.4.28.4. Endereço de IP

2.4.28.5. Endereço IP para servidor de gerenciamento

2.4.28.6. Localização no Active Directory

2.4.28.7. Unidade organizacional

2.4.28.8. Grupo

2.4.28.9. Sistema operacional

2.4.28.10. Número do pacote de serviço

2.4.28.11. Arquitetura Virtual

2.4.28.12. Registro de aplicativos

2.4.28.13. Nome da Aplicação

2.4.28.14. Versão do aplicativo

2.4.28.15. Fabricante

2.4.28.16. Tipo e versão

2.4.28.17. Arquitetura

2.4.29. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

2.4.30. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede

pública.

2.4.31. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

- 2.4.31.1. Dispositivos Desktop/Servidores
- 2.4.31.2. Dispositivos móveis
- 2.4.31.3. Dispositivos de rede
- 2.4.31.4. Dispositivos virtuais
- 2.4.31.5. Componentes OEM
- 2.4.31.6. Periféricos de computador
- 2.4.31.7. Dispositivos IoT conectados
- 2.4.31.8. Telefones VoIP

2.4.31.9. Repositórios de rede

2.4.32. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

- 2.4.32.1. Nome da Aplicação
- 2.4.32.2. Caminho do aplicativo
- 2.4.32.3. Metadados do aplicativo
- 2.4.32.4. Aplicativo Certificado digital
- 2.4.32.5. Categorias de aplicativos predefinidas pelo fornecedor

2.4.32.6. SHA256 e MD5

2.4.33. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

- 2.4.33.1. Bluetooth
- 2.4.33.2. Dispositivos móveis
- 2.4.33.3. Modems externos
- 2.4.33.4. CD/DVD
- 2.4.33.5. Câmeras e scanners
- 2.4.33.6. MTPs

2.4.33.7. E a transferência de dados para dispositivos móveis

2.4.34. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

2.4.35. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

2.4.36. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

- 2.4.36.1. Estruturas de domínios e grupos de trabalho do Windows
- 2.4.36.2. Estruturas de grupos do Active Directory

2.4.36.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador

2.4.37. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos

detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

2.4.38. A solução proposta deve permitir realizar as seguintes ações para endpoints:

- 2.4.38.1. Verificação manual;
- 2.4.38.2. Verificação no acesso;
- 2.4.38.3. Verificação por demanda;
- 2.4.38.4. Verificação de arquivos compactados
- 2.4.38.5. Verificação de arquivos individuais, pastas e unidades;
- 2.4.38.6. Bloqueio e verificação de scripts
- 2.4.38.7. Proteção contra alteração de registros;
- 2.4.38.8. Proteção contra estouro de buffer;

2.4.38.9. Verificação em segundo plano/inativa;

- 2.4.39. Verificação de unidade removível na conexão com o sistema;
- 2.4.40. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.
- 2.4.41. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.
- 2.4.42. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.
- 2.4.43. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.
- 2.4.44. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.
- 2.4.45. A solução proposta deve suportar Windows Failover Cluster.
- 2.4.46. A solução proposta deve ter um recurso de clustering integrado.
- 2.4.47. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.
- 2.4.48. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.
- 2.4.49. O servidor de gestão da solução proposta deverá incluir funções de segurança prédefinidas para o Auditor, Supervisor e Oficial de Segurança.
- 2.4.50. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.
- 2.4.51. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.
- 2.4.52. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.
- 2.4.53. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.
- 2.4.54. A solução proposta deve contar com filtragem de firewall por endereço local, interface

física e Time-To-Live (TTL) de pacotes.

- 2.4.55. A solução proposta deverá possuir controles para download de DLL e drivers.
- 2.4.56. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo específico de prevenção de intrusão.
- 2.4.57. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.
- 2.4.58. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).
- 2.4.59.** A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.
- 2.4.60. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.
- 2.4.61. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
- 2.4.62. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.
- 2.4.63. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
- 2.4.64. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.
- 2.4.65. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
- 2.4.66. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.
- 2.4.67. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
- 2.4.68. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
- 2.4.69. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal.
- 2.4.70. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.
- 2.4.71. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser

acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

- 2.4.72. A solução proposta deve permitir ao administrador personalizar relatórios.
- 2.4.73. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.
- 2.4.74. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.
- 2.4.75. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.
- 2.4.76. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.
- 2.4.77. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.
- 2.4.78.** A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.
- 2.4.79. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;
- 2.4.80. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.
- 2.4.81. A solução proposta deve suportar integração com solução APT.
- 2.4.82. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.
- 2.4.83.** A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:
 - 2.4.83.1. Windows
 - 2.4.83.2.** Linux
- 2.4.84.** A solução proposta deverá suportar os seguintes servidores de banco de dados:
 - 2.4.84.1. Windows:
 - 2.4.84.1.1. Microsoft SQL Server
 - 2.4.84.1.2. Microsoft Banco de dados SQL do Azure
 - 2.4.84.1.3. MySQL Standard e Enterprise
 - 2.4.84.1.4. MariaDB
 - 2.4.84.1.5. PostgreSQL
 - 2.4.84.2. Linux:
 - 2.4.84.2.1. MySQL
 - 2.4.84.2.2. MariaDB
 - 2.4.84.2.3.** PostgreSQL
- 2.4.85. A solução proposta deverá suportar as seguintes plataformas virtuais:

2.4.85.1. Windows:

- 2.4.85.1.1. VMware vSphere 6.7 e 7.0
- 2.4.85.1.2. Estação de trabalho VMware 16 Pro
- 2.4.85.1.3. Servidor Microsoft Hyper-V 2012 de 64 bits
- 2.4.85.1.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- 2.4.85.1.5. Microsoft Servidor Hyper -V 2016 de 64 bits
- 2.4.85.1.6. Servidor Microsoft Hyper-V 2019 de 64 bits
- 2.4.85.1.7. Servidor Microsoft Hyper-V 2022 de 64 bits
- 2.4.85.1.8. Citrix XenServer 7.1 LTSR
- 2.4.85.1.9. Citrix XenServer 8.x
- 2.4.85.1.10. Oracle VM VirtualBox 6.x

2.4.85.2. Linux:

- 2.4.85.2.1. VMware vSphere 6.7, 7.0 e 8.0
- 2.4.85.2.2. VMware Desktop 16 Pro e 17 Pro
- 2.4.85.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits
- 2.4.85.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- 2.4.85.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits
- 2.4.85.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits
- 2.4.85.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits
- 2.4.85.2.8. Citrix XenServer 7.1 e 8.x
- 2.4.85.2.9.** Oracle VM VirtualBox 6.x e 7.x

2.4.86. A solução proposta deve suportar criptografia em vários níveis:

- 2.4.86.1. Criptografia completa do disco – incluindo disco do sistema
- 2.4.86.2. Criptografia de arquivos e pastas
- 2.4.86.3. Criptografia de mídia removível

2.4.86.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2

2.4.87. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:

- 2.4.87.1. A criptografia de arquivos em unidades de computador locais.
- 2.4.87.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.

2.4.87.3. A criação de listas criptografadas de pastas em unidades de computador locais.

2.4.88. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:

- 2.4.88.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.

2.4.88.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.

2.4.89. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:

2.4.89.1. A criptografia de todos os arquivos armazenados em unidades removíveis.

2.4.89.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.

2.4.90. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia.

2.4.91. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.

2.4.92. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.

2.4.93. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.

2.4.94. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.

2.4.95. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.

2.4.96. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

2.4.97. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.

2.4.98. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.

2.4.99. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.

2.4.100. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.

2.4.101. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.

2.4.102. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.

2.4.103. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou

usuário.

- 2.4.104. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.
- 2.4.105. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.
- 2.4.106.** A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:
 - 2.4.106.1. Uso do Trusted Platform Module e configurações de senha.
 - 2.4.106.2.** Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.
- 2.4.107. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).
- 2.4.108. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.
- 2.4.109.** A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
 - 2.4.109.1. Instalação remota de software de terceiros
 - 2.4.109.2. Relatórios sobre software e hardware existentes
 - 2.4.109.3. Monitoramento para instalação de software não autorizado
 - 2.4.109.4.** Remoção de software não autorizado
- 2.4.110. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.
- 2.4.111. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.
- 2.4.112. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.
- 2.4.113. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.
- 2.4.114. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.
- 2.4.115. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.
- 2.4.116. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.
- 2.4.117. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança
- 2.4.118. A solução proposta deve permitir ao administrador aprovar atualizações.
- 2.4.119. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.
- 2.4.120. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.

- 2.4.121. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.
- 2.4.122. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.
- 2.4.123. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.
- 2.4.124. A solução proposta deve fornecer a facilidade de detectar/installar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).
- 2.4.125. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.
- 2.4.126. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.
- 2.4.127. A solução proposta deve incluir campos dedicados que contenham informações sobre 'Exploração encontrada para a vulnerabilidade'.
- 2.4.128. A solução proposta deve incluir campos dedicados que contenham informações sobre "Ameaça encontrada para a vulnerabilidade".
- 2.4.129. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.
- 2.4.130. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.
- 2.4.131. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.
- 2.4.132. A solução proposta deve apoiar a implantação do sistema operacional.
- 2.4.133. A solução proposta deve suportar Wake-on LAN e UEFI.
- 2.4.134. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.
- 2.4.135. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.
- 2.4.136. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.
- 2.4.137. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.
- 2.4.138. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.
- 2.4.139. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.
- 2.4.140. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.
- 2.4.141. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.
- 2.4.142. A solução proposta deve permitir ao administrador utilizar uma única

tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.

2.4.143. solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:

2.4.143.1. Inicie a instalação ao reiniciar ou desligar o computador.

2.4.143.2. Instale o gerador necessário todos os pré-requisitos do sistema.

2.4.143.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.

2.4.143.4. Baixe atualizações para o dispositivo sem instalá-las.

2.4.144. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.

2.4.145. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.

2.4.146. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:

2.4.146.1. CEF;

2.4.146.2. LEEF;

2.4.147. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.

2.4.148. O relatório da solução proposta deve conter informações CVE.

2.4.149. A solução proposta deve suportar instalação de aplicações e software de terceiros;

2.4.150. Do módulo de gerenciamento simplificado

2.4.151. A solução proposta deve suportar arquitetura cloud;

2.4.152. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

2.4.153. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

2.4.154. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.

2.4.155. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.

2.4.156. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.

2.4.157. A solução proposta deve incluir informações do endpoint:

2.4.157.1. IP público de internet;

2.4.157.2. IP interno do dispositivo;

2.4.157.3. Versão do agente de proteção;

2.4.157.4. Última comunicação com a console, contendo data e hora;

2.4.157.5. Informações do sistema operacional;

- 2.4.158. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.
- 2.4.159. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.
- 2.4.160.** A solução proposta deve incluir treinamento em segurança cibernética.
- 2.4.161. Requisitos gerais**
- 2.4.162.** A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
- 2.4.162.1.** Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo Zero-Day e outros softwares maliciosos e indesejados.
- 2.4.163. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
- 2.4.164. A solução proposta deve suportar integração com Anti-malware Scan Interface (AM-SI).
- 2.4.165. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.
- 2.4.166. A solução proposta deve suportar o subsistema Linux no Windows.
- 2.4.167.** A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
- 2.4.167.1. Proteção contra ameaças sem arquivos (Fileless);
- 2.4.167.2.** Fornecimento de proteção baseada em machine learning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;
- 2.4.168. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
- 2.4.169. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
- 2.4.170. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.
- 2.4.171. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.
- 2.4.172. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.
- 2.4.173. A solução proposta deve fornecer análise comportamental baseada em machine learning.
- 2.4.174. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.
- 2.4.175.** A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:

- 2.4.175.1. Controles de aplicativos,
- 2.4.175.2. Controle web e dispositivos
- 2.4.175.3. HIPS e Firewall
- 2.4.175.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
- 2.4.175.5. Gerenciamento de criptografia de arquivos e discos;
- 2.4.175.6.** Controle adaptativo para detecção de anomalias;
- 2.4.176. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.
- 2.4.177. A solução proposta deve ser protegida por senha para evitar que o processo do antimalware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.
- 2.4.178. A solução proposta deve ter bancos de dados de reputação locais e globais.
- 2.4.179. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.
- 2.4.180.** A solução proposta deve incluir um módulo capaz, no mínimo, de:
 - 2.4.180.1. Bloqueio de aplicativos com base em sua categorização.
 - 2.4.180.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
 - 2.4.180.3.** A adição de sub-redes e a modificação de permissões de atividade.
- 2.4.181. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.
- 2.4.182. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.
- 2.4.183. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.
- 2.4.184.** A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
 - 2.4.184.1. Modo silencioso;
 - 2.4.184.2. Discos rígidos e dispositivos removíveis;
 - 2.4.184.3.** De todos as contas de usuários do dispositivo.
- 2.4.185.** A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
 - 2.4.185.1. Exclusão imediata de dados;
 - 2.4.185.2.** Exclusão de dados adiada.
- 2.4.186.** A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
 - 2.4.186.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
 - 2.4.186.2.** Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.
- 2.4.187. A solução proposta deve ter uma abordagem proativa para impedir que malware

explore vulnerabilidades existentes em servidores e estações de trabalho.

- 2.4.188. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.
- 2.4.189. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.
- 2.4.190. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.
- 2.4.191. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.
- 2.4.192. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.
- 2.4.193. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.
- 2.4.194. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;
- 2.4.195. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;
- 2.4.196. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.
- 2.4.197. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.
- 2.4.198. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.
- 2.4.199. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.
- 2.4.200. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.
- 2.4.201. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.
- 2.4.202. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.
- 2.4.203. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.
- 2.4.204. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.
- 2.4.205. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.
- 2.4.206. A solução proposta deve ter categoria de detecção para bloquear banners de sites.

- 2.4.207. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;
- 2.4.208. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.
- 2.4.209. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.
- 2.4.210. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.
- 2.4.211. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;
- 2.4.212. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.
- 2.4.213. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.
- 2.4.214. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.
- 2.4.215. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.
- 2.4.216. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.
- 2.4.217. A solução proposta deve suportar o controle de scripts executados em PowerShell.
- 2.4.218. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.
- 2.4.219. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.
- 2.4.220. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.
- 2.4.221. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
- 2.4.222. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.
- 2.4.223. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.
- 2.4.224.** A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
- 2.4.224.1. Filtro de anexos.
- 2.4.224.2.** Verificação de mensagens de email ao receber, ler e enviar.
- 2.4.225. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
- 2.4.226. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;

- 2.4.227. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);
- 2.4.228. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.
- 2.4.229. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.
- 2.4.230. A solução proposta deve incluir suporte ao protocolo IPv6.
- 2.4.231. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
- 2.4.232. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
- 2.4.233. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.
- 2.4.234. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.
- 2.4.235. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
- 2.4.236. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.
- 2.4.237. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
- 2.4.238. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.
- 2.4.239. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
- 2.4.240. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.
- 2.4.241. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.
- 2.4.242. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.
- 2.4.243. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
- 2.4.244. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.
- 2.4.245. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.

- 2.4.246. A solução proposta deve suportar endereços IPv6.
- 2.4.247. A solução proposta deve suportar verificação em duas etapas (autenticação).
- 2.4.248. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
- 2.4.249. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
- 2.4.250. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.
- 2.4.251. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.
- 2.4.252. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.
- 2.4.253. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
- 2.4.254. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
- 2.4.255. A solução proposta deve permitir a gestão de um componente que controle o trabalho com dispositivos de E/S externos.
- 2.4.256. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.
- 2.4.257. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.
- 2.4.258. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.
- 2.4.259. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
- 2.4.260. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.
- 2.4.261. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.
- 2.4.262. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
- 2.4.263. A solução proposta deve ter a capacidade de excluir atualizações baixadas.
- 2.4.264. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.
- 2.4.265. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.
- 2.4.266. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.
- 2.4.267. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão

para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.

2.4.268. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

2.4.269. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

2.4.270. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.

2.4.271. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.

2.4.272. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

2.4.272.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.

2.4.272.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

2.4.273. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.

2.4.274. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

2.4.275. Do modulo de gerenciamento de dispositivos móveis

2.4.276. O modulo deve ser integrado a console de gerenciamento;

2.4.277. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

2.4.277.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)

2.4.278. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

2.4.278.1. iOS 10–17 ou iPadOS 13–17

2.4.279. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.

2.4.280. A solução proposta deve suportar dispositivos iOS supervisionados.

2.4.281. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.

2.4.282. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.

2.4.283. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.

2.4.284. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).

- 2.4.285. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.
- 2.4.286. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.
- 2.4.287. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.
- 2.4.288. A solução proposta deve ter recursos de containerização para dispositivos Android.
- 2.4.289.** A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
- 2.4.289.1. Dados em contêineres
 - 2.4.289.2. Contas de e-mail corporativo
 - 2.4.289.3. Configurações para conexão à rede Wi-Fi corporativa e VPN
 - 2.4.289.4. Nome do ponto de acesso (APN)
 - 2.4.289.5. Perfil do Android for Work
 - 2.4.289.6. Recipiente KNOX
 - 2.4.289.7.** Chave do gerenciador de licença KNOX
- 2.4.290.** A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
- 2.4.290.1. Todos os perfis de configuração instalados;
 - 2.4.290.2. Todos os perfis de provisionamento;
 - 2.4.290.3.** O perfil iOS MDM;
- 2.4.291. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas.
- 2.4.292. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo.
- 2.4.293.** A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controle de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:
- 2.4.293.1. Critérios de verificação do dispositivo;
 - 2.4.293.2.** Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;
- 2.4.294. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.
- 2.4.295.** A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
- 2.4.295.1. Cartões de memória e outras unidades removíveis;
 - 2.4.295.2. Câmera do dispositivo;
 - 2.4.295.3. Conexões Wi-Fi;

- 2.4.295.4. Conexões Bluetooth;
- 2.4.295.5. Porta de conexão infravermelha;
- 2.4.295.6. Ativação do ponto de acesso Wi-Fi;
- 2.4.295.7. Conexão de área de trabalho remota;
- 2.4.295.8. Sincronização de área de trabalho;
- 2.4.295.9. Definir configurações da caixa de correio do Exchange;
- 2.4.295.10. Configurar caixa de e-mail em dispositivos iOS MDM;
- 2.4.295.11. Configure contêineres Samsung KNOX;
- 2.4.295.12. Definir as configurações do perfil do Android for Work;
- 2.4.295.13. Configurar e-mail/calendário/contatos;
- 2.4.295.14. Definir as configurações de restrição de conteúdo de mídia;
- 2.4.295.15. Definir configurações de proxy no dispositivo móvel;
- 2.4.295.16.** Configurar certificados e SCEP;
- 2.4.296. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay.
- 2.4.297.** A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
 - 2.4.298. Google Play, Huawei App Gallery e Apple App Store;
 - 2.4.299. Portal de inscrição móvel KNOX;
- 2.4.300.** Pacotes de instalação pré-configurados independentes;
- 2.4.301. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.
- 2.4.302. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.
- 2.4.303.** A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
 - 2.4.303.1. VMware AirWatch 9.3 ou posterior;
 - 2.4.303.2. MobileIron 10.0 ou posterior;
 - 2.4.303.3. IBM MaaS360 10.68 ou posterior;
 - 2.4.303.4. Microsoft Intune 1908 ou posterior;
 - 2.4.303.5.** SOTI MobiControl 14.1.4 (1693) ou posterior;
- 2.4.304. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.
- 2.4.305.** A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
 - 2.4.305.1. Google Play;
 - 2.4.305.2. Galeria de aplicativos Huawei;
 - 2.4.305.3.** Loja de aplicativos da Apple;

- 2.4.306. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.
- 2.4.307. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.
- 2.4.308. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.
- 2.4.309. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.
- 2.4.310. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.
- 2.4.311. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.
- 2.4.312. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
- 2.4.313. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
- 2.4.314. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.
- 2.4.315. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
- 2.4.316. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.
- 2.4.317. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.
- 2.4.318. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
- 2.4.319.** A solução proposta deve proteger contra ameaças online em dispositivos iOS.
- 2.4.320. Do módulo de EDR**
- 2.4.321. Deve apresentar um gráfico de propagação de ameaças com os principais processos, conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
- 2.4.322. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
- 2.4.323. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
- 2.4.324. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
- 2.4.325.** Deve apresentar informações detalhadas contendo:
- 2.4.325.1. Usuário que executou a ação;
- 2.4.325.2.** Informações acesso privilegiado;
- 2.4.326. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam

detectadas.

- 2.4.327. A solução proposta deve suportar integração com serviço de reputação em nuvem.
- 2.4.328. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)
- 2.4.329. O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).
- 2.4.330. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;
- 2.4.331. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.
- 2.4.332. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.
- 2.4.333. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.
- 2.4.334. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.
- 2.4.335. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.
- 2.4.336. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.
- 2.4.337. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.
- 2.4.338. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.
- 2.4.339. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.
- 2.4.340.** A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:
- 2.4.341.
- 2.4.342. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).
- 2.4.343. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.
- 2.4.344. Informações gerais sobre a detecção, incluindo modo de detecção.
- 2.4.345. Alterações no registro associadas à detecção.
- 2.4.346. Histórico da presença de arquivos no dispositivo.
- 2.4.347. Ações de resposta executadas pela aplicação.
- 2.4.348. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os

principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.

- 2.4.349. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
- 2.4.350. Processo
- 2.4.351. Conexões de rede
- 2.4.352. Alterações no registro
- 2.4.353. Detalhes do download de objeto
- 2.4.354. A solução proposta deve fornecer orientação de resposta (resposta guiada).
- 2.4.355. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente.
- 2.4.356. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
- 2.4.357. Impedir a execução de objetos
- 2.4.358. Isolamento de host
- 2.4.359. Excluir objeto do host ou grupo de hosts
- 2.4.360. Encerrar um processo no dispositivo
- 2.4.361. Colocar um objeto em quarentena
- 2.4.362. Execute a verificação do sistema
- 2.4.363. Execução remota de programa/processo/comando
- 2.4.364. Iniciar a varredura IoC para um grupo de hosts.**
- 2.4.365. Requisitos para documentação da solução.**

2.5. ITEM 04 - Serviço de Gestão de Backups com garantia e suporte por 12 meses

- 2.5.1. Solução de proteção de servidores do ambiente físico e/ou virtualizado, para criação de ambiente de backup/recuperação (backup/restore), local e remoto, para discos, unidade de fitas e nuvem. A solução deve oferecer a possibilidade de replicação/DR (Disaster Recovery) entre estruturas on-site e off-site. A solução deverá compreender, serviços de instalação, configuração, repasse de conhecimento e garantia.
- 2.5.2. A solução ofertada deverá, obrigatoriamente, atender as especificações mínimas previstas quanto as funcionalidades, integrações e compatibilidades como o ambiente físico e virtualizado para criação e recuperação do ambiente de servidores virtuais e físicos, com o mínimo de indisponibilidade e reestruturação da parte física necessário, de forma que recupere, total e/ou granular, qualquer item assegurado por sua funcionalidade de backup/restauração e de replicação.
- 2.5.3. A licença de software licenciará cada instância que será protegida, esta poderá ser virtual ou física.
- 2.5.4. Todos os itens da solução deverão ser integrados com a solução de virtualização.
- 2.5.5. A solução deverá incluir funcionalidades de proteção de dados (backup) e replicação integradas em uma única solução, incluindo retorno (rollback) de réplicas e replicação desde e até a infraestrutura On-site e Off-site.
- 2.5.6. A Solução não deverá necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais.
- 2.5.7. Deverá garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através das soluções de virtualização VMware, Hyper-V e Nutanix AHV, conforme

contratada.

- 2.5.8. Deverá ter a capacidade de replicação de dados armazenados entre storages ou máquinas de configuração e de fabricantes diferentes.
- 2.5.9. Deverá proteger o ambiente, sem interromper a atividade das máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção (backup) e migrações em conjunto.
- 2.5.10. Deverá ter a capacidade de testar a consistência do backup e replicação (S.O., aplicação, VM), emitindo relatório de auditoria para garantir a capacidade de recuperação.
- 2.5.11. Deverá prover a deduplicação e compressão das máquinas virtuais diretamente pela solução a durante a operação de backup.
- 2.5.12. Deverá ser capaz de proteger, de forma indistinta uma máquina virtual completa, discos virtuais e os dados contidos nela.
- 2.5.13. Deverá poder recuperar arquivos e/ou pastas contidos dentro de uma máquina virtual sem precisar restaurá-la.
- 2.5.14. Deverá ter a capacidade de integração através de API's dos fabricantes de infraestrutura virtualizada para a proteção de dados.
- 2.5.15. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de "rastreamento de blocos modificados" (CBT - changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação).
- 2.5.16. Deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (backup) a saber:
 - 2.5.16.1. Diretamente através de Storage Area Network (SAN);
 - 2.5.16.2. Diretamente do storage, através do hypervisor I/O (Virtual Appliance);
 - 2.5.16.3. Mediante uso da rede local (LAN);
 - 2.5.16.4. Diretamente do snapshot do storage onde os dados das VM's estejam armazenados.
- 2.5.17. Deverá proporcionar um controle centralizado de implementação distribuída, para isso deverá incluir uma console, integrada ou não, que possibilite uma visão consolidada de sua arquitetura distribuída e conjunto de múltiplos servidores de proteção (backup), relatórios centralizados, alertas consolidados e restauração de autosserviço de máquinas virtuais no nível de sistema de arquivos (granular), com delegação de permissões sobre máquinas virtuais individuais.
- 2.5.18. Deverá poder manter um backup sintético, eliminando assim a necessidade de realizar backups completos (full) periódicos, incremental permanente, o que permitirá economizar tempo e espaço.
- 2.5.19. Deverá contar com tecnologia de deduplicação também para o ambiente de máquinas virtuais para gerar economia de espaço de armazenamento no repositório de backups sem a necessidade de hardware de terceiros (appliancededuplicadora).
- 2.5.20. Deverá proporcionar proteção quase contínua de dados (near-CDP), permitindo a minimização dos Objetivos de Pontos de Recuperação (RPO).
- 2.5.21. Deverá prover/devolver o serviço aos usuários através da inicialização da máquina virtual que falhou, diretamente do backup, armazenado no repositório de backup de segurança, sem necessidade, inclusive de "hidratação" dos dados gravado no repositório do backup, os quais obrigatoriamente deverão estar "deduplicados" e "comprimidos".
- 2.5.22. Deverá permitir a recuperação de mais de uma máquina virtual e/ou ponto de restauração

simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais.

- 2.5.23. Todo serviço de migração das máquinas virtuais do repositório de backup até o armazenamento na produção restabelecida, não deverá afetar a disponibilidade e acesso pelo usuário, sem paradas.
- 2.5.24. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar.
- 2.5.25. Deverá permitir realizar buscas rápidas mediante os índices dos arquivos que sejam controlados por um sistema operacional Windows, quando este seja o sistema operacional executado dentro da máquina virtual da qual se tenha realizado o backup.
- 2.5.26. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.
- 2.5.27. Deverá permitir realizar a truncagem de logs transacionais (transaction logs) para máquinas virtuais com Microsoft Exchange e SQL Server.
- 2.5.28. Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos.
- 2.5.29. Deverá permitir recuperar no nível de objetos de qualquer aplicação virtualizada, em qualquer sistema operacional, utilizando as ferramentas de gestão das aplicações existentes.
- 2.5.30. Deverá incluir ferramentas de recuperação, mediante as quais os administradores de servidores de correio eletrônico, tais como Microsoft Exchange 2010 sp1, 2013 e superiores, possam recuperar objetos individuais, tais como contatos, mensagens, compromissos, anexos, entre outros, sem a necessidade de recuperar os arquivos da máquina virtual como um todo ou reiniciar a mesma.
- 2.5.31. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de serviços de diretório, tais como Microsoft Active Directory, possam recuperar objetos individuais, tais como usuários, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.
- 2.5.32. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de banco de dados, tais como Microsoft SQL Server, possam recuperar objetos individuais, tais como bases, tabelas, registros, entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.
- 2.5.33. Deverá oferecer visibilidade instantânea, capacidades avançadas de busca e recuperação rápida de elementos individuais para Microsoft Sharepoint, desde a versão 2010, sem a necessidade de agentes (recuperação granular).
- 2.5.34. Deverá incluir ferramentas de recuperação de elementos individuais para Microsoft Exchange 2010-SP1 em diante, sem que seja necessário inicializar a máquina virtual a partir do backup e que possa ser extraído a frio (ex. mensagens, tarefas, contatos, etc.) e sem requerer infraestrutura intermediária (staging), fazer busca rápidas no servidor de e-mail.
- 2.5.35. Deverá oferecer testes automatizados de recuperação para todas as máquinas virtuais protegidas, gerando confiabilidade de 100% na execução correta das máquinas virtuais e de suas aplicações (DNS Server, Controlador de domínio, Servidor de e-mail, etc.).
- 2.5.36. Deverá permitir criar uma cópia da máquina virtual de produção, para criação de ambiente de homologação, teste, QA, etc; Em qualquer estado anterior para a resolução de problemas, provas de procedimentos, capacitação, entre outros.

- 2.5.37. Deverá ser possível executar uma ou várias máquinas virtuais a partir do arquivo de backup, em um ambiente isolado, sem a necessidade de espaço de armazenamento adicional e sem modificar os arquivos de backup.
- 2.5.38. Deverá oferecer arquivamento em fita, suportando VTL (Virtual Tape Libraries), biblioteca de fitas e drives LTO3 ou superior, possibilitando a gravação paralela em múltiplos drives, além da criação de pools de mídia globais e pools de mídia GFS.
- 2.5.39. Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção.
- 2.5.40. Deverá ser fornecida com a funcionalidade de acelerar a rede “WAN” para geração de cópia ou replicação das máquinas virtuais, sem utilização de agentes, nem configurações de rede especiais.
- 2.5.41. Deverá incluir suporte para VMware vCloudDirector com visibilidade integrada da infraestrutura vCD no console de backup, fazendo backup de meta-dados e dos atributos associados com vApps e VMs, permitindo a recuperação diretamente ao vCD.
- 2.5.42. Deverá incluir um plug-in para VMware vSphere Web Client, a fim de permitir o monitoramento da infraestrutura de backup diretamente do vSphere Web Client, com visibilidade detalhada e geral do estado dos trabalhos e recursos de backup.
- 2.5.43. Deverá operar em ambientes virtualizados através das soluções da VMware e Hyper-V, incluindo: VMware vSphere 5.5 e/ou Microsoft Hyper-V 2008 R2 e superiores. Além de Nutanix AVH nas versões de 5.5.x a 6.0.x CE 2019.11.22 ou posterior para a Community Edition.
- 2.5.44. Deverá ter a capacidade de monitoramento em tempo real, sem a necessidade de agentes, da infraestrutura virtual e de backup, inclusive máquinas virtuais, simultaneamente para Hyper-V e VMware, com notificação de problemas de backup e desempenho, com geração de alertas e base de conhecimento embutida para resolução dos mesmos.
- 2.5.45. Deverá ter a capacidade de monitoramento e análise de capacidade do ambiente para crescimento, ajustes e planejamentos de crescimento.
- 2.5.46. Deverá garantir a recuperação granular e consistente, sem necessidade de agentes adicionais para o ambiente virtualizado através das soluções acima, principalmente para os seguintes softwares:
- 2.5.46.1. Microsoft Active Directory Server 2003 SP2 em diante;
 - 2.5.46.2. Microsoft Exchange Server 2010 SP1 em diante;
 - 2.5.46.3. Microsoft SQL Server 2008 em diante;
 - 2.5.46.4. Microsoft Sharepoint 2010 em diante.
- 2.5.47. Deverá ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos backups realizados.
- 2.5.48. Deverá regular de forma dinâmica e parametrizável, a exigência sobre os sistemas protegidos, de forma tal, que se possa definir limites de utilização de performance em discos para diminuir o impacto na infraestrutura de produção, durante as atividades de backup.
- 2.5.49. Deverá permitir um método de fácil de recuperação, desde ambientes de contingência, com as ações pré configuradas para evitar ações manuais em caso de desastre, similar a um botão de emergência.
- 2.5.50. Deverá oferecer a possibilidade de armazenar os arquivos de backup de forma criptografada, com algoritmo mínimo de 256 bits, ativando e desativando tal operação, assim como assegurar o trânsito da informação através desse cenário, mesmo que impacte a performance da gravação.
- 2.5.51. Deverá permitir a criação de níveis de delegação de tarefas (perfis) de recuperação no

nível de elementos da aplicação, inclusive para outros usuários, de forma a diminuir a carga de atividades executadas pelo administrador da plataforma.

- 2.5.52. Deverá dispor de funcionalidades integradas que permitam a seleção de um repositório de backup que esteja alojado em um provedor de serviços na nuvem (backup ou replicação na nuvem - cloud providers).
- 2.5.53. Deverá integrar uma solução unificada de monitoração de ambientes virtualizados, com fornecimento de relatórios capazes de apresentar informações do tipo:
 - 2.5.53.1. Relatórios que permitam o planejamento de capacidade;
 - 2.5.53.2. Relatórios que permitam determinar a ineficiência dos recursos em uso;
 - 2.5.53.3. Relatórios que facilitem a visibilidade de tendências negativas e anomalias;
 - 2.5.53.4. Quadros de controle claros, apresentáveis e integráveis em sites web.
- 2.5.54. Deverá correlacionar a execução de trabalhos de backup e réplica com os objetos do ambiente virtual.
- 2.5.55. Deverá oferecer a capacidade de relatar o cumprimento das políticas de proteção de dados e disponibilidade de acordo com parâmetros definidos.
- 2.5.56. Deve suportar múltiplas operações dos componentes/servidores participantes da estrutura de backup, permitindo atividades de backup e recuperação simultâneas.
- 2.5.57. Deve suportar repositório de backup com aumento de escala ilimitado para o armazenamento de dados com suporte aos seguintes sistemas de armazenamento:
 - 2.5.57.1. Microsoft Windows;
 - 2.5.57.2. Linux;
 - 2.5.57.3. Pastas compartilhadas;
 - 2.5.57.4. Appliances deduplicadoras.
- 2.5.58. Suportar servidores proxy de backup virtuais ou físicos para backup de máquinas virtuais.
- 2.5.59. A solução ofertada deve ser capaz de recuperar/executar o servidor virtual protegido, a partir do snapshot do storage conforme integração com os modelos suportados citados no item acima.
- 2.5.60. Deve possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem.
- 2.5.61. Deve estar licenciado para utilização de, no mínimo, 1 biblioteca de fita com número independente da quantidade de drives e slots operando simultaneamente e com compartilhamento entre os jobs de backup.
- 2.5.62. Deve ser ofertada a versão mais atual do software de backup, liberada oficialmente pelo fabricante do software. Caso haja necessidade, por razões de compatibilidade com os demais componentes de hardware e software do ambiente de backup, a Contratante se reserva o direito de utilizar a versão do software imediatamente anterior à versão mais atual, sem nenhum ônus adicional para a Contratante.
- 2.5.63. Deve dar suporte ao BitLocker.
- 2.5.64. A solução ofertada deve ter a capacidade de realizar o restore granular ou total de um servidor virtual a partir do snapshot do storage.
- 2.5.65. Devem ser fornecidas **30 licenças** da solução de backup dos servidores (físicos e/ou virtuais) para a excelência da prestação do serviço.
- 2.5.66. A solução deverá ter a **capacidade de 20TB líquido de armazenamento**.
- 2.5.67. A solução deverá ser composta de hardware e software necessários para a execução do

gerenciamento de backup.

2.6. ITEM 05 - Serviço de Conectividade Wifi com garantia e suporte por 12 meses

- 2.6.1. Deverão ser fornecidos 12 equipamentos compatíveis com a controladora existem na ADEPARA (FortiGate 100E)
- 2.6.2. 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;
- 2.6.3. 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;
- 2.6.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;
- 2.6.5. Deve permitir ser gerenciado remotamente através de links WAN;
- 2.6.6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
- 2.6.7. 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 devem ser tunelados até o controlador wireless;
- 2.6.8. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
- 2.6.9. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
- 2.6.10. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;
- 2.6.11. 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;
- 2.6.12. Possuir funcionalidade de ajuste de potência automática de forma a estender cobertura no caso de falha de APs vizinhos gerenciados pela mesma controladora;
- 2.6.13. Deve suportar mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs;
- 2.6.14. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);
- 2.6.15. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede;
- 2.6.16. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 2.6.17. 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;
- 2.6.18. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
- 2.6.19. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos

dispositivos através do recurso conhecido como Fast Roaming;

- 2.6.20. 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;
- 2.6.21. 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;
- 2.6.22. Deve implementar o padrão IEEE 802.11e;
- 2.6.23. Deve implementar o padrão IEEE 802.11h;
- 2.6.24. Implementar agregação de pacotes A-MPDU e A-MSDU no Access Point;
- 2.6.25. Implementar LPDC - Low Density Parity Check no Access Point;
- 2.6.26. Implementar (MLD) - Maximum Likelihood Demodulation no Access Point;
- 2.6.27. Implementar Maximum Ratio Combining (MRC) no Access Point;
- 2.6.28. Deve possuir indicadores luminosos (LED) para indicação de status;
- 2.6.29. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at;
- 2.6.30. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
- 2.6.31. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
- 2.6.32. Deve possuir certificado emitido pela Wi-Fi Alliance;
- 2.6.33. Deve possuir certificado de homologação válido e vigente emitido pela ANATEL;
- 2.6.34. Características do Hardware
- 2.6.35. Deve ser do tipo Indoor
- 2.6.36. Suportar throughput de 867 Mbps
- 2.6.37. Suportar 512 usuários recomendados por rádio
- 2.6.38. Implementar as tecnologias 802.11 a/b/g/n/ac
- 2.6.39. Operar nas frequências de 2.4 / 5 GHz
- 2.6.40. Possuir ao menos 2 rádios
- 2.6.41. Implementar SU-MIMO 2x2
- 2.6.42. Implementar 802.11ac Wave2
- 2.6.43. Implementar MU-MIMO 1
- 2.6.44. Implementar 802.11ac VHT 20/40/80 MHz
- 2.6.45. Ter potência máxima de ao menos 24 dBm
- 2.6.46. Sensibilidade RX de ao menos -91 dBm
- 2.6.47. Possuir ao menos 2 spatial stream
- 2.6.48. Ter ao menos 4 antenas internas
- 2.6.49. O ganho das antenas internas em 2.4GHz deve ser ao menos 4 dBi
- 2.6.50. O ganho das antenas internas em 5GHz deve ser ao menos 5 dBi
- 2.6.51. Ter 1 antenas internas BLE

- 2.6.52. Deve possuir 1 interfaces de rede 1 Gigabit Ethernet
- 2.6.53. Suportar IEEE 802.3az
- 2.6.54. Permitir operar em 12VDC
- 2.6.55. Possuir trava Kensington
- 2.6.56. Deve suportar temperatura de operação até 45 ° C
- 2.6.57. Implementar Transmit Beamforming (TxBF)
- 2.6.58. Ser certificado WPA3
- 2.6.59. Possuir analisador de espectro
- 2.6.60. Implementar MESH

2.7. Item 06 - Serviços Técnicos Especializados

2.7.1. Os serviços técnicos especializados têm como objetivo garantir o correto funcionamento, segurança, desempenho e disponibilidade de soluções críticas de infraestrutura de TI. Estes serviços incluem atividades de instalação, configuração, manutenção, suporte e otimização de ambientes corporativos que envolvem firewalls, pontos de acesso, soluções antivírus e sistemas de backup.

2.7.2. Atividades incluídas:

- 2.7.2.1. Planejamento e design da política de segurança;
- 2.7.2.2. Instalação física e lógica de appliances (item 01 e 02).
- 2.7.2.3. Configuração de interfaces, zonas, roteamento e NAT;
- 2.7.2.4. Implementação de políticas de acesso (firewall rules), web filtering, IPS, VPNs (IPsec/SSL), controle de aplicativos.
- 2.7.2.5. Integração com Active Directory e autenticação de usuários;
- 2.7.2.6. Validação de alta disponibilidade (HA), balanceamento e failover;
- 2.7.2.7. Testes de conectividade e segurança;
- 2.7.2.8. Documentação técnica e orientações pós-implantação;
- 2.7.2.9. Instalação física e lógica dos APs (item 05);
- 2.7.2.10. Planejamento de canais, SSIDs, VLANs e políticas de QoS;
- 2.7.2.11. Integração com controladoras físicas ou em nuvem;
- 2.7.2.12. Criação de redes para funcionários, convidados e BYOD com políticas de segurança distintas;
- 2.7.2.13. Otimização de roaming e handoff entre APs;
- 2.7.2.14. Documentação da arquitetura wireless;
- 2.7.2.15. Instalação e configuração da console de gerenciamento (Item 03);
- 2.7.2.16. Deploy dos agentes em endpoints e servidores (manual, remoto ou via GPO);
- 2.7.2.17. Criação de políticas por grupos (bloqueios, firewall, DLP, atualização);
- 2.7.2.18. Integração com SIEM ou plataforma de monitoramento;
- 2.7.2.19. Monitoramento inicial e ajustes finos;
- 2.7.2.20. Instalação e configuração do Servidor de Backup (item 04);
- 2.7.2.21. Avaliação do ambiente (servidores físicos, VMs, banco de dados, NAS);

- 2.7.2.22. Planejamento da estratégia de backup: tipo (full/incremental), periodicidade, retenção;
- 2.7.2.23. Configuração de proxies, repositórios e transport modes (Direct SAN, HotAdd, etc.);
- 2.7.2.24. Criação e agendamento de jobs de backup e cópia off-site;
- 2.7.2.25. Configuração de políticas de replicação, se aplicável;
- 2.7.2.26. Teste de restore: arquivo individual, VM completa, bare metal recovery;
- 2.7.2.27. Habilitação de relatórios e alertas;
- 2.7.2.28. Documentação técnica com topologia e procedimentos de restauração.

3. ACORDO DE NÍVEL DE SERVIÇO

3.1. Manutenção e Operabilidade do Ambiente

3.1.1. A LICITANTE se compromete a garantir a operacionalidade da solução, atuando de forma proativa e reativa para resolver qualquer problema técnico que seja reportado. Para tanto deve prover os seguintes serviços:

- Suporte técnico disponível 24 horas por dia, 7 dias por semana.
- Substituição de peças defeituosas nos itens fornecidos, dentro de um prazo máximo de 72 horas úteis após a notificação do problema, para minimizar o tempo de inatividade do sistema.
- Manutenção, correção e atualização da solução ofertada, durante o período de vigência do objeto.

3.2. Registro de Resposta a Solicitações de Suporte

3.2.1. O registro e tratamento das solicitações de suporte seguirão um protocolo estrito baseado na criticidade dos incidentes. O ADEPARÁ poderá registrar ocorrências através sistema web da CONTRATADA ou por meio de uma central de atendimento 0800 ou com número local da cidade de Belém. Os níveis de resposta são categorizados da seguinte forma:

a) Severidade Alta

- Aplicável quando a solução ou equipamentos fornecidos se tornarem completamente indisponíveis.
- Tempo de resposta para início de diagnóstico presencial: 20 minutos, após solicitação.

b) Severidade Média

- Situações em que não há interrupção total da solução ou dos equipamentos, mas há perda parcial de funcionalidade ou degradação significativa de desempenho.
- Tempo de resposta para início de diagnóstico presencial: 2 horas úteis, após a solicitação.
- Atendimento on-site, se necessário, deverá ocorrer dentro do mesmo período.

c) Severidade Baixa

- Casos que envolvem esclarecimentos de dúvidas gerais ou solicitações de serviços não urgentes.
- Tempo de resposta para início de diagnóstico remoto: 8 horas úteis.
- Atendimento on-site, se necessário, será agendado e realizado em até de 2 dias úteis.

ANEXO II-A – PLANILHA COM ITENS E QUANTITATIVOS

<i>Item</i>	Descrição	Unidade de Medida	Qtde	Valor Unitário	Valor Total
1	Serviço de Firewall de próxima geração	Mês	12	R\$ 31.100,04	R\$ 373.200,48
2	Serviço SD-WAN	Mês	12	R\$ 41.429,19	R\$ 497.150,28
3	Serviços de Proteção das Estações de Trabalho e Servidores de Rede (Antivírus)	Mês	12	R\$ 10.506,70	R\$ 126.080,40
4	Serviço de Gestão de Backups	Mês	12	R\$ 3.954,25	R\$ 47.451,00
5	Serviço de Conectividade Wifi/	Mês	12	R\$ 13.711,15	R\$ 164.533,80

ANEXO II-B MODELOS DE DOCUMENTOS

MODELO 01 - TERMO DE CONFIDENCIALIDADE E SIGILO

A AGENCIA AGROPECUÁRIA DO ESTADO DO PARA - ADEPARA
REF: LICITAÇÃO PE Nº ____/2024

Prezados(as) Senhores(as):

A empresa _____, CNPJ nº _____, assume o compromisso de manter a confidencialidade e sigilo sobre todas as informações jurídicas e técnicas relacionadas às informações obtidas junto ao Instituto de Terras do Pará.

Por este termo de confidencialidade e sigilo comprometo-me:

1. A não utilizar as informações a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;
 2. A não efetuar nenhuma gravação ou cópia de documentação confidencial ou arquivos de imagens a que tiver acesso;
 3. A não apropriar material confidencial, de uso restrito e/ou sigiloso que venha a ser disponível;
 4. A não repassar o conhecimento das informações confidenciais, inclusive as plantas baixas e detalhes das edificações visitadas, responsabilizando-se por todas as pessoas que vierem a ter acesso às informações, por seu intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e / ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.
- A vigência da obrigação de confidencialidade e sigilo, assumida pela minha pessoa por meio deste termo, terá a validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste termo.

Pelo não cumprimento do presente Termo de Confidencialidade e Sigilo, fica o abaixo assinado ciente de todas as sanções judiciais que poderão advir.

_____, _____ de _____ de 2024 (local e Data)

Razão Social da Proponente
Assinatura e carimbo do Sócio ou Titular
Ou Representante Legal

MODELO 02 - CARTA DE APRESENTAÇÃO DA PROPOSTA DE PREÇOS
A AGENCIA AGROPECUÁRIA DO ESTADO DO PARA - ADEPARA
REF: LICITAÇÃO PE Nº ____/2024

Prezados(as) Senhores(as):

Em atendimento ao item x.x do Edital do Pregão Eletrônico nº xx/2024 e seus Anexos, apresentamos a Vossas Senhorias nossa Proposta de Preços para prestação de XXXX, de acordo com as especificações técnicas constante neste edital e seus anexos.

A presente proposta foi formulada com base nas especificações, condições técnicas, administrativas e contratuais estabelecidos no Edital do Pregão Eletrônico n.º xx/2024 e seus Anexos, os quais aceitamos e nos comprometemos a cumprir integralmente.

Declaramos que a proposta, em anexo, tem validade pelo prazo de 60 (sessenta) dias, contados da data de abertura desta Licitação.

Declaramos que nos preços cotados estão computadas todas as despesas com tributos, impostos, taxas, e despesas, seja qual for a sua natureza, incluindo, mas não se limitando a, fretes, seguros, encargos sociais, trabalhistas e fiscais, ISS, despesas de viagem, locomoção, estadia, alimentação e quaisquer outras, segundo a legislação em vigor, representando a compensação integral pela prestação dos serviços.

Declaramos que os preços foram cotados sob nossa responsabilidade e renunciando a qualquer solicitação de alteração sobre os preços estabelecidos na proposta.

Estamos cientes que não cabe o direito de qualquer indenização, reembolso ou compensação pela exclusão ou rejeição de nossa proposta.

Apresentamos o local/url onde encontrar na internet, prospectos, manuais ou outras informações dos fabricantes correspondentes aos equipamentos ofertados: _____

(Indicar expressamente a(s) marcas e os modelos dos equipamentos oferecidos, não sendo aceito a utilização de expressões como “referência” ou “similar” ou “conforme nossa disponibilidade de estoque”).

Seguem anexos:

- Toda documentação técnica, em nível de detalhe, que permita completa avaliação dos equipamentos que irão compor a solução do objeto licitado, destacando os itens que se identificam com as especificações definidas, que podem ser através de catálogos dos modelos indicados.
- Planilha de Itens Quantitativos (ANEXO II-A).

Dados da Empresa:

Razão Social:

CNPJ/MF:

Endereço:

Tel./Fax:

Endereço Eletrônico (e-mail):

CEP: _____ Cidade: _____ UF: _____ Banco: _____

Agência: _____ C/C: _____

Dados do Representante Legal da Empresa

Nome: _____

Endereço: _____ CEP: _____ Cidade: _____ UF: _____

CPF/MF: _____ Cargo/Função: _____ RG no

: _____ Expedido por: _____ Naturalidade: _____

Nacionalidade: _____

OBSERVAÇÕES:

Havendo discordância entre as especificações deste objeto descritas no COMPRASNET e as especificações constantes do Termo de Referência, prevalecerão as últimas.

Belém-PA, ____ de ____ 2024

Atenciosamente,

Razão Social da Proponente

Assinatura e carimbo do Sócio ou Titular
ou Representante Legal

ESTUDO TÉCNICO PRELIMINAR

PAE nº 2025/3141716

DESCRIÇÃO DA NECESSIDADE		
QUAL A NECESSIDADE A SER ATENDIDA?	A necessidade a ser atendida é descrita como a implementação de recursos de segurança de tecnologia da informação, integrados e projetados para proporcionar uma segurança robusta e abrangente no ambiente de TI desta Agência de Defesa Agropecuária do Estado do Pará – ADEPARÁ	
DESCRIÇÃO DOS REQUISITOS DE CONTRATAÇÃO		
QUAL O TIPO DE OBJETO?	☐ Bem. ☒ Serviço.	
QUAL A NATUREZA?	☒ Continuada.	☐ Com monopólio. ☒ Sem monopólio.
	☐ Não continuada.	
QUAL A VIGÊNCIA?	☐ 30 dias (pronta entrega). ☐ 180 dias. ☐ 12 meses. ☐ Indeterminado. ☐ dias. ☒ Outro: 12 ☒ meses. ☐ anos.	
PODERÁ HAVER PRORROGAÇÃO?	☒ Sim. ☐ Não. ☐ Não se aplica porque o prazo é indeterminado.	
HÁ TRANSIÇÃO COM CONTRATO ANTERIOR?	☐ Sim. Contrato nº: nnnn/aaaa. Prazo final: dd/mm/aaaa. ☒ Não.	
PADRÃO MÍNIMO DE QUALIDADE	Item	Descrição detalhada
	1	Atendimento dos requisitos mínimos definidos junto ao termo de referência.

	2	Para fins de comprovação de aptidão, deverão ser apresentados atestados de capacidade técnica, com recursos compatíveis com o objeto em estudo, relativos aos itens de maior relevância.
	3	A oferta deverá prover todos os recursos necessários para que cada grupo ou conjunto detenha condições de auferir os resultados mínimos necessários.
	4	A execução do objeto estará diretamente vinculada ao atendimento de níveis mínimos de serviços, definidos para estipular padrões de qualidade mínimos aceitáveis.
	5	Em anexo e junto ao futuro termo de referência, serão definidos os requisitos de demais critérios e padrões mínimos de qualidade para cada lote.
HÁ CRITÉRIOS DE SUSTENTABILIDADE?	☐ Sim. Especificar: <i>(Indicar o critério ou prática).</i> ☒ Não.	
HÁ NECESSIDADE DE TREINAMENTO?	☐ Sim. ☒ Não.	
LEVANTAMENTO DE MERCADO		
ONDE FORAM PESQUISADAS AS POSSÍVEIS SOLUÇÕES?	☐ Consulta a fornecedores. ☒ Contratações similares. ☐ Internet. ☐ Audiência pública. ☐ Outro. Especificar: <i>(Indicar o meio).</i>	
JUSTIFICATIVA TÉCNICA E ECONÔMICA PARA A ESCOLHA DA MELHOR SOLUÇÃO	A crescente complexidade das ameaças cibernéticas requer a implementação de soluções robustas de segurança como o NGFW(Next Generation Firewall), um produto com várias capacidades de segurança, como filtros web, controle de aplicações, IPS e SandBox. Seu objetivo é proteger o acesso do usuário à Internet, bem como os serviços publicados por esta instituição, garantindo assim a continuidade dos serviços que a Adepará presta a sociedade. A aquisição de serviços de Firewall de próxima geração é uma necessidade técnica que visa proteger a infraestrutura de TI, garantir a continuidade das operações e atender às demandas de segurança em um ambiente digital cada vez mais complexo. A escolha de soluções adequadas não só mitigará riscos, mas também proporcionará uma base sólida para o crescimento e a inovação tecnológica da organização.	
HÁ RESTRIÇÃO DE FORNECEDORES?	☐ Sim. ☒ Não.	

DESCRIÇÃO DA SOLUÇÃO	
O QUE SERÁ CONTRATADO?	Empresa especializada para na Prestação de Serviços de Atividade de Execução Continuada, pelo período de 12 meses, compreendendo: - Solução de Firewall de próxima geração; - Solução SD-WAN; - Serviço de Proteção das Estações de Trabalho e Servidores de Rede (Tanto físicos, quanto virtuais) para identificar e mitigar infecções por malwares; - Serviço de Gestão de Backups; - Serviço de Conectividade Wifi; Serviços Técnicos Especializados.
QUAL O PRAZO DA GARANTIA CONTRATUAL?	☐ Não há. ☐ 90 dias. ☐ 12 meses. ☐ dias. ☒ Outro: 12 ☒ meses. ☐ anos.
HÁ NECESSIDADE DE ASSISTÊNCIA TÉCNICA?	☐ Sim. Justificativa: (Indicar o motivo da necessidade de assistência técnica para a contratação). ☒ Não.
HÁ NECESSIDADE DE MANUTENÇÃO?	☒ Sim. Descrever solução: Atualizações de Software e Firmware: Realizar atualizações regulares de software e firmware do firewall para corrigir vulnerabilidades e melhorar o desempenho. Revisão das Regras de Segurança: Revisar e ajustar as regras de filtragem periodicamente para garantir que estejam alinhadas com as políticas de segurança da organização. Monitoramento Contínuo: Implementar monitoramento contínuo do tráfego de rede e análise de logs para detectar atividades suspeitas e responder rapidamente a incidentes. Testes de detecção: Conduza testes de detecção regulares para identificar vulnerabilidades e avaliar a eficácia das defesas do firewall. Documentação com sucesso: Manter registros detalhados das configurações do firewall, atualizações realizadas e incidentes de segurança, facilitando auditorias e análises futuras. Treinamento da Equipe: Promover treinamento contínuo para a equipe de TI e colaboradores sobre as melhores práticas em segurança cibernética e o funcionamento do firewall.

	7. Verificação de Logs: Realizar auditorias periódicas dos logs do firewall para detectar acessos não autorizados ou anomalias sem tráfego. 8. Manutenção Preventiva: Implementar ações preventivas, como revisões trimestrais das configurações e ajustes baseados no desempenho do firewall. 9. Planos de Redundância e Failover: Definir planos de redundância para garantir alta disponibilidade, configurando firewalls em failover para evitar interrupções no serviço. 10. Relatórios regulares: Produzir relatórios regulares sobre o estado do firewall e as atividades de manutenção, ajudando na tomada de decisões informadas sobre segurança. ☐ Não.			
ESTIMATIVA DO QUANTITATIVO NECESSÁRIO				
COMO SE OBTVE O QUANTITATIVO ESTIMADO?	☐ Análise de contratações anteriores. ☐ Análise de contratações similares. ☒ Outro. Especificar: Análise de usuários, equipamentos e sistemas atualmente sustentados.			
DESCRIÇÃO DO QUANTITATIVO?	O quantitativo previsto é o relacionado abaixo, pensando nas necessidades da ADEPARÁ para os próximos exercícios:			
ESPECIFICAÇÃO	Item	Descrição	Und	Qtd
	1	Serviço de Firewall de próxima geração	Meses	12
	2	Serviços SD - WAN	Meses	12
	3	Serviços de Proteção das Estações de Trabalho e Servidores de Rede (Antivírus)	Meses	12
	4	Serviço de Gestão de Backups	Meses	12
	5	Serviço de Conectividade Wifi	Meses	12
	6	Serviços Técnicos Especializados	Meses	12
ESTIMATIVA DO VALOR DA CONTRATAÇÃO				
MEIOS USADOS NA PESQUISA	☐ Pannel de preços. ☒ Contratações similares. ☐ Simas. ☒ Fornecedores. ☐ Internet. ☐ Outro. Especificar: (Indicar o meio).			

ESTIMATIVA DE PREÇO	Item	Descrição	Valor Unitário	Qtd	Valor Total
	1	Serviço de Firewall de próxima geração	R\$ 31.100,04	12	R\$ 373.200,48
	2	Serviços SD – WAN	R\$ 41.429,19	12	R\$ 497.150,28
	3	Serviços de Proteção das Estações de Trabalho e Servidores de Rede (Antivírus)	R\$ 10.506,70	12	R\$ 126.080,40
	4	Serviço de Gestão de Backups	R\$ 3.594,25	12	R\$ 47.451,00
	5	Serviço de Conectividade Wifi	R\$ 13.711,15	12	R\$ 164.533,80
	6	Serviços Técnicos Especializados	R\$ 19.771,25	12	R\$ 237.255,00
				TOTAL	R\$ 1.445.670,96

JUSTIFICATIVA PARA O PARCELAMENTO DA SOLUÇÃO

A SOLUÇÃO SERÁ DIVIDIDA EM ITENS?	☐ Sim.		
	☒ Não. Por quê?	☐ Objeto indivisível. ☒ Tecnicamente inviável. ☒ Aproveitamento da competitividade.	☒ Perda de escala. ☐ Economicamente inviável. ☐ Outro. Especificar: (Indicar o motivo).

CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES

HÁ CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES?	☐ Sim. Especificar:	
	☒ Não.	

ALINHAMENTO DA CONTRATAÇÃO COM O PLANEJAMENTO

HÁ PREVISÃO NO PLANO DE CON- TRATAÇÕES ANUAL?	☐ Sim. Especificar item do PCA: nn.	
	☐ Não. Providências: A despesa não estava prevista para esse exercício.	

RESULTADOS PRETENDIDOS

	☐ Manutenção do Funcionamento Administrativo	☐ Redução de Custos
		☐ Aproveitamento de Recursos Humanos

QUAIS OS BENEFÍCIOS PRETENDIDOS NA CONTRATAÇÃO?	☐ Redução dos Riscos do Trabalho ☐ Ganho de Eficiência ☒ Serviço/Bem de Consumo ☐ Realização de Política Pública Especificar: Criar uma camada de segurança, evitar acessos não autorizados, aumento da confiabilidade e disponibilidade, mitigação de riscos e impactos, maior eficácia operacional, potencial para aumentar a eficiência dos usuários com a introdução de recursos de segurança avançados, além de uma gestão unificada e simplificada para supervisão da segurança, cópias de segurança e acesso, simplificando a administração e monitoramento de todo o ambiente de tecnologia da informação a partir de uma única interface. ☒ Outro.
PROVIDÊNCIAS PENDENTES	
HÁ PROVIDÊNCIAS PENDENTES PARA O SUCESSO DA CONTRATAÇÃO?	☐ Sim. Especificar: <i>(Apresentar cronograma de providências a serem adotadas antes e durante o contrato para assegurar o êxito do resultado, como capacitação de servidores, adequação do espaço físico etc).</i> ☒ Não.
IMPACTOS AMBIENTAS E MEDIDAS DE MITIGAÇÃO	
HÁ PREVISÃO DE IMPACTO AMBIENTAL NA CONTRATAÇÃO?	☐ Sim. Especificar os impactos: <i>(Detalhar).</i> Especificar as medidas de mitigação dos impactos: <i>(Detalhar).</i> ☒ Não.
CONCLUSÃO	
A CONTRATAÇÃO POSSUI VIABILIDADE TÉCNICA, SOCIOECONÔMICA E AMBIENTAL?	☒ Sim. A contratação de serviços de Firewall de Próxima Geração (NGFW) e SD-WAN é altamente viável do ponto de vista técnico. Primeiramente, os NGFWs oferecem uma proteção avançada contra ameaças cibernéticas, incluindo detecção de intrusão, filtragem de aplicativos e inspeção de tráfego SSL, que são essenciais em um ambiente de ameaças cada vez mais sofisticadas. Além disso, eles proporcionam uma gestão centralizada das políticas de segurança, facilitando a aplicação consistente de regras de segurança em toda a rede. Por outro lado, a SD-WAN permite uma otimização significativa do tráfego de rede ao utilizar

	múltiplas conexões de internet de forma inteligente, garantindo alta disponibilidade e desempenho mesmo em condições de rede adversas. A integração de SD-WAN com NGFW também possibilita a aplicação de políticas de segurança segmentadas e dinâmicas baseadas no contexto, como localização do usuário ou tipo de aplicação, o que melhora a segurança e a eficiência operacional. Juntos, esses serviços permitem uma rede mais segura, ágil e escalável, adaptável às necessidades da Adepará. A adoção dessa solução tecnológica pode contribuir para a redução do impacto ambiental associado às operações de TI da ADEPARÁ. A consolidação de recursos e a implementação de práticas de eficiência energética podem ajudar a diminuir o consumo de energia e os resíduos gerados, promovendo uma operação mais sustentável e responsável do ponto de vista ambiental. ☐ Não.
--	--

Cidade (PA), 05 de novembro de 2025.

(Assinatura)

Emerson Ribeiro

Gerência de Tecnologia e Informação - GTI

CONTRATO ADEPARÁ Nº XXXX/AAAA
PAE nº E-2025/3141716

RESUMO



CONTRATANTE

Agência de Defesa Agropecuária do Estado do Pará |
AUTARQUIA
CNPJ nº 05.470.347.0001-11.



CONTRATADO

Nome da razão social da pessoa jurídica
CNPJ nº xx.xxx.xxx/xxxx-xx.



OBJETO

Prestação de serviço de segurança de informação (firewall), constantes nos itens **1, 2, 3, 4, 5 e 6** do TR.

LOCAL DE PRESTAÇÃO DO SERVIÇO

O serviço será realizado na sede administrativa da ADEPARÁ, localizada na Tv. Mariz e Barros, 1184 - Pedreira, Belém - PA, 66080-008.



VALOR TOTAL

R\$ xxx.xxx,xx.

REAJUSTE

Índice ☐ IPCA ☐ INPC ☐ INCC ☒ IGPM

Período A cada **12 meses**, a contar de **11/11/2025**.

PAGAMENTO

Forma Ordem bancária.

Prazo **30 dias corridos**, a contar do recebimento da nota fiscal ou fatura atestada pelo fiscal do contrato.



FISCALIZAÇÃO

O fiscal do contrato é o servidor **NOME DO SERVIDOR**, CPF nº xxx.xxx.xxx-xx, matrícula nº nnnn, lotado no [inserir setor]. (Esses dados devem ser inseridos por ocasião da assinatura do contrato).



VIGÊNCIA

Prazo **12 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

AGÊNCIA DE DEFESA AGROPECUÁRIA DO ESTADO DO PARÁ, autarquia, CNPJ nº 05.470.347.0001-11, com sede na Tv. Mariz e Barros, nº 1184, Bairro: Pedreira, Belém-PA, CEP: 66.085-023, neste ato representado pelo **DIRETOR GERAL JAMIR JUNIOR PARAGUASSU MACEDO**, nomeado pela Decreto do Gabinete do Governador, publicada no DOE de 16 de Junho de 2020, pag 04, portador da matrícula funcional nº 54189457/2.

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 XX**, constante no PAE nº **E-2025/3141716** e é regido pela Lei Federal nº 14.133/21.

CLÁUSULA 3

Objeto

3.1 O objeto da contratação é a **prestação de serviço de segurança de informação (firewall)**, compreendendo, conforme descrito no Termo de Referência, o qual **ADERE** a este documento para todos os fins:

- **Serviço de Firewall de próxima geração;**
- **Solução SD-WAN;**
- **Serviços de Proteção das Estações de Trabalho e Servidores de Rede (Antivírus);**
- **Serviço de Gestão de Backups;**

- **Serviço de Conectividade Wifi;**
- **Serviços Técnicos Especializados;**

3.2 Este instrumento se vincula ao edital licitatório citado na Cláusula 2, à proposta do licitante vencedor e aos anexos desses documentos.

3.3 Os serviços contratados são os seguintes itens descritos no Termo de Referência:

Lote	Item	Preço unit	Qtd	Total
1	1	R\$ 0,00	0	R\$ 0,00
	2	R\$ 0,00	0	R\$ 0,00
	3	R\$ 0,00	0	R\$ 0,00
	4	R\$ 0,00	0	R\$ 0,00
	5	R\$ 0,00	0	R\$ 0,00
	6	R\$ 0,00	0	R\$ 0,00
TOTAL				R\$ 0,00

CLÁUSULA 4

Local e hora da prestação do serviço

O local e a hora da prestação dos serviços contratados são aqueles previstos no Termo de Referência.

CLÁUSULA 5

Preço

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

As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria do orçamento do Estado do Pará, para o exercício de **2025**, na classificação abaixo:

Fonte	01501.000061
Programa de Trabalho	20.122.1297–8338 (Operacionalização das Ações Administrativas)
Elemento de Despesa	339040
Ação detalhada	282908

CLÁUSULA 7

Reajuste

7.1 O contrato será reajustado pelo **IGPM**.

7.2 É devido reajuste contratual apenas a cada **12 meses**, a contar de **11/11/2025** (data do orçamento estimado).

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 independerá 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 **30 dias corridos**, a contar do recebimento da nota fiscal ou fatura atestada pelo fiscal do contrato.

8.2 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.

9.2 A garantia corresponderá a **5%** 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 **15 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 A garantia de execução do contrato não desobriga o CONTRATADO de apresentar a garantia contratual dos serviços adquiridos, no mínimo, 12 meses, a partir do seu recebimento pela contratante.

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.

10.2 O CONTRATADO tem a obrigação de:

- a.** Cumprir todas as obrigações constantes deste contrato e seus anexos, assumindo exclusivamente os riscos e as despesas decorrentes de sua execução.
- b.** Aceitar acréscimos ou supressões unilaterais impostos pelo CONTRATANTE de até **25%** do valor atualizado do contrato nas mesmas condições pactuadas inicialmente.
- c.** Manter preposto aceito pelo CONTRATANTE no local da prestação do serviço para o representar na execução do contrato.
- d.** A indicação do preposto do CONTRATADO ou a sua manutenção poderá ser recusada pelo CONTRATANTE mediante justificativa, devendo o CONTRATADO designar outro para o exercício da atividade.
- e.** Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior e prestar esclarecimentos ou informações por eles solicitados.
- f.** Alocar os empregados em número compatível para o cumprimento deste contrato e com a habilitação e conhecimento adequados para a execução do serviço, fornecendo os materiais, equipamentos, ferramentas e utensílios necessários para tanto, cuja quantidade, qualidade e tecnologia deverão atender às recomendações dos órgãos de regulação responsáveis e à legislação aplicável.

- g.** No prazo fixado pelo fiscal do contrato, reparar, corrigir ou refazer às suas expensas o serviço no qual se verificar vícios, defeitos ou incorreções resultantes de sua má execução contratual ou dos materiais empregados.
- a.** Durante a vigência do contrato, não contratar cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o 3º grau, de dirigente do CONTRATANTE ou de agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato.
- b.** 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.
- c.** Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato e obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao CONTRATANTE.
- d.** Comunicar ao fiscal do contrato, no prazo de **24 horas**, qualquer ocorrência anormal que se verifique no local da execução do objeto contratual.
- e.** Prestar todo esclarecimento ou informação solicitada pelo CONTRATANTE ou por seus prepostos, garantindo-lhes, a qualquer tempo, o acesso ao local dos trabalhos e aos documentos relativos à execução do serviço.
- f.** Por determinação do CONTRATANTE, paralisar a atividade que não esteja sendo bem executada ou que ponha em risco a segurança das pessoas ou seus bens.
- g.** Durante a vigência do contrato, promover a guarda, manutenção e vigilância de materiais, ferramentas e tudo o que for necessário à execução do serviço.

- h.** Conduzir os trabalhos observando às normas da legislação aplicável e às determinações dos Poderes Públicos, mantendo o local dos serviços limpo e nas melhores condições de segurança, higiene e disciplina.
- i.** Submeter previamente e por escrito ao CONTRATANTE qualquer mudança nos métodos executivos especificados no memorial descritivo ou documento similar para sua análise e aprovação.
- j.** Não permitir:
 - 1.** o trabalho de pessoa menor de 16 anos no objeto deste contrato, exceto na condição de aprendiz para os maiores de 14 anos; e
 - 2.** a utilização do trabalho da pessoa menor de 18 anos em trabalho noturno, perigoso ou insalubre, em qualquer hipótese.
- 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.

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 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.

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

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

Multa	
Moratória	Compensatória
a. 0,33% sobre o valor da parcela inadimplida por dia de atraso injustificado até o limite de 30 dias corridos .	20% sobre o valor total do contrato, no caso de inexecução total do seu objeto.
b. 0,33% 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 Antes da aplicação das sanções, o CONTRATADO será notificado para apresentar defesa no prazo de **15 dias úteis**, contado de sua intimação.

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

12.7 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.

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

12.9 A aplicação das sanções deve observar:

- a. A natureza e gravidade da infração.
- b. As peculiaridades do caso.
- c. As circunstâncias agravantes e/ou atenuantes.
- d. Os danos causados ao CONTRATANTE.
- e. A implantação ou aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.10 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.

12.11 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.

12.12 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.

12.13 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.

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

Extinção do contrato

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

14.2 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.

14.3 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.

14.4 Na hipótese do item 14.3, o CONTRATANTE poderá optar, ainda, pela extinção do contrato e adotar as medidas previstas em lei para a continuidade da execução do objeto.

CLÁUSULA 15

Fiscalização

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 16

Interpretação

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 17

Tratamento adequado dos conflitos de interesse

Observado o disposto na Cláusula 16, 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 18

Divulgação e publicação

18.1 O CONTRATANTE divulgará este contrato no Portal Nacional de Contratações Públicas (PNCP) em até **10 dias úteis** e o publicará no Diário Oficial do Estado em forma de extrato, no prazo de **10 dias úteis**.

18.2 Os prazos contidos no item 18.1 são contados da data da assinatura do contrato.

CLÁUSULA 19

Vigência

19.1 O prazo de vigência da contratação é de **12 (dose) meses**, com início e ____/____/____ e término em ____/____/____, prorrogável sucessivamente por até 10 anos, na forma do artigo 107 da Lei nº 14.133, de 2021.

19.2 A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o CONTRATADO, atentando, ainda, para o cumprimento dos seguintes requisitos:

19.2.1. Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

19.2.2. Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

19.2.3. Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

19.2.4. Haja manifestação expressa do CONTRATADO informando o interesse na prorrogação;

19.2.5. Seja comprovado que o CONTRATADO mantém as condições iniciais de habilitação; e

19.3. O CONTRATADO não tem direito subjetivo à prorrogação contratual.

19.4. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

19.5. O contrato não poderá ser prorrogado quando o CONTRATADO tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

CLÁUSULA 20

Foro

As PARTES elegem o foro da Comarca de Belém-PA para resolver os litígios oriundos deste contrato, observado o disposto na Cláusula 17.

Belém (PA), ____ de _____ de 2025.

JAMIR JUNIOR PARAGUASSU MACEDO

Diretor Geral
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



ASSINATURAS

Número do Protocolo: 2025/3141716

Anexo/Sequencial: 91

Este documento foi assinado eletronicamente na forma do Art. 6º do Decreto Estadual Nº 2.176, de 12/09/2018.

Assinatura(s) do Documento:

Assinado eletronicamente por: YANE EVANDRA ANDRADE FARIAS, **CPF:** ***.040.202-**

Em: 12/11/2025 21:17:53

Aut. Assinatura: b53b94b5ff0019d0cc22d181bd672a3862b92156bb609ed390babada15523132



Identificador de autenticação: b34ce5cb-b036-4fa3-8fa4-af9e53c29e8b

Confira a autenticidade deste documento em
<https://www.sistemas.pa.gov.br/validacao-protocolo>