ATA DE REGISTRO DE PREÇOS Nº 109/2024
PREGÃO Nº 056/2024
PROCESSO ADMINISTRATIVO Nº 2024-X3CN2
CIDADES Nº 2024.500E1700001.02.0026

Pelo presente instrumento, a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA**, Fundação Pública com Personalidade Jurídica de Direito Privado, inscrita no CNPJ sob o nº 36.901.264/0001-63, com sede na Rua Pernambuco, nº 1100, Edifício Estilo Center, 3ª Andar- Praia da Costa, Vila Velha/ES, CEP: 29.101-284, representada legalmente pelo seu **Diretor de Gente, Gestão, Finanças e Compras, Sr. JORGE TEIXEIRA E SILVA NETO, e Diretor de Operações, Logística, Tecnologia da Informação e Comunicação, Infraestrutura e Manutenção, Sr. LEONARDO CEZAR TAVARES,** adiante denominada **CONTRATANTE**, considerando o julgamento da licitação na modalidade de **PREGÃO, PARA REGISTRO DE PREÇOS**, sob **nº 056/2024**, RESOLVE registrar os preços das empresas, atendendo as condições previstas no Instrumento Convocatório e as constantes desta Ata de Registro de Preços, e regido pela Lei Federal nº 14.133/2021, pelos Decretos Estaduais nº 5.354-R/2023 e 5.545-R/2023, e suas alterações e em conformidade com as disposições a seguir:

1 – DO OBJETO

1.1 – A presente Ata tem por objeto o registro de preços para a eventual **REGISTRO DE PREÇOS PARA AQUISIÇÃO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION) ATRAVÉS DO PROJETO DE INVESTIMENTO, VISANDO ATENDER AS NECESSIDADES DO SETOR DE TECNOLOGIA DA INFORMAÇÃO DO HOSPITAL ESTADUAL CENTRAL- DR. BENÍCIO TAVARES PEREIRA**, conforme especificações constantes no Anexo I da presente Ata de Registro de Preços , assim como as propostas cujos preços tenham sido registrados, independentemente de transcrição.

2 – DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1 – O preço registrado, as especificações do objeto, as quantidades mínimas e máximas de cada item, fornecedor(es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

ITEM	DESCRIÇÃO DO OBJETO	UND	QTD	VALOR UNITÁRIO	VALOR TOTAL
01	FIREWALL NGFW COM LICENCA/GARANTIA DE 36 (TRINTA E SEIS) MESES DE APPLICATION CONTROL, IPS, AMP, WEB FILTERING, ANTISPAM, SOLUCAO DE LOGS, ANALISE E RELATORIOS.	UNIDADE	01	R$ 142.000,00	R$ 142.000,00

2.2 – A listagem do cadastro de reserva referente ao presente registro de preços consta como Anexo I a esta Ata.

3 – ÓRGÃO OU ENTIDADE GERENCIADORA E PARTICIPANTE(S)

3.1 – A entidade gerenciadora será a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA**.

3.2 – São órgãos ou entidades participantes do registro de preços as unidades hospitalares geridas pela FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA.

3.3 – É vedado efetuar acréscimos nos quantitativos fixados na Ata de Registro de Preços.

4 – DA ADESÃO À ATA DE REGISTRO DE PREÇOS

4.1 – Durante a vigência da ata, os órgãos e as entidades da Administração Pública estadual, distrital e municipal que não participaram do procedimento de IRP poderão aderir à ata de registro de preços na condição de não participantes, mediante requerimento de adesão enviado, eletronicamente, a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) com os seguintes elementos mínimos:

4.1.1 – Identificação da ARP de interesse;

4.1.2 – Indicação dos itens e respectivas quantidades;

4.1.3 – Endereços de entrega ou de prestação dos serviços;

4.1.4 – Dados de contato do requerente;

4.1.5 – Assinatura e identificação do subscritor; e

4.1.6 – Outras informações eventualmente requeridas pela **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata).

4.2 – A autorização da **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) apenas será realizada após a aceitação da adesão pelo fornecedor.

4.3 – A **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.

4.4 – Após a autorização da **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata), o órgão ou entidade não participante deverá efetivar a aquisição ou a contratação solicitada em até noventa dias, observado o prazo de vigência da ata.

4.5 – Dos limites para as adesões:

4.5.1 – As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) e para os participantes.

4.5.2 – O quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) e os participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.

4.5.3 – Para aquisição emergencial de medicamentos e material de consumo médico-hospitalar por órgãos e entidades da Administração Pública estadual, distrital e municipal, a adesão à ata de registro de preços gerenciada pelo Ministério da Saúde não estará sujeita ao limite previsto no item 4.5.1.

5 – VALIDADE, FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

5.1 – A validade da Ata de Registro de Preços será de 01 (um) ano, contados a partir da assinatura, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

5.1.1 – O contrato decorrente da ata de registro de preços terá sua vigência estabelecida no próprio instrumento contratual e observará no momento da contratação e a cada exercício financeiro a disponibilidade de registros orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 01 (um) exercício financeiro.

5.1.1.1 – O instrumento contratual de que trata o item deverá estar vigente no prazo de validade da ata de registro de preços.

5.1.2 – Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos registros orçamentários respectivos.

5.2 – A contratação com os fornecedores registrados na ata será formalizada pelos órgãos ou entidades interessadas por intermédio de instrumento contratual, informação registros orçamentários, ordem de fornecimento ou outro instrumento hábil, conforme o art. 95 da Lei nº 14.133/2021.

5.3 – Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133/2021.

5.4 – Após a homologação da licitação ou da contratação direta, deverão ser observadas as seguintes condições para formalização da ata de registro de preços:

5.4.1 – Serão registrados na ata os preços e os quantitativos do licitante vencedor;

5.4.2 – Será incluído na ata, na forma de anexo, o registro dos licitantes ou dos fornecedores que:

5.4.2.1 – Aceitarem cotar os bens, as obras ou os serviços com preços iguais aos do adjudicatário, observada a classificação da licitação; e

5.4.2.2 – Mantiverem sua proposta original.

5.4.3 – Será respeitada, nas contratações, a ordem de classificação dos licitantes ou dos fornecedores registrados na ata.

5.5 – O registro a que se refere o item 5.4.2 tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.

5.6 – Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.

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

5.7.1 – Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital; e

5.7.2 – Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas no item 9.

5.8 – O preço registrado com indicação dos licitantes e fornecedores será divulgado no PNCP e no site da Fundação e ficará disponibilizado durante a vigência da ata de registro de preços.

5.9 – Após a homologação da licitação, o licitante mais bem classificado será convocado para assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital de licitação sob pena de decair o direito, sem prejuízo das sanções previstas na Lei nº 14.133/2021.

5.9.1 – O prazo de convocação poderá ser prorrogado 01 (uma) vez, por igual período, mediante solicitação do licitante ou fornecedor convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata).

5.10 – A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no Sistema de Registro de Preços.

5.11 – Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital ou no aviso de contratação, e observado o disposto no item 5.7 e subitens, fica facultado à **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

5.12 – Na hipótese de nenhum dos licitantes que trata o item 5.4.2.1, aceitar a contratação nos termos do item anterior, a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata), observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

5.12.1 – Convocar para negociação os demais licitantes ou fornecedores remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

5.12.2 – Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

5.13 – A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

6 – ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

6.1 – Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

6.1.1 – Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos da alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133/2021;

6.1.2 – Em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

6.1.3 – Na hipótese de previsão no edital de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos da Lei nº 14.133/2021.

6.1.3.1 – No caso do reajuste, deverá ser respeitada a contagem da anualidade e o índice previstos para a contratação;

6.1.3.2 – No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

7 – NEGOCIAÇÃO DE PREÇOS REGISTRADOS

7.1 – Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) convocará o fornecedor para negociar a redução do preço registrado.

7.1.1 – Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas.

7.1.2 – Na hipótese prevista no item anterior, a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado e não convocará os licitantes ou fornecedores que tiveram seu registro cancelado.

7.1.3 – Se não obtiver êxito nas negociações, a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) procederá ao cancelamento da ata de registro de preços, adotando as medidas cabíveis para obtenção de contratação mais vantajosa.

7.1.4 – Na hipótese de redução do preço registrado, a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços para que avaliem a conveniência e a oportunidade de diligenciarem negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133/2021.

7.2 – Quando o preço de mercado se tornar superior aos preços registrados, é facultado ao fornecedor requerer a revisão, mediante demonstração de fato superveniente que tenha provocado elevação que impossibilite o cumprimento das obrigações contidas na ata e desde que atendidos os seguintes requisitos:

7.2.1 – O requerimento seja formulado antes da formalização do contrato ou execução;

7.2.2 – A modificação das condições que impactam na formação do preço seja substancial e extraordinária, de forma a caracterizar alteração desproporcional entre os encargos do fornecedor da ARP e os da **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata);

7.2.3 – Seja efetivamente comprovada a desatualização, por meio de apresentação de planilha de custos e documentação comprobatória correlata que demonstre que os preços registrados se tornaram inviáveis nas condições inicialmente pactuadas.

7.3 – A iniciativa e o encargo da demonstração da necessidade de atualização de preço serão do fornecedor, cabendo a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) a análise e deliberação a respeito do pedido.

7.4 – Ao receber o pedido, a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) poderá decidir pela suspensão da ata, até a conclusão da análise.

7.5 – Comprovada a desatualização decorrente de fato superveniente que prejudique o cumprimento da ata, a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) poderá:

7.5.1 – Efetuar a atualização do preço registrado, nos termos requeridos pelo fornecedor, mediante celebração de termo aditivo; e

7.5.2 – Cancelar o preço registrado, liberando o fornecedor do compromisso assumido, sem a aplicação de sanções administrativas.

7.6 – Se não houver prova efetiva da desatualização dos preços e da existência de fato superveniente, o pedido será indeferido pela **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) e o fornecedor continuará obrigado a cumprir os compromissos pelo valor registrado, sob pena de cancelamento do registro de preços e de aplicação das penalidades administrativas previstas em lei e na ata.

7.7 – Na hipótese do cancelamento do registro de preços previsto no item 7.2.2, a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) poderá convocar os demais fornecedores integrantes do cadastro de reserva que aceitaram cotar o objeto em preços iguais aos do vencedor ou que mantiveram sua proposta final.

7.8 – Excepcionalmente, na hipótese do item 7.6, a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) poderá liberar o fornecedor do compromisso assumido sem a aplicação de sanções quando, constatada a existência de fato superveniente que implique em desatualização dos preços, não for possível quantificar seu impacto no valor originalmente registrado.

7.9 – O reajuste e a repactuação dos preços registrados dependerão de requerimento do fornecedor, observando as normas aplicáveis aos contratos administrativos.

7.9.1 – A **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) comunicará os órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços sobre a efetiva alteração do preço registrado, para que avaliem a necessidade de alteração contratual, observado o disposto no art. 124 da Lei nº 14.133/2021.

8 – REMANEJAMENTO DAS QUANTIDADES REGISTRADAS NA ATA DE REGISTRO DE PREÇOS

8.1 – As quantidades previstas para os itens com preços registrados nas atas de registro de preços poderão ser remanejadas entre órgãos ou entidades participantes do lote, incluindo o gerenciador, quando este for participante, e para os quantitativos ainda não contratados.

8.2 – O órgão ou entidade solicitante realizará consulta formal e direta aos demais participante informando o(s) item(ns) e o(s) quantitativo(s) que deseja.

8.3 – O órgão ou entidade cedente verificará a possibilidade de remanejamento e, se constatada a possibilidade, somente poderá autorizar o remanejamento mediante declaração de sua autoridade competente atestando a disponibilidade de saldo não contratado e a ciência quanto à redução do seu quantitativo solicitado.

8.4 – O órgão ou entidade solicitante deverá submeter o pedido a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) juntamente com a justificativa para o acréscimo e a autorização de remanejamento do órgão ou entidade cedente.

8.5 – Recebido o pedido, **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) verificará a conformidade da solicitação e procederá à formalização de termo aditivo.

8.6 – Em nenhuma hipótese o fornecedor beneficiário da ARP poderá negar ou condicionar o fornecimento ao órgão ou entidade participante que teve sua solicitação atendida em função do processo de remanejamento.

9 – CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS

9.1 – O fornecedor terá o registro do seu preço cancelado quando:

9.1.1 – Descumprir as condições da ARP;

9.1.2 – Não formalizar o contrato ou retirar a ordem de fornecimento no prazo estabelecido pela ARP, sem justificativa aceitável;

9.1.3 – Não aceitar reduzir o seu preço registrado, na hipótese de este se tornar superior àqueles praticados no mercado; ou

9.1.4 – Sofrer sanção prevista no inciso III ou IV do caput do art. 156 da Lei nº 14.133, de 2021, observada a abrangência definida nos §§ 4º e 5º do referido dispositivo.

9.2 – Na hipótese do item 9.1.4, caso a sanção aplicada não ultrapasse o prazo de vigência da ARP, poderá a **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata), mediante decisão fundamentada, decidir pela manutenção do registro de preços, sendo vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

9.3 – O cancelamento do registro será formalizado por decisão fundamentada da autoridade máxima da **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata), assegurado o contraditório e a ampla defesa nas hipóteses previstas nos itens 9.1.1, 9.1.2 e 9.1.4.

9.4 – Além das demais hipóteses previstas neste regulamento, o cancelamento do registro de preços poderá ocorrer, justificadamente:

9.4.1 – Por razões de interesse público; ou

9.4.2 – A pedido do fornecedor, decorrente de caso fortuito ou força maior.

10 – DAS PENALIDADES

10.1 – O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no edital.

10.1.1 – As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente após terem assinado a ata.

10.2 – É da competência do gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço, exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos ou entidade participante, caso no qual caberá ao respectivo órgão ou entidade participante a aplicação da penalidade.

10.3 – O órgão ou entidade participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no item 9.1, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

11 – CONDIÇÕES GERAIS

11.1 – As condições gerais de execução do objeto, tais como os prazos para entrega e recebimento, as obrigações da **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – iNOVA CAPIXABA** (entidade gerenciadora da ata) e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, Anexo I do Edital.

11.2 – No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação de parte de itens do grupo se houver prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade.

12 – DO FORO

12.1 – Fica estabelecido o Foro de Vila Velha, munícipio do Estado do Espírito Santo, para dirimir quaisquer dúvidas oriundas direta ou indiretamente deste instrumento, renunciando-se expressamente a qualquer outro, por mais privilegiado que seja.

E assim, por estarem justos e acordados, assinam a presente Ata de Registro de Preços para que produza seus efeitos legais.

(Assinado Eletronicamente)
JORGE TEIXEIRA E SILVA NETO
Diretor de Gente, Gestão, Finanças e Compras – Fundação Inova Capixaba
Competência Delegada por meio da Portaria nº 011-R, de 28 de junho de 2024
ÓRGÃO GERENCIADOR

(Assinado Eletronicamente)
LEONARDO CEZAR TAVARES
Diretor de Operações, Logística, Tecnologia da Informação e Comunicação, Infraestrutura e Manutenção – Fundação Inova Capixaba
Competência Delegada por meio da Portaria nº 011-R, de 28 de junho de 2024
ÓRGÃO GERENCIADOR

(Assinado Eletronicamente)
ALMIR FRANZ DE LIMA
Sócio Administrador – Empresa ALTAS NETWORKS & TELECOM LTDA.
EMPRESA REGISTRADA

ANEXO I – ARP Nº 109/2024

CADASTRO DE RESERVA

NÃO HÁ PARTICIPANTES NO CADASTRO DE RESERVA

1. DESCRIÇÃO DO OBJETO

1.1 O presente Termo de Referência tem por objeto Aquisição por ata de registro de preço, Solução de Firewall de Próxima Geração (Next Generation) juntamente com a licença para suporte e atualização do mesmo, compreendendo fornecimento de equipamentos e softwares integrados em forma de appliance conforme quantidades e exigências estabelecidas neste Termo de Referência.

Lote 01

ITEM	CÓDIGO SIGA	CÓDIGO MV	DESCRIÇÃO DO PRODUTO	UNIDADE	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	273200	23998	FIREWALL NGFW COM LICENCA/GARANTIA DE 36 (TRINTA E SEIS) MESES DE APPLICATION CONTROL, IPS, AMP, WEB FILTERING, ANTISPAM, SOLUCAO DE LOGS, ANALISE E RELATORIOS.	UNIDADE	01		
						VALOR TOTAL DO LOTE 01	**R$**

1.2 Os produtos que compõem a solução ofertada, até a data do pregão eletrônico, devem fazer parte do catálogo de produtos comercializados pelo fabricante no território nacional e não constar como: End-of Support, End-of-Sales, End-of-Life, ou status similar. Neste caso, a comprovação se dará por meio da documentação oficial constante no site público da fabricante ou de declaração emitida pelo fabricante na fase de habilitação.

2.ESPECIFICAÇÃO/DETALHAMENTO DO OBJETO

2.1 CONSIDERAÇÕES GERIAS

2.1.1 Não deverão ser cotados produtos que não atendam as especificações mínimas previstas nas especificações técnicas, sob pena de desclassificação.

2.1.2 O fabricante deve ter obtido mínimo de 75% (setenta e cinco por cento) de efetividade de segurança no teste SVM - Security Value Map de Next Generation Firewall NGFW e à direita da linha da média de custo, que cresce no referido gráfico da direta para a esquerda, executado pela NSSLabs (www.nsslabs.com) em algum dos relatórios entre 2018 a 2023.

2.1.3 O fabricante deve ter obtido mínimo de 90% (noventa por cento) de efetividade de segurança no teste SVM – Security Value Map de Next Generation Intrusion Prevention Systems NGIPS executado pela NSSLabs (www.nsslabs.com) em algum dos relatórios entre 2018 e 2023.

2.1.4 A solução ofertada deve ser de fabricante constante no Quadrante Mágico do Gartner, no quesito NGFW.

2.1.5 Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos pela CONTRATADA.

2.2 FIREWALL NGFW

2.2.1 CARACTERÍSTICA DO EQUIPAMENTO

2.2.1.1 Deve suportar, no mínimo, 18 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6 (considerando pacotes de 512 bytes);

2.2.1.2 Deve suportar, no mínimo, 2.6 Gbps de throughput IPS;

2.2.1.3 Deve suportar, no mínimo, 11.5 Gbps de throughput de VPN IPSec;

2.2.1.4 Deve suportar, no mínimo, 1 Gbps de throughput de VPN SSL;
2.2.1.5 Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL;
2.2.1.6 Deve suportar, no mínimo, 2.2 Gbps de throughput de Controle de Aplicação;
2.2.1.7 Deve suportar, no mínimo, 1 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware;
2.2.1.8 Suporte a, no mínimo, 1.5 milhão de conexões simultâneas;
2.2.1.9 Suporte a, no mínimo, 56 mil novas conexões por segundo;
2.2.1.10 Estar licenciado para, ou suportar sem o uso de licença, até 2 mil túneis de VPN IPSEC Site-to-Site simultâneos;
2.2.1.11 Estar licenciado para, ou suportar sem o uso de licença, até 16 mil túneis de clientes VPN IPSEC simultâneos;
2.2.1.12 Estar licenciado para, ou suportar sem o uso de licença, até 500 clientes de VPN SSL simultâneos;
2.2.1.13 Permitir gerenciar ao menos 128 Access Points;
2.2.1.14 Possuir ao menos 18 interfaces 1Gbps RJ45;
2.2.1.15 Possuir ao menos 2 interfaces 10Gbps SFP+;
2.2.1.16 Possuir ao menos 4 interfaces 1Gbps SFP;
2.2.1.17 Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
2.2.1.18 Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
2.2.1.19 Possuir fonte de alimentação 100-240V AC interna redundante;
2.2.1.20 Possuir no máximo 1 RU de altura.
2.2.2 REQUISITOS MÍNIMOS DE FUNCIONALIDADES
2.2.2.1 Características Gerais
2.2.2.1.1 A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
2.2.2.1.2 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
2.2.2.1.3 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
2.2.2.1.4 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
2.2.2.1.5 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
2.2.2.1.6 A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;
2.2.2.1.7 Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
2.2.2.1.8 Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
2.2.2.1.9 Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
2.2.2.1.10 Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
2.2.2.1.11 Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
2.2.2.1.12 Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

2.2.2.1.13 Os dispositivos de proteção de rede devem suportar sFlow;
2.2.2.1.14 Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
2.2.2.1.15 Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet lógicas;
2.2.2.1.16 Deve suportar NAT dinâmico (Many-to-1);
2.2.2.1.17 Deve suportar NAT dinâmico (Many-to-Many);
2.2.2.1.18 Deve suportar NAT estático (1-to-1);
2.2.2.1.19 Deve suportar NAT estático (Many-to-Many);
2.2.2.1.20 Deve suportar NAT estático bidirecional 1-to-1;
2.2.2.1.21 Deve suportar Tradução de porta (PAT);
2.2.2.1.22 Deve suportar NAT de Origem;
2.2.2.1.23 Deve suportar NAT de Destino;
2.2.2.1.24 Deve suportar NAT de Origem e NAT de Destino simultaneamente;
2.2.2.1.25 Deve poder combinar NAT de origem e NAT de destino na mesma política;
2.2.2.1.26 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
2.2.2.1.27 Deve suportar NAT64 e NAT46;
2.2.2.1.28 Deve implementar o protocolo ECMP;
2.2.2.1.29 Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
2.2.2.1.30 Enviar log para sistemas de monitoração externos, simultaneamente;
2.2.2.1.31 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
2.2.2.1.32 Proteção anti-spoofing;
2.2.2.1.33 Suportar otimização do tráfego entre dois equipamentos;
2.2.2.1.34 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
2.2.2.1.35 Para IPv6, deve suportar roteamento estático e dinâmico (RIPng, OSPFv3, BGP4+);
2.2.2.1.36 Suportar OSPF graceful restart;
2.2.2.1.37 Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
2.2.2.1.38 Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
2.2.2.1.39 Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
2.2.2.1.40 Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
2.2.2.1.41 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;
2.2.2.1.42 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;
2.2.2.1.43 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;
2.2.2.1.44 A configuração em alta disponibilidade deve sincronizar: Sessões;
2.2.2.1.45 A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

2.2.2.1.46 A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
2.2.2.1.47 A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
2.2.2.1.48 O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
2.2.2.1.49 Deve possuir suporte à criação de sistemas virtuais no mesmo appliance;
2.2.2.1.50 Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;
2.2.2.1.51 Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
2.2.2.1.52 O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado a exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;
2.2.2.1.53 Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

2.2.2.1.54 A solução deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;
2.2.2.1.55 O console de administração deve suportar pelo menos inglês, espanhol e português do Brasil;
2.2.2.1.56 O console deve suportar o gerenciamento de switches e pontos de acesso wireless para melhorar o nível de segurança;
2.2.2.1.57 A solução deve oferecer suporte à integração nativa de equipamentos de proteção de e-mail, firewall de aplicativos, proxy, cache e ameaças avançadas;
2.2.2.1.58 Deverá ser comprovado que a solução ofertada foi aprovada no conjunto de critérios de avaliação contido nos testes da NSS Labs, da ICSA Labs, ou por meio de certificação similar, que cumpra a mesma finalidade ou que ateste as mesmas funcionalidades.
2.2.2.2 Controle por Política de Firewall
2.2.2.2.1 Deverá suportar controles por zona de segurança;
2.2.2.2.2 Controles de políticas por porta e protocolo;
2.2.2.2.3 Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
2.2.2.2.4 Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
2.2.2.2.5 Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;
2.2.2.2.6 Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;
2.2.2.2.7 Ele deve suportar a automação de situações como detecção de equipamentos comprometidos, status do sistema, alterações de configuração, eventos específicos e aplicar uma ação que pode ser notificação, bloqueio de um computador, execução de scripts ou funções em nuvem pública;
2.2.2.2.8 Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);

2.2.2.2.9 Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não supere a velocidade de upload;
2.2.2.2.10 Deve suportar o protocolo padrão da indústria VXLAN;
2.2.2.2.11 Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall;
2.2.2.2.12 Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução;
2.2.2.2.13 A solução deve oferecer suporte à integração nativa com a solução de sandbox, proteção de email, cache e firewall de aplicativos da Web.
2.2.2.3 Controle de aplicações
2.2.2.3.1 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
2.2.2.3.2 Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
2.2.2.3.3 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, LinkedIn, 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;
2.2.2.3.4 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;
2.2.2.3.5 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
2.2.2.3.6 Identificar o uso de táticas evasivas via comunicações criptografadas;
2.2.2.3.7 Atualizar a base de assinaturas de aplicações automaticamente;
2.2.2.3.8 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
2.2.2.3.9 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
2.2.2.3.10 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;
2.2.2.3.11 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
2.2.2.3.12 Deve possibilitar a diferenciação de tráfegos Peer2Peer, possuindo granularidade de controle/políticas para os mesmos;
2.2.2.3.13 Deve possibilitar a diferenciação de tráfegos de Instant Messaging possuindo granularidade de controle/políticas para os mesmos;
2.2.2.3.14 Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o WhatsApp e bloquear a chamada de vídeo;
2.2.2.3.15 Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
2.2.2.3.16 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);

2.2.2.3.17 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
2.2.2.3.18 Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
2.2.2.3.19 Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente.
2.2.2.4 Prevenção de Ameaças
2.2.2.4.1 Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
2.2.2.4.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
2.2.2.4.3 As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
2.2.2.4.4 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
2.2.2.4.5 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;
2.2.2.4.6 Deve permitir o bloqueio de vulnerabilidades;
2.2.2.4.7 Deve incluir proteção contra ataques de negação de serviços;
2.2.2.4.8 Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo;
2.2.2.4.9 Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo;
2.2.2.4.10 Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation;
2.2.2.4.11 Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP;
2.2.2.4.12 Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados;
2.2.2.4.13 Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
2.2.2.4.14 Detectar e bloquear a origem de portscans;
2.2.2.4.15 Bloquear ataques efetuados por worms conhecidos;
2.2.2.4.16 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
2.2.2.4.17 Possuir assinaturas para bloqueio de ataques de buffer overflow;
2.2.2.4.18 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
2.2.2.4.19 Identificar e bloquear comunicação com botnets;
2.2.2.4.20 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;
2.2.2.4.21 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
2.2.2.4.22 Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
2.2.2.4.23 Os eventos devem identificar o país de onde partiu a ameaça;

2.2.2.4.24 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
2.2.2.4.25 Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
2.2.2.4.26 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
2.2.2.4.27 Suportar e estar licenciado com proteção contra ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante.
2.2.2.5 Filtro de URL
2.2.2.5.1 Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
2.2.2.5.2 Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
2.2.2.5.3 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
2.2.2.5.4 Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
2.2.2.5.5 Possuir pelo menos 60 categorias de URLs;
2.2.2.5.6 Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
2.2.2.5.7 Permitir a customização de página de bloqueio;
2.2.2.5.8 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão continuar para permitir o usuário continuar acessando o site);
2.2.2.5.9 Além do Explicit Web Proxy, suportar proxy Web transparente.
2.2.2.6 Identificação de Usuários
2.2.2.6.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E- directory e base de dados local;
2.2.2.6.2 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
2.2.2.6.3 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;
2.2.2.6.4 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
2.2.2.6.5 Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
2.2.2.6.6 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);
2.2.2.6.7 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo

visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
2.2.2.6.8 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
2.2.2.6.9 Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução;
2.2.2.6.10 Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.
2.2.2.7 QoS e Traffic Shaping
2.2.2.7.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
2.2.2.7.2 Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
2.2.2.7.3 Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
2.2.2.7.4 Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
2.2.2.7.5 Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
2.2.2.7.6 Suportar a criação de políticas de QoS e Traffic Shaping por porta;
2.2.2.7.7 O QoS deve possibilitar a definição de tráfego com banda garantida;
2.2.2.7.8 O QoS deve possibilitar a definição de tráfego com banda máxima;
2.2.2.7.9 O QoS deve possibilitar a definição de fila de prioridade;
2.2.2.7.10 Suportar marcação de pacotes Diffserv, inclusive por aplicação;
2.2.2.7.11 Suportar modificação de valores DSCP para o Diffserv;
2.2.2.7.12 Suportar priorização de tráfego usando informação de Type of Service;
2.2.2.7.13 Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.
2.2.2.8 Filtro de Dados
2.2.2.8.1 Permitir a criação de filtros para arquivos e dados pré-definidos;
2.2.2.8.2 Os arquivos devem ser identificados por extensão e tipo;
2.2.2.8.3 Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
2.2.2.8.4 Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
2.2.2.8.5 Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
2.2.2.8.6 Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.
2.2.2.9 Geo Localização
2.2.2.9.1 Suportar a criação de políticas por geolocalização, permitindo o trafego de determinado País/Países sejam bloqueados;
2.2.2.9.2 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
2.2.2.9.3 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;
2.2.2.10 VPN (Virtual Private Network);
2.2.2.10.1 Suportar VPN Site-to-Site e Cliente-To-Site;
2.2.2.10.2 Suportar IPSec VPN;

2.2.2.10.3 Suportar SSL VPN;
2.2.2.10.4 A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
2.2.2.10.5 A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
2.2.2.10.6 A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
2.2.2.10.7 A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
2.2.2.10.8 Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
2.2.2.10.9 Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
2.2.2.10.10 Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
2.2.2.10.11 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;
2.2.2.10.12 Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
2.2.2.10.13 Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
2.2.2.10.14 Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
2.2.2.10.15 Deverá manter uma conexão segura com o portal durante a sessão;
2.2.2.10.16 O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits), Windows 11 (32 e 64 bits) e Mac OS X (v10.10 ou superior);
2.2.2.10.17 Deve suportar Auto-Discovery Virtual Private Network (ADVPN);
2.2.2.10.18 Deve suportar agregação de túneis IPSec;
2.2.2.10.19 Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPSec;
2.2.2.10.20 A VPN IPSec deve suportar Forward Error Correction (FEC);
2.2.2.10.21 Deve suportar TLS 1.3 em VPN SSL.
2.2.2.11 Wireless Controller
2.2.2.11.1 Deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;
2.2.2.11.2 Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;
2.2.2.11.3 A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
2.2.2.11.4 O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
2.2.2.11.5 A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
2.2.2.11.6 Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
2.2.2.11.7 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;
2.2.2.11.7.1 Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
2.2.2.11.8 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;
2.2.2.11.9 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;
2.2.2.11.10 A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;
2.2.2.11.11 A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das sub-redes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados localmente na interface do ponto de acesso;
2.2.2.11.12 A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
2.2.2.11.13 A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado dBm;
2.2.2.11.14 A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
2.2.2.11.15 A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
2.2.2.11.16 A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
2.2.2.11.17 A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de off-channel/Background scanning. Quando realizada através de off- channel/Background scanning, a solução deve ser capaz de identificar a utilização do ponto de acesso para caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
2.2.2.11.18 A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
2.2.2.11.19 A solução deve permitir a adição de controlador redundante operando em N+1. Neste modo, o controlador redundante deve monitorar a disponibilidade e sincronizar as configurações do principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar

automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;

2.2.2.11.20 A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas sub-redes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

2.2.2.11.21 A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;

2.2.2.11.22 A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;

2.2.2.11.23 Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

2.2.2.11.24 A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

2.2.2.11.25 A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

2.2.2.11.26 A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

2.2.2.11.27 A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

2.2.2.11.28 A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

2.2.2.11.29 A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

2.2.2.11.30 A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

2.2.2.11.31 Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

2.2.2.11.32 A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;

2.2.2.11.33 A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

2.2.2.11.34 A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

2.2.2.11.35 A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;

2.2.2.11.36 A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;
2.2.2.11.37 A solução deve implementar regras de firewall (stateful) para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que deve usar como critério endereços de origem e destino (IPv4 e IPv6), portas e protocolos;
2.2.2.11.38 A solução deve implementar recurso de web filtering para controle de websites acessados na rede wireless. Deve possuir uma base de conhecimento para categorização dos sites e permitir configurar quais categorias de sites serão permitidos e bloqueados para cada perfil de usuário e SSID;
2.2.2.11.39 A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle. Deve permitir o funcionamento deste recurso e a atualização periódica da base de aplicações durante todo o período de garantia da solução;
2.2.2.11.40 A base de reconhecimento de aplicações através de DPI deve identificar com, no mínimo, 1500 (mil e quinhentas) aplicações;
2.2.2.11.41 A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;
2.2.2.11.42 A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;
2.2.2.11.43 A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:
2.2.2.11.43.1 Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);
2.2.2.11.43.2 Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; Split-Tunneling
2.2.2.11.43.3 ASLEAP;
2.2.2.11.43.4 Null Probe Response / Null SSID Probe Response;
2.2.2.11.43.5 Long Duration;
2.2.2.11.43.6 Ataques contra Wireless Bridges;
2.2.2.11.43.7 Weak WEP;
2.2.2.11.43.8 Invalid MAC OUI.
2.2.2.11.44 A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de autenticação;
2.2.2.11.45 A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;
2.2.2.11.46 A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
2.2.2.11.47 Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
2.2.2.11.48 Deve implementar autenticação administrativa através do protocolo RADIUS;
2.2.2.11.49 Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
2.2.2.11.50 Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
2.2.2.11.51 A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;

2.2.2.11.52 Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
2.2.2.11.53 A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
2.2.2.11.54 A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
2.2.2.11.55 A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
2.2.2.11.56 A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
2.2.2.11.57 A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
2.2.2.11.58 A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
2.2.2.11.59 A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
2.2.2.11.60 A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
2.2.2.11.61 A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
2.2.2.11.62 A solução deve garantir que usuários se autentiquem em captive portal que faça uso de endereço IPv6;
2.2.2.11.63 A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
2.2.2.11.64 Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
2.2.2.11.65 A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;
2.2.2.11.66 A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
2.2.2.11.67 A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras sub-redes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
2.2.2.11.68 A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
2.2.2.11.69 A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
2.2.2.11.70 A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
2.2.2.11.71 A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

2.2.2.11.72 A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;
2.2.2.11.73 A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
2.2.2.11.74 A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet- like MIB);
2.2.2.11.75 A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato. pcap;
2.2.2.11.76 A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
2.2.2.11.77 A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
2.2.2.11.78 A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
2.2.2.11.79 A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
2.2.2.11.80 A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;
2.2.2.11.81 A solução deve possuir ferramentas de diagnósticos e debug;
2.2.2.11.82 A solução deve suportar comunicação com elementos externos através de APIs;
2.2.2.11.83 SD Deve implementar balanceamento de link por hash do IP de origem;
2.2.2.11.84 Deve implementar balanceamento de link por hash do IP de origem e destino;
2.2.2.11.85 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;
2.2.2.11.86 Deve implementar balanceamento de link por custo configurado do link;
2.2.2.11.87 Deve suportar o balanceamento de, no mínimo, 256 links;
2.2.2.11.88 Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec;
2.2.2.11.89 Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
2.2.2.12 Deve gerar log de eventos que registrem - WAN
2.2.2.12.1 alterações no estado dos links do SDWAN, monitorados pela checagem de saúde; Deve suportar Zero-Touch Provisioning;
2.2.2.12.2 Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes;
2.2.2.12.3 Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;
2.2.2.12.4 A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;
2.2.2.12.5 A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS;
2.2.2.12.6 Suportar UDP Hole Punching em arquitetura ADVPN;
2.2.2.12.7 A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoE configurado;

2.2.2.12.8 As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo;
2.2.2.12.9 Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN;
2.2.2.12.10 Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link.
2.2.3 SOLUÇÃO DE LOGS, ANÁLISE E RELATÓRIOS
2.2.3.1 CARACTERÍSTICAS DO SISTEMA
2.2.3.1.1 Deve ser do mesmo fabricante da solução de firewall (NGFW) ofertada;
2.3.1.1.2 Deve ser obrigatoriamente uma solução em nuvem do próprio fabricante da solução de firewall (NGFW) ofertada;
2.3.1.1.3 Possuir capacidade de recebimento e retenção de logs de pelo menos 1 ano.
2.2.3.2 REQUISITOS MÍNIMOS DE FUNCIONALIDADE
2.2.3.2.1 Funcionalidades Gerais
2.2.3.2.2 Suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções;
2.2.3.2.3 Permitir a criação de administrador geral, que tenha acesso geral a todas as informações;
2.2.3.2.4 Deve possuir a funcionalidade de segundo fator de autenticação via token (aplicação) e e-mail;
2.2.3.2.5 Deve possuir um dashboard centralizado;
2.2.3.2.6 Deve possuir no mínimo as seguintes opções disponíveis no portal de visualização:
2.2.3.2.6.1Visão geral da rede
2.2.3.2.6.1.2 Deve conter no mínimo as seguintes informações para serem customizadas na lista de visualização:
2.2.3.2.6.1.2.1 Modelo/número de série do equipamento;
2.2.3.2.6.1.2.2 Versão do firmware;
2.2.3.2.6.1.2.3 Status (se o equipamento estiver conectado através de um túnel de gerenciamento);
2.2.3.2.6.1.2.4 Status SD-WAN;
2.2.3.2.6.1.2.5 Último relatório compilado;
2.2.3.2.6.1.2.6 Data de expiração da licença/subscrição;
2.2.3.2.6.1.2.7 Tráfego de entrada/saída;
2.2.3.2.6.1.2.8 Endereço IP público;
2.2.3.2.6.1.2.9 Última vez que uma configuração de backup foi criada.
2.2.3.2.6.1.2.10 Deve possuir a visualização em formato de mapa, permitindo visualizar a localização geográfica do equipamento.
2.2.3.2.6.2 Gerenciamento de scripts;
2.2.3.2.6.3 Criação e alteração de configurações dos relatórios;
2.2.3.2.6.4 Inventário para visualização de equipamentos sendo monitorados;
2.2.3.2.6.5 Gerenciamento de contas de administrador.
2.2.3.2.6 Deve possuir visualização de log em tempo real, com filtros;
2.2.3.2.7 Deve possuir análise drilldown para localização em tempo real, usuários, e análise de atividade de rede e alerta de perfis;
2.2.3.2.8 Deve possuir gerador de relatório com modelos de relatórios personalizados e relatórios de agendamento em diferentes formatos para exibir análises baseadas em localização ou ilustrar plataformas de uso de rede;
2.2.3.2.9 Deve mostrar o status de arquivos suspeitos passando por análise de sandbox baseado em nuvem;

2.2.3.2.10 Deve possuir integração com Microsoft Active Directory;
2.2.3.2.11 Deve permitir a configuração de alertas de e-mail para emergências específicas da estrutura de rede, como a Solução de logs, análise e relatórios perdendo conexão com o dispositivo ou falha na fonte de alimentação do dispositivo (firewall);
2.2.3.2.12 Possuir definição de perfis de acesso ao console com permissão granular, como: acesso admin e acesso de somente leitura;
2.2.3.2.13 Deve suportar acesso via API;
2.2.3.2.14 Deve permitir a utilização de Multi-tenancy;
2.2.3.2.15 Deve permitir o gerenciamento de firewalls, bem como a criação de backups e atualização de firmware remotamente;
2.2.3.2.16 Deve permitir a utilização de ferramenta de sandbox do mesmo fabricante da solução de firewall (NGFW) fornecida;
2.2.3.2.17 Deve possuir no mínimo os relatórios:
2.2.3.2.17.1 DNS;
2.2.3.2.17.2 Utilização de aplicação com maior banda consumida;
2.2.3.2.17.2.1 Deve possuir identificação de aplicação peer-to-peer (bittorrent, xunlei, gnutella, filetopia), compartilhamento e armazenamento de arquivos (onebox, google drive, Dropbox, apple cloud) e aplicações voz/vídeo em streaming (youtube, skype, spotify, vimeo, netflix).
2.2.3.2.17.3 Resumo:
2.2.3.17.3.1. Análise de ameaças, tráfego, atividade web, análise de VPN, atividade do sistema.
2.2.3.2.17.4 Atividade WEB:
2.2.3.2.17.4.1 Categorias web mais visitadas;
2.2.3.2.17.4.2 Websites mais visitados;
2.2.3.2.17.4.3 Categorias web e websites mais visitados;
2.2.3.2.17.4.4 Usuários web mais ativos;
2.2.3.2.17.4.5 Mais web sites visitados por usuários mais ativos;
2.2.3.2.17.4.6 Usuários mais ativos dos mais visitados webs sites.
2.2.3.2.17.5 Atividades:
2.2.3.2.17.5.1 Seções: visibilidade de aplicações, análise de tráfego web, análise de comportamento do usuário.
2.2.3.2.17.6 Avaliação de ameaças cibernéticas;
2.2.3.2.17.7 Produtividade do usuário:
2.2.3.2.17.7.1 Utilização de aplicações;
2.2.3.2.17.7.2 Utilização da web.
2.2.3.2.17.8 Prevenção de ameaças:
2.2.3.2.17.8.1 Exploração de vulnerabilidade de aplicações (exploits);
2.2.3.2.17.8.2 Prevenção de vírus;
2.2.3.2.17.8.3 Aplicações de alto risco.
2.2.3.2.17.9 Utilização de rede:
2.2.3.2.17.9.1 Largura de banda.
2.2.3.2.17.10 Relatório de administrador e eventos do sistema:
2.2.3.2.17.10.1 Admin login
2.2.3.2.17.10.1.1 Resumo de login;
2.2.3.2.17.10.1.2 Resumo de login por data;
2.2.3.2.17.10.1.3 Lista de logins sem sucesso.
2.2.3.2.17.10.2 Eventos de sistema:
2.2.3.2.17.10.2.1 Eventos por severidade;

2.2.3.2.17.10.2.2 Eventos de severidade crítica;
2.2.3.2.17.10.2.3 Eventos de alta severidade.
2.2.3.2.17.11 Relatório de VPN:
2.2.3.2.17.11.1 Resumo:
2.2.3.2.17.11.1.1 Tendência de utilização de tráfego VPN;
2.2.3.2.17.11.1.2 Logins de usuários VPN;
2.2.3.2.17.11.1.3 Tentativas de login sem sucesso;
2.2.3.2.17.11.1.4 Principais Usuários VPN Dialup.
2.2.3.2.17.11.2 SSL VPN
2.2.3.2.17.11.2.1 Principais fontes de túneis VPN SSL por largura de banda;
2.2.3.2.17.11.2.2. Principais usuários de túnel SSL VPN por largura de banda;
2.2.3.2.17.11.2.3 Principais usuários de modo web SSL VPN por duração;
2.2.3.2.17.11.2.4 Principais usuários SSL VPN por duração.
2.2.3.2.17.11.3 IPsec VPN:
2.2.3.2.17.11.3.1 Principais túneis IPsec site-to-site por largura da banda;
2.2.3.2.17.11.3.2 Principais túneis Dialup IPsec por largura de banda;
2.2.3.2.17.11.3.3 Principais usuários Dialup IPsec por largura de banda;
2.2.3.2.17.11.3.4 Principais usuários Dialup IPsec por duração.
2.2.3.2.18 Permitir importação e exportação de relatórios;
2.2.3.2.19 Deve ter a capacidade de criar relatórios no formato HTML;
2.2.3.2.20 Deve ter a capacidade de criar relatórios em formato PDF;
2.2.3.2.21 Deve ter a capacidade de criar relatórios no formato XML;
2.2.3.2.22 Deve ter a capacidade de criar relatórios no formato CSV;
2.2.3.2.23 Deve permitir exportar os logs no formato CSV;
2.2.3.2.24 Deve gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
2.2.3.2.25 Permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs;
2.2.3.2.26 Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
2.2.3.2.27 Ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
2.2.3.2.28 Deve ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real;
2.2.3.2.29 Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
2.2.3.2.30 Ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
2.2.3.2.31 Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
2.2.3.2.32 Envio por e-mail de relatórios automaticamente;
2.2.3.2.33 Deve permitir que o relatório seja enviado por email ao destinatário específico;
2.2.3.2.34 Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
2.2.3.2.35 É necessário exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado;
2.2.3.2.36 Deve permitir o uso de filtros nos relatórios;
2.2.3.2.37 Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

2.2.3.2.38 Permitir especificar o idioma dos relatórios criados;
2.2.3.2.39 Gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
2.2.3.2.40 Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
2.2.3.2.41 Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
2.2.3.2.42 Possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
2.2.3.2.43 Deve ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles;
2.2.3.2.44 Importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios;
2.2.3.2.45 Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
2.2.3.2.46 Deve ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma;
2.2.3.2.47 Gerar alertas de eventos a partir de logs recebidos;
2.2.3.2.48 Oferecer suporte ao serviço Indicadores de Comprometimento (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredicto (classificação geral da ameaça), o número de ameaças detectadas;
2.2.3.2.49 Deve permitir o suporte a logs na nuvem pública do Amazon S3;
2.2.3.2.50 Deve permitir o suporte a logs na nuvem pública do Microsoft Azure;
2.2.3.2.51 Deve permitir o suporte aos registros de nuvem pública do Google Cloud;
2.2.3.2.52 Suportar o padrão SAML para autenticação do usuário administrador.
2.2.4. Relatórios de Firewall
2.2.4.1 Deve ter relatório de conformidade com o PCI DSS;
2.2.4.2 Possuir relatório de uso do aplicativo SaaS;
2.2.4.3 Possuir relatório de prevenção de perda de dados (DLP);
2.2.4.4 Possuir relatório IPS (Intruder Prevention System);
2.2.4.5 Possuir relatório de reputação do cliente;
2.2.4.6 Possuir relatório de análise de segurança do usuário;
2.2.4.7 Possuir relatório de análise de ameaças cibernéticas;
2.2.4.8 Possuir breve relatório resumido diário de eventos e incidentes de segurança;
2.2.4.9 Possuir relatório de tráfego DNS;
2.2.4.10 Possuir relatório de tráfego de e-mail;
2.2.4.11 Possuir relatório dos 10 principais aplicativos usados na rede;
2.2.4.12 Possuir relatório dos 10 principais sites usados na rede;
2.2.4.13 Possuir relatório de uso de mídia social;
2.2.4.14 Possuir relatório de avaliação de risco para email;
2.2.4.15 Possuir relatório de conformidade com o PCI sem fio;
2.2.4.16 Possuir um relatório de APs e SSIDs autorizados, bem como clientes WIFi;
2.2.4.17 Possuir relatório de vulnerabilidades da solução de segurança gerenciada do equipamento terminal (endpoint);

3. JUSTIFICATIVAS

3.1 FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA AQUISIÇÃO

3.1.1 Como acontece com a maioria das tecnologias, os equipamentos de TI sofrem um processo de depreciação natural, que associado ao avanço das tecnologias, exige uma renovação periódica do parque tecnológico, de forma a garantir a compatibilidade e disponibilidade dos recursos de TI adequados à necessidade dos usuários.
3.1.2 Assim, considerando o atual estado de conservação do parque tecnológico do HEC, faz-se necessário que seja feita a sua renovação, por meio de nova aquisição.
3.1.3 Considerando que o atual Firewall que o HEC possui em suas dependências está descontinuado pelo fabricante, não sendo possível mais renovar a garantia, efetuar atualizações e fazer correções de bugs;
3.1.4 Considerando que o atual Firewall foi adquirido e instalado em **2016** e as tecnologias evoluíram muito e as novas soluções de segurança estão muito mais eficientes;
3.1.5 Atualmente a solução de firewall existente no HEC é limitada e não atende as expectativas em relação a análise granular de tráfego, tampouco as questões de proteção da rede contra ataques externos e filtros de conteúdo/aplicações, reforçando assim a necessidade de modernização desta tecnologia empregando o uso de firewall de próxima geração.
3.1.6 O objeto em questão deverá ser adquirido em lote único, pois todos os componentes precisam estar instalados e em funcionamento para atendimento de maneira mais eficiente e com a mitigação dos riscos para todos os sistemas do HEC como uma solução única. Separar estes itens, aumentaria demasiadamente o risco de atrasos no projeto, na implementação, na interoperabilidade entre os sistemas e equipamentos, gerando uma complexidade muito maior na instalação e no suporte do ambiente, que é crítico para a continuidade dos serviços e atividades do HEC.

3.2 JUSTIFICATIVA DO QUANTITATIVO:
3.2.1 A aquisição da licença de 36 (trinta e seis) meses se faz necessária por se tratar de serviço essencial ao funcionamento do HEC e atendimento aos pacientes do sistema público de saúde. Pois trata-se de serviço essencial contínuo.

3.3 DO SISTEMA DE REGISTRO DE PREÇOS - SRP
3.3.1 O objeto a ser adquirido será por meio do Sistema de Registro de Preços – SRP, conforme pormenorizada em tópico específico do Estudo Técnico Preliminar - ETP, que consta devidamente instruído no processo:
(X) SIM ( ) NÃO
3.3.2 A adoção do sistema de registro de preços para a compra de firewalls oferece múltiplas vantagens, incluindo economia, agilidade, flexibilidade, transparência e eficiência administrativa. Este sistema não só facilita o processo de aquisição, mas também assegura que a organização mantenha uma infraestrutura de segurança robusta e atualizada, atendendo às necessidades de proteção de dados e redes de forma eficaz e econômica.

4. DA CLASSIFICAÇÃO DO SERVIÇO
4.1 O objeto a ser adquirido atende à condição de serviço comum.
(X) SIM ( ) NÃO

5. ENTREGA E RECEBIMENTO
(X) ENTREGA IMEDIATA E ÚNICA
( ) ENTREGA PROGRAMADA
5.1 A entrega do objeto deverá ser feita diretamente no almoxarifado do HEC, situado na R. São José, 76 - Parque Moscoso, Vitória - ES, 29018-140.

5.2 A instalação de equipamentos/softwares que componham a solução deverá ser instalada no HEC.
5.3 A entrega deverá ocorrer sempre em dias úteis e no horário de expediente de segunda feira a sexta-feira no horário de 08h00hs às 12h00hs e das 13h00hs às 17h00h.
5.4 A entrega deve ocorrer em até 20 dias corridos, contados a partir do recebimento da ordem de fornecimento ou de sua publicação, valendo o que ocorrer primeiro.
5.4.1 No caso de entrega programada, o fornecimento deverá seguir o cronograma estabelecido abaixo: N/A
5.5 A entrega deverá ser agendada, via e-mail **coord.ti@hec.es.gov.br** ou pelo telefone 27-3636-4793, com no mínimo 02 dias corridos antes da entrega.
5.6 Os produtos/materiais deverão ser entregues em suas embalagens originais de forma intacta, com identificação do produto, data de fabricação, data de validade, peso líquido, número do Lote, registro no órgão fiscalizador (ABNT, SIM, SIE, SIF INMETRO) quando couber, nome do fabricante, contendo marca, procedência, tudo de acordo com a legislação em vigor, de forma a permitir a completa segurança durante o transporte.
5.7 Caso seja detectado alguma falha no fornecimento, que esteja em desconformidade com o contrato, a contratada deverá regularizar satisfatoriamente no prazo máximo de até 48 (quarenta e oito) horas, após a notificação, sem prejuízo das sanções previstas. O material deve estar em plena validade, observando-se os prazos indicados pelos fabricantes.
5.8 Não serão aceitos materiais com validade vencida ou com data de fabricação defasada que comprometa a sua plena utilização.
5.9 Os itens que compõem o objeto deverão estar em plena validade, observando-se os prazos indicados pelos fabricantes.
5.10 Não será admitida a entrega dos produtos sem a apresentação da ordem de compra/fornecimento ou outro instrumento similar e devidamente acompanhado do documento fiscal (Exemplo: Nota Fiscal).

6. EXIGÊNCIA DE AMOSTRA:
6.1 AMOSTRA
(X) CATÁLOGO
( ) PRODUTO
( ) PRODUTO E CATÁLOGO
( ) OUTROS: _____
( ) NÃO SE APLICA
6.1.1 No caso da exigência do catálogo, este deverá ser encaminhado junto com os documentos de habilitação.
6.1.1.1 Caso o setor demandante tenha necessidade de comprovação das especificações, poderá ser solicitado uma amostra do produto e, deverá ser entregue no prazo máximo de até XX (xxxx) dias úteis após a convocação.
6.1.2 No caso de exigência do produto, a empresa deverá encaminhar amostra para o Setor XXXXX (informar o setor que está realizando a aquisição), situado na (endereço completo), num prazo de até XX (xxxxxx) dias úteis, contados a partir da convocação, identificando corretamente o número do processo.
6.1.2.1 A amostra deverá ser nova, original de fábrica, estar em perfeitas condições de uso, além de devidamente embalada e lacrada.
6.1.2.2 O produto deverá ser da marca e modelo indicados na proposta comercial escrita.
6.1.2.3 Caso a amostra apresentada seja considerada inadequada, será analisada a proposta da empresa subsequente.
6.1.2.4 A empresa que apresentar amostra que não atenda às exigências previstas neste

Termo de Referência será desclassificada.
6.1.2.5 A empresa que não encaminhar a amostra no prazo estabelecido será desclassificado, sendo convocada a proposta subsequente.
6.1.2.6 Após o vencimento do prazo de entrega da amostra não será aceita eventual complementação, ajuste, modificação ou substituição no produto apresentado para fins de adequá-lo às especificações constantes do Termo de Referência.
6.1.2.7 A amostra apresentada poderá ser aberta, manuseada e testada.
6.1.2.8 A(s) amostra(s) rejeitada(s) deverá(ão) ser retirada(s) junto no local apresentado, no prazo máximo de 10 (dez) dias úteis, após este prazo a amostra poderá ser descartada sem gerar direito a indenização.

7. GARANTIA DO PRODUTO
(X) APLICA
( ) NÃO SE APLICA
7.1 O prazo de garantia dos produtos contra defeitos ou vícios de fabricação será de, no mínimo, 12 (doze) meses.
7.1.1 Prevalecerá a garantia oferecida pelo fabricante dos produtos, se for prazo superior ao estabelecido no item acima.
7.1.2 O prazo de substituição dos produtos que apresentarem defeitos ou vícios de fabricação será de até 05 (cinco) dias úteis, contados do recebimento da notificação.
7.2 A empresa deverá fornecer certificado de garantia, por meio de documento próprio ou declaração expressa no Termo de Recebimento Definitivo.
7.3 A CONTRATADA deverá prestar ampla garantia legal a todos os produtos entregues e serviços prestados, no local da instalação deste HEC, durante 5 (cinco) anos, contados do recebimento definitivo pela CONTRATANTE do produto ou serviço, corrigindo qualquer vício ou problema encontrado, sem qualquer ônus para a CONTRATANTE, prestando os serviços de manutenção preventiva e corretiva;
7.4 Caso o problema não seja solucionado a CONTRATADA deverá substituir o equipamento em, no máximo, 48 (quarenta e oito) horas. Equipamento esse semelhante ou superior ao equipamento a ser substituído. Deverá ser prevista a garantia do fornecimento de qualquer parte, peça ou componente dos equipamentos fornecidos por um período mínimo de 05 (cinco) anos;
7.5 A garantia consistirá na reparação das eventuais falhas dos equipamentos, mediante a substituição de peças e/ou componentes que se apresentem defeituosos, de acordo com os manuais e normas técnicas específicas para os equipamentos, devendo ser prestada no local da instalação do equipamento;
7.6 Todo e qualquer desligamento que se fizer necessário nos equipamentos durante os serviços de manutenção dar-se-á somente após a prévia informação e consentimento da CONTRATANTE;
7.7 Capacidade de início de atendimento em até 1 hora para ocasiões de serviço 100% indisponível e verificação remota prévia;
7.8 Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;
7.9 A garantia deve incluir envio de peças ou equipamentos de reposição no local de instalação do equipamento, obedecendo a modalidade NBD (Next Business Day);
7.10 Os chamados em garantia poderão ser abertos diretamente com a CONTRATADA ou autorizada oficial do fabricante através de ligação telefônica gratuita (0800) no idioma Português, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana).

7.11 Aplica-se no que couber, as disposições do Código de Proteção e Defesa do Consumidor, instituído pela Lei nº 8.078, de 11 de setembro de 1990.

7.12 O prazo de validade dos produtos não poderá ser inferior a 80% (oitenta por cento) da validade total, a contar do recebimento definitivo.

8. DO PRAZO DE VIGÊNCIA

8.1 O prazo de vigência da contratação é de 36 (trinta e seis) meses contados da assinatura do contrato ou da publicação do contrato no Diário Oficial), prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

9. ASSISTÊNCIA TÉCNICA
(x) APLICA
( ) NÃO SE APLICA
9.1 O produto objeto deste Termo de Referência terá assistência técnica de, no mínimo, 12 (doze) meses, contados a partir da data da entrega. Incluindo garantia gratuita durante o período da assistência técnica.

10. PAGAMENTO
10.1 A CONTRATANTE pagará à CONTRATADA pelo serviço efetivamente prestado no mês de referência, após a apresentação da Nota Fiscal correspondente, devidamente aceita pela CONTRATANTE, vedada a antecipação.
10.1.1 A CONTRATADA deverá apresentar a nota fiscal à CONTRATANTE até o 5º (quinto) dia útil subsequente da prestação do serviço, devidamente aceita pela CONTRATANTE.
10.1.2 A Nota Fiscal deverá ser emitida no CNPJ da Fundação iNOVA Capixaba somente quando a prestação do serviço for realizada na sede (matriz). Caso contrário, a Nota Fiscal deverá ser emitida no CNPJ da unidade hospitalar (filial).
10.2 O pagamento far-se-á por meio de uma única transferência bancária e será realizado até 30 (trinta) dias após a apresentação da Nota Fiscal.
10.2.1 Os pagamentos serão sempre realizados por meio de transferência bancária, devendo a CONTRATADA informar o domicílio bancário na Nota Fiscal.
10.3 Os pagamentos ficam condicionados ainda à apresentação das certidões de regularidade fiscal e trabalhista, junto com as Notas Fiscais.
10.4 Se houver alguma incorreção na Nota Fiscal, esta será devolvida à CONTRATADA para correção, ficando estabelecido que o prazo para pagamento será contado a partir da data de apresentação da nova Nota Fiscal, sem qualquer ônus ou correção a ser paga pela CONTRATANTE.
10.5 Nos termos do Decreto Estadual nº 5.460-R/2023 e da Instrução Normativa RFB nº 1.234/2012 ou a que vier a substituí-la, a CONTRATANTE deverá proceder a retenção do Imposto de Renda (IR) na Fonte ao efetuar qualquer pagamento à pessoa jurídica pelo fornecimento de bens ou prestação de serviços.
10.5.1 A CONTRATADA deverá emitir a(s) nota(s) fiscal(is), fatura(s) ou qualquer(quaisquer) outro(s) documento(s) de cobrança com o destaque do IR na Fonte. 10.5.2 Excetuam-se se dessa obrigação as hipóteses elencadas no art. 4º da IN RFB nº 1.234/2012, devendo a CONTRATADA apresentar, em conjunto com os demais documentos de cobrança, declaração do respectivo enquadramento, na forma dos anexos da referida Instrução Normativa.

11. PREVISÃO ORÇAMENTÁRIA

11.1 As despesas decorrentes deste objeto correrão à conta do orçamento da Fundação iNOVA Capixaba e serão especificadas no tempo da contratação ou emissão da ordem de serviço ou instrumento equivalente.

12. RESPONSABILIDADES DAS PARTES

12.1 RESPONSABILIDADE DA CONTRATADA

12.1.1 A contratada deve cumprir todas as obrigações, assumindo os riscos e as despesas decorrentes da boa e perfeita execução do objeto.

12.1.2 Entregar o objeto em perfeitas condições, de acordo com as condições e prazos e local propostos, conforme especificações.

12.1.3 Manter o objeto em pleno funcionamento dentro do período da garantia, quando for o caso.

12.1.4 Providenciar a imediata correção das deficiências apontadas pelo setor competente do Contratante.

12.1.4.1 Substituir, reparar ou corrigir, às suas expensas, o objeto com avarias ou defeitos.

12.1.5 Manter, durante toda a execução do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas.

13. RESPONSABILIDADE DA CONTRATANTE

13.1 Receber o objeto no prazo e condições estabelecidas no Termo de Referência e seus anexos.

13.2 Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Termo de Referência e seus anexos.

13.3 A Fundação não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados a essa aquisição, bem como por qualquer dano causado a terceiros em decorrência de ato da contratada, de seus empregados, prepostos ou subordinados.

14. CONDIÇÕES DA HABILITAÇÃO

14.1 Os documentos necessários à habilitação deverão estar com prazo vigente, à exceção daqueles que, por sua natureza, não contenham validade, não sendo aceitos “protocolos de entrega” ou “solicitação de documento” em substituição aos documentos exigidos.

14.2 Como condição prévia ao exame da documentação de habilitação, será verificado o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação, mediante a consulta aos seguintes cadastros:

a) Cadastro de Fornecedores do Estado do Espírito Santo – CRC/ES;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, mantido pela Controladoria Geral da União.

14.3 Apresentação de comprovação de que a empresa possui, em seu quadro funcional ou que mantenha vínculo com a empresa através de cópia de contrato, no mínimo, um profissional alocado no projeto de implantação do sistema com certificação PMP do PMI (Project Management Institute) ou MBA em Gestão de Projetos. As comprovações deverão ser realizadas por meio da apresentação de diplomas, atestados ou certificados;

14.4 Deverá possuir em seu quadro funcional ou que mantenha vínculo com a licitante através de cópia de contrato, ao menos um profissional certificado junto ao fabricante dos equipamentos e soluções ofertados (firewall e solução de logs, análise e relatórios;

14.5 Apresentar comprovação de que os técnicos que irão realizar os serviços tenham a qualificação profissional necessária e sejam certificados pelo fabricante do equipamento;
14.6 Documento comprovando nível de parceria oficial e válido com a fabricante envolvida na solução de segurança proposta, atestando conhecimentos avançados em soluções de NGFW;
14.7 Apresentar no mínimo 01 (um) Atestado de Capacidade Técnica, expedida por pessoa jurídica de direito público ou privado, emitido em papel timbrado e assinado por seu Representante Legal, comprovando ter a Licitante desempenhado de forma satisfatória serviço de entrega, instalação, configuração e suporte técnico da solução de Firewall ofertada, em ambiente com, no mínimo, 100 usuários;
14.8. Os produtos que compõem a solução ofertada, até a data do pregão eletrônico, devem fazer parte do catálogo de produtos comercializados pelo fabricante no território nacional e não constar como: End-of Support, End-of-Sales, End-of-Life, ou status similar. Neste caso, a comprovação se dará por meio documentação oficial constante no site público da fabricante ou de declaração emitida pelo fabricante.

15. DO SIGILO, PROPRIEDADE DAS INFORMAÇÕES E ACORDO DE CONFIDENCIALIDADE

15.1 Todas as informações obtidas e/ou produzidas decorrentes da contratação e execução das atividades são de propriedade do HEC;
15.2 A CONTRATADA e todos os funcionários envolvidos no processo de contratação e execução das atividades deverão manter sigilo absoluto sobre quaisquer informações do HEC;
15.3 É proibida a interceptação de qualquer tráfego oriundo ou destinado ao HEC sem autorização judicial;
15.4 A CONTRATADA, através de seu representante legal, deverá assinar o Acordo de Confidencialidade, e dar ciência do mesmo a toda sua equipe de profissionais e subcontratados que participarão da execução do contrato;
15.5 A CONTRATADA deverá atender às seguintes condições relativas à informação que venha a conhecer, em função da prestação dos serviços ao HEC:
15.5.1. Não poderá divulgar ou utilizar nenhuma informação adquirida do HEC ou relativa à solução instalada, sem a autorização prévia do HEC;
15.5.2. Respeitar a Confidencialidade da Informação e Propriedade Intelectual do HEC;
15.5.3. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do HEC ou de terceiros de que tomar conhecimento em razão da execução do objeto contratado, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros.

16. REGULARIDADE FISCAL, TRABALHISTA E QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

16.1 Prova de inscrição no Cadastro Nacional de Pessoa Jurídica – CNPJ.
16.2 Prova de regularidade fiscal perante a Fazenda Nacional, mediante certidão conjunta expedida pela RFB/PGFN, referente a todos os créditos tributários federais e à Dívida Ativa da União, inclusive aqueles relativos à Seguridade Social.
16.3 Prova de regularidade com a Fazenda Estadual (onde for sediada a empresa e a do Estado do Espírito Santo, quando a sede não for deste Estado).
16.4 Prova de regularidade com a Fazenda Pública Municipal da sede da licitante.
16.5 Prova de regularidade com o Fundo de Garantia por Tempo de Serviço – FGTS.
16.6 Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa.

16.7 Certidão Negativa de Falência, Recuperação Judicial e Extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, observada a data de validade definida no instrumento.

17. QUALIFICAÇÃO TÉCNICA DA EMPRESA

(x) APLICA

( ) NÃO SE APLICA

17.1 Atestados(s) de Capacidade Técnica emitido(s) por pessoas jurídicas de direito público ou privado, atestando que a empresa presta ou já prestou serviços de características semelhantes objeto deste termo, em especificações e que não possui nada que desabone a sua capacidade de prestação dos serviços.

17.1.1 O Atestado acima deverá constar os seguintes dados: nome do CONTRATANTE e da CONTRATADA, data de início e término dos serviços; local de execução; especificações técnicas dos serviços executados, assim como os volumes de procedimentos e informação sobre o bom desempenho dos serviços.

17.1.2 O atestado deverá ser apresentado em documento timbrado, contendo a assinatura do representante legal; o CNPJ, telefone de contato; e-mail e endereço da pessoa jurídica público ou privada, responsável pela sua emissão com respectiva data de emissão do documento.

17.1.3 Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

17.1.4 Será admitido, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de atestados de períodos diferentes e de forma concomitante, não havendo obrigatoriedade de os anos serem ininterruptos.

17.1.5 Os atestados apresentados, poderão ser diligenciados de acordo com a Lei Federal n° 14.133/21 e demais alterações posteriores.

18. GESTÃO E FISCALIZAÇÃO DO CONTRATO

18.1 A Fundação designará formalmente, em instrumento próprio, o(s) colaborador(es) responsável(is) pela gestão e fiscalização do serviço a ser contratado para acompanhamento do objeto deste Termo de Referência.

19. SANÇÕES ADMINISTRATIVAS

19.1 O não cumprimento total ou parcial das obrigações assumidas na forma e prazos estabelecidos sujeitará a Contratada às penalidades constantes na legislação em vigor, sempre assegurados os princípios do contraditório e da ampla defesa, que estarão descritas no instrumento contratual.

20. CONDIÇÕES GERAIS

20.1 Caso haja a descontinuidade da especialidade/serviço contratado na unidade hospitalar, a Fundação se reserva no direito de encerrar o contrato sem que incida qualquer tipo de penalidade para esta, devendo seguir as regras instituídas em contrato.

20.2 A ata de registro de Preço terá vigência de 12 meses, podendo ser encerrada por sua vigência ou suficiência de saldo, valendo o que ocorrer primeiro.

21. RESPONSÁVEIS PELO TERMO DE REFERÊNCIA

21.1 Este Termo de Referência foi elaborado por Luciano da Silva Nascimento da Coordenação de Tecnologia de informação e Karla Evangelista do Grupo Especial de TRs do Hospital Estadual Central de Vitória.

22. DA DECLARAÇÃO DE UTILIZAÇÃO DA MINUTA PADRONIZADA

22.1 Declaro(amos) que, para a elaboração deste Termo de Referência, foi utilizada a minuta padronizada do TR exclusivo para aquisição, extraída do site oficial da Fundação iNOVA Capixaba em 10/09/2024.

23. DA DECLARAÇÃO MATERIAL MÉDICO E MEDICAMENTO

( ) APLICA

23.1 Declaro(amos) que foram observados os requisitos legais aplicáveis à compra de medicamento e material médico (leis, decretos, portarias, resoluções) e o objeto foi descrito de forma CLARA e PRECISA, utilizando-se a Denominação Comum Brasileira (DCB) ou, na sua falta, a Denominação Comum Internacional (DCI)

(x) NÃO SE APLICA

(Assinado Eletronicamente)
Luciano da Silva Nascimento
Coordenação de Tecnologia de Informação
Hospital Estadual Central de Vitória

ANEXO III – ARP Nº 109/2024

MINUTA DE TERMO DE CONTRATO

CONTRATO Nº ___/2024
PROCESSO Nº _____
PREGÃO Nº ____/2024
ID CidadES Nº _____

TERMO DE CONTRATO QUE ENTRE SI CELEBRAM A FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE - iNOVA CAPIXABA E A EMPRESA _____, PARA A _____.

A **FUNDAÇÃO ESTADUAL DE INOVAÇÃO EM SAÚDE – INOVA CAPIXABA**, adiante denominada **CONTRATANTE**, Fundação Pública com Personalidade Jurídica de Direito Privado, inscrita no CNPJ sob o nº 36.901.264/0001-63, com sede na Rua Pernambuco, n°1.100, Edifício Estilo Center, 3°Andar, Bairro Praia da Costa, Vila Velha/ES CEP: 29.101-284, representada legalmente pelo seu _____, Sr. _____, e por seu _____, Sr. _____, e a Empresa _____, doravante denominada **CONTRATADA**, com sede à _____, inscrita no CNPJ sob o nº _____, neste ato representada por seu _____, Sr. _____[1] e, em observância às disposições contidas na Lei nº 14.133/2021, resolvem celebrar o presente Termo de Contrato, mediante as cláusulas e condições a seguir enunciadas.

1 – CLÁUSULA PRIMEIRA: DO OBJETO (art. 92, I e II)

1.1 – O objeto deste instrumento é a _____, nas condições estabelecidas no Termo de Referência.

1.2 – Descrição do objeto:

ITEM	CÓDIGO	DESCRIÇÃO DO OBJETO	MARCA/MODELO	UND	QTD	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)

VALOR TOTAL PARA GRUPO/LOTE	

1.3 – Integram este instrumento, como partes indissociáveis e independentemente de transcrição, os seguintes anexos:

(a) o Edital e todos os seus Anexos;

[1] Os dados do representante da contratada estão registrados no formulário 'DADOS COMPLEMENTARES PARA ASSINATURA DO INSTRUMENTO CONTRATUAL', o qual foi classificado como sigiloso no E-docs, em conformidade com as disposições da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), para cumprir as normas de privacidade estabelecidas

(b) o Edital e todos os seus Anexos;

(c) o Questionário de Integridade (https://forms.gle/cFTJ687GMSUceqHQ9)

2 – CLÁUSULA SEGUNDA: DOS CASOS OMISSOS (art. 92, III)

2.1 – Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 14.133/2021 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078/1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

3 – CLÁUSULA TERCEIRA: DO REGIME DE EXECUÇÃO E DA GESTÃO CONTRATUAL (art. 92, IV e XVIII)

3.1 – Fica estabelecido o regime de execução indireta, sob a modalidade empreitada por preço unitário, nos termos do art. 6º, XXVIII, da Lei nº 14.133/2021.

3.2 – O modelo de gestão contratual consta no Termo de Referência, anexo a este Contrato.

4 – CLÁUSULA QUARTA: DA VIGÊNCIA E DA PRORROGAÇÃO (art. 92, VII)

4.1 – O prazo de vigência da contratação é de _____ (preencher), e terá início no dia da publicação do respectivo instrumento no Diário Oficial ou site da Fundação – quando for o caso, sendo finalizado com a entrega, recebimento e pagamento, na forma do artigo 105 da Lei n° 14.133/2021.

4.2 – A gestão do contrato, inclusive quanto à prorrogação, deve observar o que o disposto no art. 22, do Decreto Estadual nº 5.545-R/2023 e em orientações complementares;

4.3 – Aplica-se a este Contrato a hipótese de extinção prevista no art. 106, III, da Lei Federal nº 14.133/2021, mediante justificativa da medida excepcional e prévia oitiva da Assessoria Jurídica da Fundação.

5 – CLÁUSULA QUINTA: DO PREÇO (art. 92, V)

5.1 – Pelas aquisições recebidas, a Contratada receberá o valor unitário de R$ _____ (_____), e nele deverão estar inclusos todas as espécies de tributos, diretos e indiretos, encargos sociais e quaisquer despesas inerentes à execução do objeto contratual;

5.2 – No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação;

5.3 – O valor acima é meramente estimativo, de forma que os pagamentos devidos a Contratada dependerão dos quantitativos efetivamente fornecidos.

5.4 – Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data da apresentação da proposta, em __/__/____ (preencher).

5.5 – O reajuste do preço contratado levará em consideração o Índice Nacional de Preços ao Consumidor – INPC, divulgado pelo Instituto Brasileiro de Geografia e Estatística – IBGE, ou outro índice que vier a substituí-lo.

5.6 – O reequilíbrio econômico e financeiro, em qualquer de suas espécies, em especial o reajuste e a repactuação, observará, conforme a natureza do objeto contratual, as regras previstas nos arts. 45 a 53 do Decreto Estadual nº 5545-R/2023 e na Lei Federal nº 14.133/2021, inclusive quanto à renúncia irretratável por ausência de requerimento formal durante a vigência do contrato e antes de eventual prorrogação (art. 46 do Decreto).

5.7 – Após o interregno de um ano, mediante pedido do contratado, os preços iniciais poderão ser reajustados, mediante a aplicação, pelo contratante, do índice INPC – IBGE (Índice Nacional de Preços ao Consumidor), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, com base na seguinte fórmula.

5.8 – Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

5.9 – No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

5.10 – Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

5.11 – Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor. Na ausência de previsão legal quanto ao índice substituto, será adotado o novo índice definido para a Administração Estadual na contratação de serviços semelhantes.

5.12 – O reajuste de preços será formalizada por apostilamento.

5.13 – Os reajustes não interferem no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico dos contratos com base no disposto no art. 124, inciso II, alínea “d”, da Lei nº 14.133, de 2021.

5.14 – O contratado deverá complementar a garantia contratual anteriormente prestada, de modo que se mantenha a proporção inicial em relação ao valor contratado.

6 – CLÁUSULA SEXTA: DAS CONDIÇÕES DE PAGAMENTO (art. 92, V)

6.1 – A Contratante pagará à Contratada pelas aquisições recebidas, efetivamente entregues no mês de referência, conforme medição, vedada a antecipação, nos moldes do Termo de Referência;

6.2 – A CONTRATADA deverá apresentar a nota fiscal à CONTRATANTE até o 5º (quinto) dia útil subsequente da prestação do serviço, devidamente aceita pela CONTRATANTE;

6.3 – O pagamento far-se-á por meio de uma única transferência bancária e será realizado até 30 (trinta) dias após a apresentação da Nota Fiscal.

6.4 – Os pagamentos serão sempre realizados por meio de transferência bancária, devendo a Contratada informar o domicílio bancário na Nota Fiscal;

6.5 – Os pagamentos ficam condicionados ainda à apresentação das certidões de regularidade fiscal e trabalhista, junto com as Notas Fiscais.

6.6 – Decorrido o prazo indicado no item anterior, incidirá multa financeira nos seguintes termos:

6.7 – Incumbirá à Contratada a iniciativa e o encargo do cálculo minucioso da nota fiscal devida, a ser revisto e aprovado pela Contratante, juntando-se à respectiva discriminação dos serviços efetuados, o memorial de cálculo;

6.8 – Se houver alguma incorreção na Nota Fiscal, ou circunstância que impeça a liquidação da despesa, a NF será devolvida à Contratada para correção, ficando estabelecido que o prazo para pagamento será contado a partir da data de apresentação na nova Nota Fiscal, sem qualquer ônus ou correção a ser paga pela Contratante;

6.8.1 – Neste caso, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras e o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o contratante.

6.9 – Cabe à Contratada, quando for o caso, manter-se regular perante os órgãos de controle e registro de sua atividade, na forma da Portaria SAS nº 511/2000, sob pena de sobrestar, sem culpa da Contratante, a realização dos pagamentos;

6.10 – Quando houver glosa parcial do objeto, a Contratante deverá comunicar a empresa para que emita a nota fiscal ou fatura com o valor exato dimensionado;

6.11 – A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68, da Lei nº 14.133/2021;

6.12 – A Contratante deverá realizar consulta ao SICAF para:

6.12.1 – Verificar a manutenção das condições de habilitação exigidas no edital;

6.12.2 – Identificar possível razão que impeça a participação em licitação proibição de contratar bem como ocorrências impeditivas indiretas;

6.13 – Nos termos do Decreto Estadual nº 5.460-R/2023 e da Instrução Normativa RFB nº 1.234/2012 ou a que vier a substituí-la, a Contratante deverá proceder a retenção do Imposto de Renda (IR) na Fonte ao efetuar qualquer pagamento à pessoa jurídica pelo fornecimento de bens ou prestação de serviços;

6.13.1 – A Contratada deverá emitir a(s) nota(s) fiscal(is), fatura(s) ou qualquer(quaisquer) outro(s) documento(s) de cobrança com o destaque do IR na Fonte;

6.13.2 – Excetuam-se se dessa obrigação as hipóteses elencadas no art. 4º da IN RFB nº 1.234/2012, devendo a Contratada apresentar, em conjunto com os demais documentos de cobrança, declaração do respectivo enquadramento, na forma dos anexos da referida Instrução Normativa.

7 – CLÁUSULA SÉTIMA: DA ENTREGA E DO RECEBIMENTO DO OBJETO

7.1 – O objeto do contrato será recebido na forma prevista do item 5. Entrega e Recebimento, do Anexo I - Termo de Referência.

8 – CLÁUSULA OITAVA: DA DOTAÇÃO ORÇAMENTÁRIA (art. 92, VIII)

8.1 – Os recursos necessários ao pagamento das despesas inerentes a este Contrato correrão do orçamento da Fundação iNOVA Capixaba Matriz e Filiais para o exercício de 2024.

9 – CLÁUSULA NONA: DA GARANTIA DO PRODUTO E ASSISTÊNCIA TÉCNICA

9.1 – O prazo e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato;

10 – CLÁUSULA DÉCIMA: DAS INFRAÇÕES E DAS SANÇÕES ADMINISTRATIVAS (art. 92, XIV)

10.1 – Comete infração administrativa, nos termos da Lei nº 14.133/2021, a Contratada que:

10.1.1 – Der causa à inexecução parcial do contrato;

10.1.2 – Der causa à inexecução parcial do contrato que cause grave dano à Fundação ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

10.1.3 – Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

10.1.4 – Apresentar declaração ou documentação falsa durante a execução do contrato;

10.1.5 – Fraudar a contratação ou praticar ato fraudulento na execução do contrato;

10.1.6 – Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

10.1.7 – Praticar atos ilícitos com vistas a frustrar os objetivos da contratação;

10.1.8 – Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

10.2 – O atraso injustificado na execução do contrato sujeitará a contratada à aplicação de multa de mora, nas seguintes condições:

10.2.1 – Fixa-se a multa de mora em 0,5 % (cinco décimos por cento) por dia de atraso, a incidir sobre o valor total reajustado do contrato, ou sobre o saldo reajustado não atendido, caso o contrato encontre-se parcialmente executado;

10.2.2 – Os dias de atraso serão contabilizados em conformidade com o cronograma de execução do contrato;

10.2.3 – A aplicação da multa de mora não impede que a Fundação rescinda unilateralmente o contrato e aplique as outras sanções previstas no contrato e na Lei nº 14.133/2021.

10.3 – Serão aplicadas a Contratada que incorrer em qualquer das infrações administrativas previstas acima, bem como com a inexecução total ou parcial do contrato, ensejará na aplicação das seguintes sanções:

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

10.3.2 – Multa compensatória: por perdas e danos, no montante de até 10% (dez por cento) sobre o saldo contratual reajustado não executado pelo particular;

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

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

10.4 – A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Contratante (art. 156, §9º, da Lei nº 14.133/2021);

10.5 – Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133/2021);

10.5.1 – Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133/2021);

10.5.2 – Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante a Contratada, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133/2021);

10.5.3 – Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

10.6 – A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa a Contratada, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar;

10.7 – Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133/2021):

(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 o Contratante;

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

10.8 – Os atos previstos como infrações administrativas na Lei nº 14.133/2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846/2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159, da Lei nº 14.133/2021);

10.9 – A personalidade jurídica da Contratada poderá ser desconsiderada sempre que 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 a Contratada, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133/2021);

10.10 – O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de 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. (Art. 161, da Lei nº 14.133/2021);

10.11 – 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 nº 14.133/2021.

11 – CLÁUSULA DÉCIMA PRIMEIRA: DA EXTINÇÃO E DO ADITAMENTO (art. 92, XIX)

11.1 – A extinção do Contrato poderá ocorrer nas hipóteses e condições previstas nos arts. 137, 138 e 139, da Lei nº 14.133/2021, no que couber;

11.2 – O presente contrato poderá ser aditado, estritamente, nos termos previstos na Lei nº 14.133/2021, após manifestação formal da Assessoria Jurídica da Fundação.

12 – CLÁUSULA DÉCIMA SEGUNDA: DO RECURSO (art. 165, I e II)

12.1 – Os recursos, representação e pedido de reconsideração, somente serão acolhidos nos termos do art. 165 e seguintes, da Lei nº 14.133/2021.

13 – CLÁUSULA DÉCIMA TERCEIRA: DAS OBRIGAÇÕES E DAS RESPONSABILIDADES DAS PARTES (art. 92, XIV, XVI e XVII)

13.1 – COMPETE À CONTRATADA:

13.1.1 – A Contratada se obriga a manter, durante toda a execução do CONTRATO, todas as condições de habilitação e qualificação exigidas no Termo de Referência e seus anexos, bem como apresentar as respectivas certidões negativas de débito junto com os documentos de cobrança;

13.1.2 – Manter a regularidade no Sistema de Cadastro de Fornecedores – SICAF e, quando não for possível a verificação da regularidade pelo SICAF, a Contratada deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, 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 Municipal ou Distrital do domicílio ou sede da Contratada; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

13.1.3 – Executar o objeto deste contrato rigorosamente no prazo pactuado, bem como cumprir todas as demais obrigações impostas pelo Termo de Referência e seus anexos;

13.1.4 – A Contratada deve cumprir todas as obrigações constantes deste Contrato, em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

13.1.5 – Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, inc. II, da Lei nº 14.133/2021) e prestar todo e qualquer esclarecimento ou informação solicitada pelo fiscal ou gestor do contrato;

13.1.6 – Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Fundação ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

13.1.7 – Promover por sua conta a cobertura através de seguros, dos riscos a que se julgar exposta em vista das responsabilidades que lhe cabem na execução deste contrato, devendo reparar e indenizar danos de qualquer natureza causados a Fundação ou a terceiros, provenientes da ação ou omissão sua ou de seus prepostos, na execução do objeto contratado ou dele decorrente;

13.1.8 – Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

13.1.9 – Indenizar em qualquer caso, todos os danos e prejuízos, de qualquer natureza, que causar à Fundação ou a terceiros, decorrentes de sua culpa ou dolo, na execução deste contrato, respondendo por si e por seus sucessores;

13.1.10 – Contratar por sua conta todos os seguros exigidos ou que venham a ser exigidos por lei e que incidam direta ou indiretamente sobre o objeto deste termo;

13.1.11 – A empresa deverá registrar as ocorrências havidas durante a execução deste contrato, de tudo dando ciência ao colaborador ou a comissão responsável pelo acompanhamento e fiscalização do contrato, respondendo integralmente por sua omissão;

13.1.12 – A Contratada deve fornecer, quando for o caso, os equipamentos de segurança e proteção exigidos pela legislação vigente para a execução de serviços profissionais que a função exija por norma;

13.1.13 – Observar e cumprir as Normas de Segurança e Medicina do Trabalho;

13.1.14 – Observar e cumprir as normas e os regulamentos internos da Contratante;

13.1.15 – Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

13.1.16 – Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina;

13.1.17 – Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

13.1.18 – Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante;

13.1.19 – Aceitar os acréscimos ou supressões do objeto desta contratação, nos termos do art. 125, da Lei nº 14.133/2021;

13.1.20 – É vedada a subcontratação, cessão ou transferência parcial ou total do objeto contratado;

13.1.21 – Cumprir com as demais obrigações constantes do Anexo I - Termo de Referência.

13.2 – COMPETE À CONTRATANTE:

13.2.1 – Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com o contrato e seus anexos;

13.2.2 – Efetuar o pagamento do preço previsto nos termos deste contrato;

13.2.3 – Designar colaborador(es) responsável(is) pelo acompanhamento e fiscalização da execução dos serviços;

13.2.4 – Cumprir com as demais obrigações constantes do Anexo I - Termo de Referência.

14 – CLÁUSULA DÉCIMA QUARTA: DA SUPERVENIENTE IRREGULARIDADE FISCAL OU TRABALHISTA

14.1 – Constatado que a Contratada não se encontra em situação de regularidade fiscal ou trabalhista, o mesmo será notificado para no prazo de 10 (dez) dias úteis regularizar tal situação ou, no mesmo prazo, apresentar defesa, observando-se o procedimento de aplicação de sanções;

14.2 – Transcorrido esse prazo, ainda que não comprovada a regularidade e que não seja aceita a defesa apresentada, o pagamento será efetuado, sem prejuízo da tramitação do procedimento de aplicação de sanções;

14.3 – Em não sendo aceitas as justificativas apresentadas pela Contratada, será imposta multa de 2% (dois por cento) sobre o saldo contratual não executado;

14.4 – Depois de transcorridos 30 (trinta) dias úteis da notificação da multa, se a empresa não regularizar a pendência fiscal ou trabalhista, deverá a Entidade decidir sobre iniciar ou não procedimento de rescisão do contrato, podendo deixar de fazê-lo se reputar que a extinção antecipada do contrato ocasionará expressivos prejuízos ao interesse público.

15 – CLÁUSULA DÉCIMA QUINTA: DA POLÍTICA DE INTEGRIDADE E ANTICORRUPÇÃO

15.1 – A Contratada compromete-se a preencher "Questionário de Integridade" elaborado pela Contratante, em que atestará sua idoneidade, bem como se tem instrumentos internos que respeitam os ditames da legislação anticorrupção, conforme disponibilizado no sítio da Fundação, acesso pelo link: https://inovacapixaba.es.gov.br/Media/InovaCapixaba/Governan%C3%A7a%20Corporativa/Pol%C3%ADtica%20de%20Integridade%20iNOVA%20Capixaba.pdf;

15.2 – A Contratada concorda que será responsável perante a Contratante por qualquer violação à legislação anticorrupção aplicável que venha a ser cometida por seus sócios,

administradores, diretores, gerentes ou empregados com relação a atividades direta ou indiretamente relacionadas à Contratante;

15.3 – A Contratada se obriga a notificar prontamente, por escrito, à Contratante a respeito de qualquer suspeita ou violação do disposto nas leis anticorrupção e/ou do disposto nesta CLÁUSULA, e ainda de participação em práticas de suborno ou corrupção, assim como o descumprimento de quaisquer declarações previstas no contrato;

15.4 – O não cumprimento pela Contratada das leis anticorrupção e/ou do disposto nesta CLÁUSULA será considerado uma infração grave ao CONTRATO e conferirá à Contratante o direito de, agindo de boa-fé, declarar rescindido imediatamente o CONTRATO, sem qualquer ônus ou penalidade, sendo a Contratada responsável por eventuais perdas e danos;

15.5 – A Contrata declara que tem pleno conhecimento do teor do Código de Ética, Conduta e Integridade da Fundação Estadual de Inovação em Saúde – iNOVA Capixaba, nos termos do disposto na Resolução CC/iNOVA nº 005/2021, conforme disponibilizado no sítio da fundação, acesso pelo link: https://inovacapixaba.es.gov.br/Media/InovaCapixaba/Governan%C3%A7a%20Corporativa/C%C3%B3digo%20de%20%C3%89tica,%20Conduta%20e%20Integridade%20iNOVA%20Capixaba-.pdf.

16 – CLÁUSULA DÉCIMA SEXTA: DO DIREITO DE IMAGEM E DO TRATAMENTO DE DADOS PESSOAIS

16.1 – Fica autorizado o uso da imagem dos prestadores de serviços que executam o objeto deste contrato, pela Fundação e suas unidades, em virtude das atividades inerentes ao contrato, para serem veiculadas aos públicos interno e geral, respeitando-se sempre a moral e a honra dos mesmos;

16.2 – A autorização referida no item anterior, é concedida a título gratuito, abrangendo o uso da imagem, áudio e qualquer outra mídia que tenha sido produzida na execução deste contrato em todo território nacional e no exterior;

16.3 – Autoriza-se a utilização dos dados pessoais dos prestadores de serviços para que seja tratada pela Fundação, ou por empresa por ela contratada, nos termos da Lei nº 13.709/2018 (LGPD – Lei Geral de Proteção de Dados), conforme as finalidades descritas neste contrato, nos termos do artigo 7º, incisos I e V, da referida norma, sem a necessidade de qualquer outra autorização e/ou aviso prévios;

16.4 – A autorização do uso de imagem e de dados pessoais relativa a este contrato terá validade de 5 (cinco) anos datados da relação contratual entre as partes.

17 – CLÁUSULA DÉCIMA SÉTIMA: DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

17.1 – A Fundação designará formalmente o colaborador responsável pelo acompanhamento e fiscalização da execução do contrato, competindo-lhe atestar a realização do serviço contratado, observando as disposições deste Contrato e do art. 117, da Lei 14.133/2021.

18 – CLÁUSULA DÉCIMA OITAVA: DO FORO (art. 92, §1º)

18.1 – Fica estabelecido o Foro de Vila Velha, munícipio do Estado do Espírito Santo, para dirimir quaisquer dúvidas oriundas direta ou indiretamente deste instrumento, renunciando-se expressamente a qualquer outro, por mais privilegiado que seja.

E assim, por estarem justos e acordados, assinam o presente Contrato para que produza seus efeitos legais.

_____

Fundação iNOVA Capixaba
CONTRATANTE

_____

Fundação iNOVA Capixaba
CONTRATANTE

_____

CONTRATADA

Rua Pernambuco, nº 1.100,
Edifício Estilo Center, 3º andar
- Praia da Costa-Vila Velha/ES-
CEP 29.101-284
Tel: (27) 3636-3584

ANEXO IV – ARP Nº 109/2024

PROPOSTA COMERCIAL

PREGÃO INOVA CAPIXABA ELETRÔNICO Nº 056/2024
APRESENTAÇÃO DA PROPOSTA DE PREÇOS

OBJETO: REGISTRO DE PREÇOS PARA AQUISIÇÃO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION) ATRAVÉS DO PROJETO DE INVESTIMENTO, VISANDO ATENDER AS NECESSIDADES DO SETOR DE TECNOLOGIA DA INFORMAÇÃO DO HOSPITAL ESTADUAL CENTRAL- DR. BENÍCIO TAVARES PEREIRA, conforme especificações do Anexo I do presente Edital.

Empresa: Altas Networks e Telecom Ltda
CNPJ: 05.407.609/0003-65
Endereço: Av. Olegário Maciel, 1217, sala 402, Bairro de Lourdes – Belo Horizonte – MG – CEP 30.180-111
Emails: comercial@altasnet.com.br e almir@altasnet.com.br
Tel/Fax: (31) 3449-4500 - Celular: (31) 99944-2640

QUADRO RESUMO DA PROPOSTA DE PREÇOS

Lote	Descrição do item	Valor Global da Proposta
1	FIREWALL NGFW COM LICENCA/GARANTIA DE 36 (TRINTA E SEIS) MESES DE APPLICATION CONTROL, IPS, AMP, WEB FILTERING, ANTISPAM, SOLUCAO DE LOGS, ANÁLISE E RELATÓRIOS	**R$ 142.000,00**

Documento original assinado eletronicamente, conforme MP 2200-2/2001, art. 10, § 2º, por:

LEONARDO CEZAR TAVARES
DIRETOR DE OPERAÇÕES, LOGÍSTICA, T.I.C., INFRAESTRUTURA E MANUTENÇÃO
DIROP - INOVA - GOVES
assinado em 12/11/2024 08:43:08 -03:00

JORGE TEIXEIRA E SILVA NETO
DIRETOR DE GENTE, GESTÃO, FINANÇAS E COMPRAS
DIRGF - INOVA - GOVES
assinado em 11/11/2024 16:40:22 -03:00

ALMIR FRANZ DE LIMA
CIDADÃO
assinado em 11/11/2024 13:19:10 -03:00

INFORMAÇÕES DO DOCUMENTO
Documento capturado em 12/11/2024 08:43:08 (HORÁRIO DE BRASÍLIA - UTC-3)
por ROZILENE RIBEIRO FERREIRA DE ABREU (ASSISTENTE ADMINISTRATIVO - CCOMP - INOVA - GOVES)
Valor Legal: ORIGINAL | Natureza: DOCUMENTO NATO-DIGITAL

A disponibilidade do documento pode ser conferida pelo link: https://e-docs.es.gov.br/d/2024-367L94