MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA SUL-RIO-GRANDENSE

E D I T A L

PREGÃO ELETRÔNICO Nº 20/2024
REGISTRO DE PREÇOS
(Processo Administrativo n°23163.003085.2024-04)

Torna-se público que o(a) INSTITUTO FEDERAL DE EDUCACAO, CIENCIA E TECNOLOGIA SULRIOGRANDENSE, CNPJ/MF no 10.729.992/0001-46, por meio da Coordenadoria de Licitações, sediada na Rua Gonçalves Chaves nº 3218, Centro, Pelotas/RS, realizará licitação, para registro de preços, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, do Decreto nº 11.462, de 31 de março de 2023, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. Aquisição de solução de segurança TIC , a ser utilizada nas 15 (quinze) unidades do instituto Federal Sul-rio-grandense, quantidades e exigências estabelecidas neste Edital e seus anexos

1.2. A licitação será dividida em itens, conforme tabela constante do Termo de Referência, facultando-se ao licitante a participação em quantos itens forem de seu interesse.

2. Do registro de preços

2. DO REGISTRO DE PREÇOS

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

3. Da participação na licitação

3. DA PARTICIPAÇÃO NA LICITAÇÃO

3.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

3.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

3.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

3.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

3.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

3.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015, bem como para bens e serviços produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010.

3.6. Não poderão disputar esta licitação:

3.6.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

3.6.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

3.6.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

3.6.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

3.6.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

3.6.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

3.6.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

3.6.8. agente público do órgão ou entidade licitante;

3.6.9. pessoas jurídicas reunidas em consórcio;

3.6.10. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

3.6.11. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

3.7. O impedimento de que trata o item 3.6.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

3.8. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa aque se referem os itens 3.6.2 e 3.6.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

3.9. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

3.10. O disposto nos itens 3.6.2 e 3.6.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

3.11. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

3.12. A vedação de que trata o item 3.6.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

4. Da apresentação da proposta e dos documentos de habilitação

4. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

4.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

4.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

4.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 8.1.1 e 8.13.1 deste Edital.

4.4. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

4.4.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

4.4.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

4.4.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

4.4.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

4.5. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

4.6. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

4.6.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

4.6.2.nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

4.7. A falsidade da declaração de que trata os itens 4.4 ou 4.6 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

4.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

4.9. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

4.10. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

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

4.11.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

4.11.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

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

4.12.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço;

4.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 4.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

4.14. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

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

5. Do preenchimento da proposta

5. DO PREENCHIMENTO DA PROPOSTA

5.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

5.1.1. valor unitário e total do item;

5.1.2. descrição do objeto, contendo as informações similares à especificação do Termo de Referência

5.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

5.2.1. O licitante NÃO poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.

5.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

5.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

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

5.5.1. O prazo de validade da proposta não será inferior a **60 (sessenta)** dias**,** a contar da data de sua apresentação.

5.5.2. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

5.5.3. Caso o critério de julgamento seja o de maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos previstos no item 4.9.

5.6. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

6. Da abertura da sessão, classificação das propostas e formulação de lances

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

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

6.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

6.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

6.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

6.5. O lance deverá ser ofertado pelo valor unitário do item.

6.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

6.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

6.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 0,5% (meio por cento).

6.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

6.10. O procedimento seguirá de acordo com o modo de disputa adotado.

6.11. Será adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, no qual os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

6.11.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de tempo de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

6.11.2. Encerrado o prazo previsto no item anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até dez por cento superior àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

6.11.3. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará os lances segundo a ordem crescente de valores.

6.11.4 Não havendo lance final e fechado classificado na forma estabelecida nos itens anteriores, haverá o reinício da etapa fechada, para que os demais licitantes, até o máximo de três, na ordem de classificação, possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo

6.11.5. Poderá o pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada, caso nenhum licitante classificado na etapa de lance fechado atender às exigências de habilitação.

6.12. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

6.12.1 Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante

6.12.2.No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

6.12.3. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

6.12.4. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

6.12.5. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno

porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

6.13. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

6.13.1. A mais bem classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

6.13.2. Caso a microempresa ou a empresa de pequeno porte mais bem classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

6.13.3. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

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

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

6.13.6. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

6.13.7. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

6.13.8. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

6.13.9. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

6.14. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

6.14.1. empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

6.14.2. empresas brasileiras;

6.14.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

6.14.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

6.15. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

6.15.1. negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

6.15.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

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

6.15.4. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de no mínimo **2 (duas) horas, prorrogável**, contado da solicitação do pregoeiro, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

6.15.5. É facultado ao pregoeiro prorrogar o prazo estabelecido, a seu critério ou a partir de solicitação feita pelo licitante, antes de findo o prazo.

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

7. Da fase de julgamento

7. DA FASE DE JULGAMENTO

7.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 3.8 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

7.1.1. SICAF;

7.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria Geral da União (https://www.portaltransparencia.gov.br/sanções/ceis); e

7.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sanções/cnep).

7.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

7.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, *caput*)

7.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

7.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

7.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

7.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

7.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com o edital.

7.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

7.7. Será desclassificada a proposta vencedora que:

7.7.1. contiver vícios insanáveis;

7.7.2. não obedecer às especificações técnicas contidas no Termo de Referência;

7.7.3.apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

7.7.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

7.7.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

7.8. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

7.8.1. A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

7.8.1.1. que o custo do licitante ultrapassa o valor da proposta; e

7.8.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

7.9. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

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

8. Da fase de habilitação

8. DA FASE DE HABILITAÇÃO

8.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

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

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

8.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fim de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

8.4. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

8.5. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

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

8.7. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

8.8. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

8.9. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

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

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

8.12. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

8.13. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de **NO MÍNIMO, DUAS HORAS,** prorrogável, contado da solicitação do pregoeiro.

8.14. Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto no § 1º do art. 36 e no § 1º do art. 39 da *Instrução Normativa SEGES nº 73, de 30 de setembro de 2022*.

8.15. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

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

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

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

8.16.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

8.16.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

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

8.18. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 8.13.1.

8.19. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

8.20. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

8.21. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

9. Da ata de registro de preços

9. DA ATA DE REGISTRO DE PREÇOS

9.1. Homologado o resultado da licitação, o licitante mais bem classificado terá o prazo de 5 (cinco) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

9.2. O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação do licitante mais bem classificado ou do fornecedor convocado, desde que:

9.2.1. a solicitação seja devidamente justificada e apresentada dentro do prazo; e

9.2.2. a justificativa apresentada seja aceita pela Administração.

9.3. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no sistema de registro de preços.

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

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

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

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

10. Da formação do cadastro de reserva

10. DA FORMAÇÃO DO CADASTRO DE RESERVA

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

10.1.1. dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação; e

10.1.2. dos licitantes que mantiverem sua proposta original.

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

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

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

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

10.3.1. quando o licitante vencedor não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital; ou

10.3.2.quando houver o cancelamento do registro do fornecedor ou do registro de preços, nas hipóteses previstas nos art. 28 e art. 29 do Decreto nº 11.462/23.

10.4. Na hipótese de nenhum dos licitantes que aceitaram cotar o objeto com preço igual ao do adjudicatário concordar com a contratação nos termos em igual prazo e nas condições propostas pelo primeiro classificado, a Administração, observados o valor estimado e a sua eventual atualização na forma prevista no edital, poderá:

10.4.1. convocar os licitantes que mantiveram sua proposta original para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

10.4.2. adjudicar e firmar o contrato nas condições ofertadas pelos licitantes remanescentes, observada a ordem de classificação, quando frustrada a negociação de melhor condição.

11. Dos recursos

11. DOS RECURSOS

11.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

11.2.O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

11.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

11.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

11.3.1.1. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

11.3.1.2. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

11.3.1.3. na hipótese de adoção da inversão de fases prevista no § 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

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

11.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

11.6. Os recursos interpostos fora do prazo não serão conhecidos.

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

11.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

11.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

12. Das infrações administrativas e sanções

12. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

12.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

12.1.1.deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

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

12.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

12.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

12.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

12.1.2.4. deixar de apresentar amostra;

12.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

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

12.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

12.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

12.1.5. fraudar a licitação;

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

12.1.6.1. agir em conluio ou em desconformidade com a lei;

12.1.6.2. induzir deliberadamente a erro no julgamento;

12.1.6.3. apresentar amostra falsificada ou deteriorada;

12.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

12.1.8. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

12.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

12.2.1. advertência;

12.2.2. multa;

12.2.3. Impedimento de licitar e contratar e

12.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

12.3. Na aplicação das sanções serão considerados:

12.3.1. a natureza e a gravidade da infração cometida.

12.3.2.as peculiaridades do caso concreto

12.3.3. as circunstâncias agravantes ou atenuantes

12.3.4. os danos que dela provierem para a Administração Pública

12.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de **10 (dez) dias** úteis, a contar da comunicação oficial.

12.4.1. Para as infrações previstas nos itens 12.1.1, 12.1.2 e 12.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.

12.4.2. Para as infrações previstas nos itens 12.1.4, 12.1.5, 12.1.6, 12.1.7 e 12.1.8, a multa será de 15% a 30% do valor do contrato licitado.

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

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

12.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 12.1.1, 12.1.2 e 12.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

12.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 12.1.4, 12.1.5, 12.1.6, 12.1.7 e 12.1.8, bem como pelas infrações administrativas previstas nos itens 12.1.1, 12.1.2 e 12.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

12.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 12.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

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

12.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

12.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

12.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

12.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

13. Da impugnação do edital e do pedido de esclarecimento

13. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

13.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

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

13.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, por meio do e-mail: if-colicit@ifsul.edu.br

13.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

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

13.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

14. Das disposições gerais

14. DAS DISPOSIÇÕES GERAIS

14.1. Será divulgada ata da sessão pública no sistema eletrônico.

14.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

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

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

14.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

14.6. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

14.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

14.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

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

14.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico em www.ifsul.edu.br/2024.

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

14.12. ANEXO I - Termo de Referência

14.12.1.1 Apêndice do Anexo I – Estudo Técnico Preliminar

14.2.2.ANEXO II – Modelo de proposta de preços;

14.2.3. ANEXO III – Minuta de Ata de Registro de Preços

..... , ... de ..... de 2024

15. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

ERNESTO MONTEIRO PEREZ

Autoridade competente

ANEXO I

TERMO DE REFERÊNCIA COMPRAS DE TIC – LEI 14.133/2021

Processo Administrativo n°23163.002283.2024-42

Referência: Arts. 12 a 24 da Instrução Normativa SGD/ME nº 94, de 2022

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1 - Aquisição de *solução* de segurança a ser utilizada nas 15 unidades do Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense conforme condições, quantidades, exigências e estimativas, estabelecidas nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	CATMAT	DESCRIÇÃO	QTD	Valor Uni.	Valor Total
1	484747	FIREWALL DE BORDA TIPO 1 COM LICENCIAMENTO PARA 36 MESES (Hardware e Licenciamento)	2	R$ 748.963,74	R$ 1.497.927,48
2	484747	FIREWALL DE BORDA TIPO 2 COM LICENCIAMENTO PARA 36 MESES (Hardware e Licenciamento)	2	R$ 458.964,64	R$ 917.929,28
3	484747	FIREWALL DE BORDA TIPO 3 COM LICENCIAMENTO PARA 36 MESES (Hardware e Licenciamento)	10	R$ 323.994,30	R$ 3.239.943,00
4	484747	FIREWALL DE BORDA TIPO 4 COM LICENCIAMENTO PARA 36 MESES (Hardware e Licenciamento)	14	R$ 81.614,91	R$ 1.142.608,74
5	27472	SOFTWARE DE GESTÃO CENTRALIZADA PARA NGFW COM SUPORTE/GARANTIA DE 3 ANOS	1	R$ 87.769,82	R$ 87.769,82
6	27472	SOFTWARE DE RELATORIA/LOGS CENTRALIZADA PARA NGFW COM SUPORTE/GARANTIA DE 3 ANOS	4	R$ 114.125,15	R$ 456.500,60
7	27014	BANCO DE HORAS – SUPORTE TÉCNICO (HORAS)	180	R$ 415,71	R$ 74.827,98

1.2 -Cada item do objeto da contratação deverá ser do mesmo padrão tecnológico para melhor atendimento às necessidades da administração bem como entregue o mesmo modelo/marca a todas as unidades participantes deste processo a fim de garantir a manutenção, implantação e padronização pela área de Tecnologia da Informação do IFSUL. Deste modo não será definido cota reservada para microempresas e empresas de pequeno porte. A decisão justifica-se com base no Art.
49, inciso III da Lei Complementar 123/2016 e do § 4o, Art. 8º do Decreto 8538/2015.

1.3. As especificações técnicas e exigências em cada item estão descritas no **Apêndice anexo** deste Termo de Referência.

1.4. O órgão gerenciador é o Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense - Reitoria.

1.5. Estimativas de consumo individualizadas, do órgão*:*

	ITEM 1	ITEM 2	ITEM 3	ITEM 4	ITEM 5	ITEM 6	ITEM 7
Reitoria	2				4	1	180
Passo Fundo			2				
Santa na do Livramento			2				
Sapiranga				2			
Sapucaia				2			
Camaquã			2				
Gravataí				2			
Pelotas		2					
Pelotas - CAVG				2			
Venancio Aires			2				
Bagé				2			
Charqueadas			2				
Lajeado				2			
Jaguarão				2			

2. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

2.1 Nos termos do parágrafo único, do art. 1o, da Lei 10.520, de 2002, os objetos descritos são de natureza comum.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

3.1 A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares e apêndice deste Termo de Referência.

3.2 A solução de TIC consiste em um solução de **Firewall de próxima Geração,** que oferece uma plataforma de rede integrada baseada em inspeção profunda (deep packet inspection), provendo múltiplos mecanismos de proteção num único equipamento, tais como Intrusion Prevention System (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS).

O firewall de próxima geração além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte, permitindo: Instalação in- line sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, Stateful Inspection Protocol, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

4. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

4.1 A presente contratação justifica-se pois o IFSUL é uma instituição com mais de 23.000 estudantes, 2273 servidores e 296 estagiários, que demandam equipamentos e infraestrutura de rede segura para realizarem suas atividades acadêmicas e administrativas, garantindo a continuidade do negócio.

Atualmente o IFSUL possui 15 unidades, todos sem solução de Firewall ou com solução de firewall sem licenças, sem garantias e sem suporte, deixando toda a instituição em vulnerabilidade, situação que demanda por investimento para renovação de toda a solução provendo maior segurança e Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças.

4.2 O objeto da contratação está previsto no Plano de Contratações Anual, conforme apresentado no Documento de Oficialização de demanda.

4.3 O objeto da contratação também está alinhado com a Estratégia de Governo Digital e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) do IFSul, conforme apresentado no Documento de Oficialização de Demanda.

4.4 Por tratar de oferta de serviços públicos digitais, o objeto da contratação será integrado à Plataforma Gov.br, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016, e suas atualizações, de acordo com as especificações deste Termo de Referência

5. **PAPÉIS E RESPONSABILIDADES** São obrigações da CONTRATANTE:

5.1 nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.2 receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

5.3 verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

5.4 comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

5.5 acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;

5.6 efetuar o pagamento à contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

5.7 aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.8 liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.9 comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.10 prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

6. A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

7. A Administração realizará pesquisa de preços periodicamente, em prazo não superior a 180 (cento e oitenta) dias, a fim de verificar a vantajosidade dos preços registrados em Ata.

8. São obrigações do CONTRATADO

8.1 A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

- efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;
- O objeto deve estar acompanhado do manual do usuário, com uma versão em português e da relação da rede de assistência técnica autorizada;
- responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);
- substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;
- comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;
- manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

9. **Habilitação técnica do fornecedor**

9.1 Atestado de aptidão fornecido por pessoa jurídica de direito público ou privado, em nome da empresa, comprovando a realização de instalação contendo serviços com características semelhantes ao objeto da licitação, considerando-se cumulativamente as parcelas de maior relevância e quantitativos mínimos a seguir definidos, na forma do art. 30, II c/c §2º da Lei nº 14.133/21;

9.2 Deverá comprovar fornecimento, instalação e suporte de no mínimo 12 equipamentos de Firewall;

9.3 Certidão de Acervo Técnico emitido pelo Conselho Regional de Engenharia e Agronomia (CREA), o qual comprove a aptidão do (s) Responsável (is) Técnico (s) indicado (s) pela proponente para execução dos serviços, devendo constar no Acervo Técnico o(s) atestado(s) apresentado(s). O atestado de capacidade técnica e a certidão de acervo técnico deverão referir-se às atividades técnicas que façam parte das atribuições legais do profissional, sendo que somente serão aceitas as atribuições de execução e fiscalização;

9.4 Declaração indicando o engenheiro ou arquiteto que atuará como responsável técnico pela execução dos serviços contratados, acompanhado de prova de o profissional pertencer ao quadro permanente de funcionários da empresa (comprovação através de apresentação de contrato social, no caso de sócio; cópia da carteira de trabalho ou contrato particular de prestação de serviço; prova de sua eleição como Diretor(a) da proponente; ou Certidão de Registro de Pessoa Jurídica junto ao CREA onde conste como responsável técnico);

9.5 A licitante deverá comprovar que possui solução de Gerenciamento de Acesso Privilegiado (PAM), solução que permite fazer o compliance de todos os acessos administrativos efetuados nas ferramentas gerenciadas, permitindo que seja realizado a gravação de sessão de forma nativa e automática (sem a possibilidade de intervenção do usuário para interromper a gravação da tela), para permitir auditoria e consultas às ações realizadas pelo administrador:

- Comprovação feita através de: Apresentação de nota fiscal, vinculando a solução com a empresa, de aquisição da solução de PAM. "Teste de bancada" ou homologação, através da comprovação de integração da solução de PAM do órgão licitante com as soluções gerenciadas do órgão licitante;

- Justificativa: Com essa solução, o ÓRGÃO LICITANTE poderá realizar auditorias e acompanhar o trabalho sendo feito pela LICITANTE vencedora, através das gravações de sessões de acesso. Como a LICITANTE é uma empresa terceira acessando o ambiente do ÓRGÃO LICITANTE, é de suma importância que seja realizado o controle e monitoramento das ações que estes acessos externos farão no ambiente do ÓRGÃO LICITANTE e quais configurações serão feitas ou poderão ser feitas. Uma solução de PAM também permitirá o acesso dos funcionários da LICITANTE às soluções do ÓRGÃO LICITANTE, sem que tenham acesso à senha real do dispositivo, desta forma, maximizando a segurança e confidencialidade dos acessos.

9.6 Apresentação de comprovação de que a empresa possui, em seu quadro funcional, no mínimo, 1 (um) profissional alocado no projeto de implantação do sistema com certificação PMP (Project Management Institute) ou MBA em Gestão de Projetos. As comprovações deverão ser realizadas por meio da apresentação de diplomas, atestados ou certificados:

- Justificativa: Tal exigência se faz indispensável devido à complexidade e importância dos serviços para o ÓRGÃO LICITANTE, garantindo a instalação dos princípios da eficiência, da legalidade e do máximo aproveitamento dos recursos técnicos da solução adquirida em benefício da operação.

9.7 Certidão de registro da empresa no Conselho Regional de Engenharia e Agronomia (CREA), dentro de seu prazo de validade. As empresas que não possuem Registro no CREA no Estado do Rio Grande do Sul deverão apresentar Certidão de Registro de Pessoa Jurídica do CREA do seu estado e, no caso de sagrar-se vencedora do certame, deverá apresentar, quando da assinatura do contrato, visto do CREA/RS.

9.8 Deverá possuir pelo menos, 2 (dois) profissionais com certificações em soluções técnicas de segurança da informação dos principais fabricantes do Gartner, como por exemplo: Fortinet NSE7, Cisco CCNP Security, Cisco CCIE Security, Palo Alto PCNSE.

- Justificativa: Tal exigência se faz indispensável devido à complexidade e importância dos serviços para o ÓRGÃO LICITANTE, garantindo a instalação dos princípios da eficiência, da legalidade e do máximo aproveitamento dos recursos técnicos da solução adquirida em benefício da operação.

9.9 Deverá possuir pelo menos, 1 (um) profissional com certificações em soluções de Switching dos principais fabricantes do Gartner, como por exemplo: Aruba ACSP, Cisco CCNP, Juniper JNCIP-ENT.

- Justificativa: Tal exigência se faz indispensável devido à complexidade e importância dos serviços para o ÓRGÃO LICITANTE, garantindo a instalação dos princípios da eficiência, da legalidade e do máximo aproveitamento dos recursos técnicos da solução adquirida em benefício da operação.

9.10 Deverá possuir, em seu quadro de funcionários, ao menos um colaborador com as seguintes certificações: CISSP (Certified Information Systems Security Professional) ou CompTIA CASP+ (Advanced Security Practitioner), CompTIA Cybersecurity Analyst (CySA+) ou Systems Security Certified
Practitioner (SSCP), CompTIA Security+ ou Certified in Cybersecurity (CC), CompTIA Network+ CCIE ou CCNP;

- Justificativa: Tal exigência se faz indispensável devido à complexidade e importância dos serviços para o ÓRGÃO LICITANTE, garantindo a instalação das soluções seguindo as melhores práticas no âmbito da Segurança da Informação.

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

9.12 Deve possuir nível de parceiro máximo junto ao fabricante da solução, devendo ser comprovado através de declaração própria do fabricante.

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

10. ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO.

10.12 O prazo de entrega dos bens é de 60 dias, contados do envio da Ordem de Fornecimento e Nota de Empenho através de correspondência eletrônica, em remessa única, no endereço de cada unidade participante, conforme subitens abaixo.

10.13 Reitoria - Rua Gonçalves Chaves, nº 3218, Centro. Pelotas/RS. CEP 96015-560;

10.14 Campus Bagé - Av. Leonel de Moura Brizola, 2501 - Bairro Pedra Branca - Bagé/RS - CEP 96.418-400

10.15 Campus Charquesdas - Rua General Balbão, 81 - Bairro Centro - Charqueadas/RS - CEP 96.745-000;

10.16 Campus Gravataí - Rua Men de Sá, 800 - Bairro Bom Sucesso/Gravataí-RS - CEP: 94.135-300;

10.17 Campus Jaguarão - Rua Corredor das Tropas, 801- Jaguarão/RS - CEP 96.300-000;

10.18 Campus Lajeado - Rua João Goulart, 2150 - Bairro Olarias - Lajeado/RS - CEP 95.900-000;

10.19 Campus Passo Fundo - Estrada Perimetral Leste, 150 - Passo Fundo/RS - CEP 99.064-440;

10.20 Campus Pelotas - Praça Vinte de Setembro, 455 - Centro - Pelotas/RS - CEP 96.015-360;

10.21 Campus Pelotas VG - Av. Ildelfonso Simões Lopes, 2791 - Bairro Arco-Íris - Pelotas/RS - CEP 96.060-290;

10.22 Campus Santana do Livramento - Av. Paul Harris, 410 - Bairro Centro - Santana do Livramento/RS - CEP 97.574360;

10.23 Campus Sapiranga - Av Carlos Gilberto Weis, 155 - Oeste - Sapiranga/RS - CEP 93.800-000;

10.24 Campus Sapucaia do Sul - Av. Copacabana, 100 - Bairro Piratini - Sapucaia do Sul/RS - CEP 93.216-120; 10.25 Campus Venâncio Aires - Av. das Indústrias, 1865 - Bairro Universitário - Venâncio Aires/RS - CEP 95.800-000;

10.26 Campus Camaquã - Ana Gonçalves da Silva, 901 - Camaquã - RS - CEP: 96785-130.

10.27 Os bens serão recebidos provisoriamente no prazo de até´ 5 dias, pelo(a) responsável pela TI e Patrimônio da Unidade, para efeito de verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

10.28 Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 5 dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

10.29 Os bens serão recebidos definitivamente no prazo de 10 dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

10.30 Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo

10.31 O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução e entrega do objeto conforme termo de referência.

11. MODELO DA EXECUÇÃO

11.12 Nos termos do art. 67 Lei nº 14.133/21, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

11.1.1. O recebimento de material de valor superior a R$ 80.000,00 (oitenta mil reais) será confiado a uma comissão de, no mínimo, 3 (três) membros, designados pela autoridade competente.

11.13 A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 14.133/21.

11.14 O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

12. DAS SANÇÕES ADMINISTRATIVAS

12.12 Comete infração administrativa nos termos da Lei nº 14.133/21 e da Lei nº 10.520, de 2002, a Contratada que:

12.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

12.1.2. ensejar o retardamento da execução do objeto;

12.1.3. fraudar na execução do contrato;

12.1.4. comportar-se de modo inidôneo;

12.1.5. cometer fraude fiscal;

12.1.6. não mantiver a proposta.

12.13 A Contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

9.2.1. advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

9.2.2. multa moratória 0,33% (zero vírgula trinta e três por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

9.2.3. multa compensatória 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

9.2.4. em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

9.2.5. suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

9.2.6. impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

9.2.7. declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

12.14 Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 14.133/21, as empresas e os profissionais que:

9.3.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

9.3.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

9.3.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

12.15 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 14.133/21, e subsidiariamente a Lei nº 9.784, de 1999.

12.16 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

12.17 As penalidades serão obrigatoriamente registradas no SICAF.

PELOTAS, 23 de julho de 2024.

INSTITUTO FEDERAL
SUL-RIO-GRANDENSE

Instituto Federal Sul -rio-grandense
Diretoria de Tecnologia da Informação

ESTUDO TÉCNICO PRELIMINAR

INTRODUÇÃO
O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação. **Referência: Art. 11 da IN SGD/ME nº 94 de 2022.**

1 - Descrição da Solução de Tecnologia da Informação

No presente documento, a Equipe de Planejamento da Contratação, designada conforme o Documento de Formalização de Demanda (DOD), tem o objetivo de pesquisar, analisar e apresentar uma Solução de Tecnologia da Informação e Comunicação, viável, para a aquisição de solução de firewall para o IFSul.

A constante modernização dos aparatos de Tecnologia da Informação e a evolução das aplicações da Internet trazem a necessidade da adoção de soluções de segurança da informação que garantam a integridade dos dados trafegados e armazenados dentro do ambiente de rede do IFSul. Principalmente considerando os normativos relacionados a segurança da informação e em atendimento à Portaria SGD/MGI nº 852, de 28 de março de 2023, que dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI) entendendo que a segurança da informação deve ser tema relevante e deve ser tratada como tópico relacionado aos riscos estratégicos da instituição.

A solução atualmente existente no IFSul não abrange os campus e devido as suas limitações, falta de licenças e garantias, dificulta que os administradores da rede evitem ataques externos aos sistemas acadêmicos, tampouco que usuários, mesmo sem intenção, propaguem algum arquivo mal-intencionado (malware), colocando em risco todos dados da rede do IFSul.

É incontestável, em termos técnicos, que o IFSul precisa modernizar sua infraestrutura de segurança da informação de perímetro, visando proteger toda rede de dados com uma solução de firewall de próxima geração.
Frente ao exposto, a Diretoria de Tecnologia da Informação – DTI vem avaliando soluções de segurança e chegou ao desenho deste projeto, em conformidade com todo o arcabouço normativo que regulamenta a área de segurança da informação, para análise e seleção da melhor solução para atender a demanda de modernização da infraestrutura de segurança da informação de perímetro.

Ao fim do projeto de levantamento, a equipe constatou a necessidade da aquisição de uma solução de firewall de próxima geração para a segurança da rede de dados e computadores do IFSul.

2 - Definição e Especificação das Necessidades e Requisitos

2.1 - Necessidades e Requisitos de Negócio		
ID	Funcionalidades	Envolvidos
1	A Solução deve possuir recurso de proteção a Ameaça Persistente Avançada (APT). Estudos apontam cada vez mais um número maior de ataques APT. Esta técnica permite ao hacker burlar sistemas de Antivírus e IPS, uma vez que esses sistemas se baseiam em evidências e dependem da descoberta e estudo do vírus para criação de uma „vacina". Os sistemas APT são proativos e analisam o comportamento dos arquivos para detectar vírus que ainda não foram descobertos e consequentemente não possuem vacinas. Portanto faz-se necessário o recurso de proteção à Ameaça Persistente Avançada (APT) nesta solução.	DTI
2.	A solução deve suportar Alta Disponibilidade de forma com que falhas físicas não interfiram nas funcionalidades de proteção e disponibilidade dos sistemas e Internet. Redundância automática de equipamentos de modo a permitir que os sistemas não sejam comprometidos dado uma falha física no equipamento;	DTI
3.	A solução deve proteger os sistemas do IFSUL em tempo real e prover visibilidade granular das tentativas de ataques sem perda de desempenho. Deve possibilitar as seguintes inspeções: a) Intrusion Prevention System (IPS): Deve possuir modulo para proteção de ataques a vulnerabilidades conhecidas e desconhecidas; b) Antivírus: Deve possuir módulo para proteção em tempo real contra vírus e malwares conhecidos e desconhecidos; c) Aplicação: A solução deverá possuir recursos de reconhecimento de aplicações e grupos de aplicações de forma granular. Ex. Reconhecer e distinguir aplicações como facebook e chat do facebook; d) Filtro URL: Para efetuar controle dos acessos aos sites a solução deverá conter funcionalidades de filtro URL, através de categorização automática dos sites; e) Filtro de arquivos: Deve possuir módulo para filtro de arquivos por tipo. Ex. Filtrar arquivos .dll;	DTI

4.	Deverá integrar com a base de usuários LDAP / Active Directory existente atualmente no IFSul. Deverá possuir a capacidade de identificar o usuário de rede com integração ao LDAP / Active Directory sem a necessidade de instalação de agente nas estações dos usuários. A integração com a base de usuários existente do IFSul é imprescindível para facilitar a gestão e a visibilidade dos acessos por usuário e grupo de usuários.	DTI
5.	A solução deve permitir o gerenciamento centralizado das configurações, alertas e logs. A solução apresentada deverá realizar gerenciamento centralizado e correlacionar eventos de todas as inspeções, de forma a facilitar a criação de novas configurações e auditar possíveis incidentes.	DTI

6.	Manutenção do ambiente Os técnicos envolvidos deverão estar treinados no processo de instalação e configuração do ambiente. Recomendável manter o contrato de suporte com o fabricante vigente, a fim de minimizar riscos em caso de falhas de hardware e bugs de sistema. Dentre as vantagens de possuir um contrato de manutenção ativo, destacam-se: Hardware: possibilidade de troca de equipamento ou peça no caso de falha, possibilidade de atualização de firmware para melhoria de operação ou utilização de novos recursos do equipamento, suporte do fabricante na resolução de problemas graves; Software: possibilidade de atualização das licenças de software durante o período de garantia. As atualizações são úteis para resolução de problemas (bugs), correções de segurança e implantação de novos recursos/funcionalidades da solução. A capacitação dos colaboradores nos treinamentos oficiais de fabricantes deverá possibilitar manter a operação do ambiente sem a necessidade de um contrato externo de manutenção.	DTI
7.	Capacitação do corpo técnico para a administração e gerenciamento do ambiente A referência mais apropriada é que as capacitações a serem realizadas sejam a dos próprios fabricantes da solução vencedora do certame (hardware e software) ou pelo fornecedor/integrador capacitado e certificado na solução completa. Além de ser uma capacitação para criação, manutenção e administração do ambiente, a capacitação é também considerada como um importante requisito de manutenção já que, após o fim do contrato, é importante que a equipe do IFSul tenha domínio total para manter a solução em pleno funcionamento.	DTI

2.2 - Requisitos Tecnológicos	
1	A solução deve permitir a visualização e classificação granular de todo trafego de rede, incluindo aplicações em camada 7, com geração de relatórios completos para analise detalhada do tráfego e das ameças;
2	A solução deve proteger a rede de dados contra ameaças conhecidas e desconhecidas (zero-day) como virus, malwares, bots, ransomwares, ataques DdoS, etc.
3	A solução deve permitir a criação de regras e permissões de acessos conforme política de segurança da informação e arquitetura de rede do instituto.
4	A Solução deve suportar o bloqueio ou filtro de aplicações e conteúdos conforme categorias ou URL
2.3 - Requisitos de continuidade do serviço	
Todos os itens deverão possuir licenças em caráter perpétuo para manter a solução ativa e operacional mesmo após vencimento do período de suporte e garantia.	
Ação Preventiva	Manter o contrato de suporte e garantia ativo
Ação Contingência	Renovar o contrato de suporte e garantia

3 -Estimativa da demanda - Quantidade de Bens e Serviços

A presente sessão contém o registro do quantitativo de bens e serviços necessários para a composição da solução a ser contratada, de forma detalhada, motivada e justificada. Busca-se descrever também os métodos, as metodologias e as técnicas de estimativas que foram utilizadas, nos termos do inciso I do art. 11 da Instrução Normativa SGD/ME nº 94, de 2022.

De forma a mensurar a demanda a ser atendida, levou-se em consideração um *assessment* realizado em todos os campus para identificar a demanda e a situação atual de cada um deles.

É importante ressaltar que o IFSUL é uma instituição com mais de 23.000 estudantes, 2273 servidores e 296 estagiários, que demandam equipamentos e infraestrutura de rede segura para realizarem suas atividades acadêmicas e administrativas, garantindo a continuidade do negócio.

Atualmente o IFSUL possui 15 unidades, todos com solução de firewall sem licenças, sem garantias e sem suporte, deixando toda a instituição em vulnerabilidade, situação que demanda por investimento para renovação de toda a solução provendo maior segurança e Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças.

Com base em todo o exposto, o quadro abaixo apresenta a estimativa da demanda.

BEM/SERVIÇO	ESTIMATIVA
FIREWALL TIPO 1 COM LICENÇA DE FILTRO URL, LICENÇAS DE PROTEÇÃO CONTRA AMEAÇAS CONHECIDAS E DESCONHECIDAS E SUPORTE/GARANTIA DE 36 MESES	2
FIREWALL TIPO 2 COM LICENÇA DE FILTRO URL, LICENÇAS DE PROTEÇÃO CONTRA AMEAÇAS CONHECIDAS E DESCONHECIDAS E SUPORTE/GARANTIA DE 36 MESES	4
FIREWALL TIPO 3 COM LICENÇA DE FILTRO URL, LICENÇAS DE PROTEÇÃO CONTRA AMEAÇAS CONHECIDAS E DESCONHECIDAS E SUPORTE/GARANTIA DE 36 MESES	10
FIREWALL TIPO 4 COM LICENÇA DE FILTRO URL, LICENÇAS DE PROTEÇÃO CONTRA AMEAÇAS CONHECIDAS E DESCONHECIDAS E SUPORTE/GARANTIA DE 36 MESES	12
SOFTWARE DE GESTÃO CENTRALIZADA PARA NGFW COM SUPORTE/GARANTIA DE 3 ANOS	1
SOFTWARE DE RELATORIA/LOGS CENTRALIZADA PARA NGFW COM SUPORTE/GARANTIA DE 3 ANOS	4
BANCO DE HORAS – SUPORTE TÉCNICO	180h

4 -Análise das Soluções

4.1 -Identificação das Soluções

Solução 1	
Entidade	Solução 1: Firewall UTM

Descrição	Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs. Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.
Fornecedor	Empresa Privada. Tipo de solução desenhada especificamente para cada instituição, considerando trafego, número de usuários e outras variáveis.
Solução 2	
Entidade	Solução 2: Firewall de Próxima Geração
Descrição	É uma plataforma de rede integrada que é baseada em inspeção profunda (deep packet inspection), provendo múltiplos mecanismos de proteção num único equipamento, tais como Intrusion Prevention System (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda promete entregar performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação in-line sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, Stateful Inspection Protocol, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.
Fornecedor	Iniciativa Privada. Tipo de solução desenhada especificamente para cada instituição, considerando trafego, número de usuários e outras variáveis.
Solução 3	
Entidade	Solução 3: Composição de Soluções de Segurança

Descrição	Trata-se da composição de múltiplos equipamentos criando assim uma solução de proteção completa. As proteções que se esperam são: Intrusion Prevention System (IPS), Antivírus, Ameaça Persistente Avançada, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, Filtro de Websites e Gerenciamento de banda (QoS). A solução poderá ser de 1 ou mais fornecedores de acordo com a funcionalidade desejada.
Fornecedor	Iniciativa Privada. Tipo de solução desenhada especificamente para cada instituição, considerando trafego, número de usuários e outras variáveis.

4.2 - Análise comparativa das soluções existentes

Comparação de Alternativas				
Requisitos	**Solução**	**Sim**	**Não**	**Não se aplica**
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	1, 2 e 3	X X X		
A Solução está disponível no Portal do Software Público Brasileiro?(quando se tratar de software)	1, 2 e 3			X X X
A Solução é composta por software livre ou software público? (quando se tratar de software)	1, 2 e 3			X X X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	1, 2 e 3			X X X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1, 2 e 3			X X X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	1, 2 e 3			X X X

5 - Registro de soluções inviáveis

Solução 1 é inviável, pois Unified Threat Management (UTM) não é apropriado para ambientes complexos com múltiplas unidades como a do IFSUL, pois A solução de “UTM” embora permita a gerência centralizada e correlação dos logs de todos os módulos que incluem na solução, não contempla o módulo de proteção a Ameaça Persistente Avançada (APT);

As soluções de “UTM” não possuem nativamente proteção a Ameaça Persistente Avançada (APT), sendo necessário a composição do UTM com outro equipamento para atender esta demanda; Tornando a solução mais cara, mais complexa e mais difícil de gerenciar.

Solução 3 é inviável, Pois uma composição de Soluções de Segurança para atender um ambiente descentralizado, mantendo uma gestão centralizada se forma inviável, pois não existe meios para gerenciar todo o ambiente. Além disso, na “solução composta”, seria inviável ter um nível aceitável de integração para configuração e logs centralizados, uma vez que estaremos lidando com equipamentos de diferentes fabricantes;

Ainda, nas “soluções compostas” para inspeção de Ameaça Persistente Avançada, não oferece meios para realização de inspeção centralizada, sendo assim, é necessário adicionado outro equipamento com a função única de inspecionar Ameaça Persistente Avançada, tornando o valor mais elevado e a gestão da solução mais complexa.

6 - Solução escolhida:

Solução 2

6.1 - Descrição da Solução Escolhida			
Solução	2	DESCRIÇÃO	**Solução 2: Firewall de próxima Geração** É uma plataforma de rede integrada que é baseada em inspeção profunda (deep packet inspection), provendo múltiplos mecanismos de proteção num único equipamento, tais como Intrusion Prevention System (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda promete entregar performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação in-line sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, Stateful Inspection Protocol, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

6.1.1 - Justificativa para a solução

Solução 2: Firewall de Próxima Geração Após estudos de mercado, conclui-se que a solução de Firewall de Próxima Geração demonstrou ser a melhor opção para alcançar os objetivos que o IFSul pretende com esta aquisição, principalmente por centralizar todas as inspeções num único local, o que permite a gestão centralizada e correlacionada dessas informações em tempo real. A utilização deste tipo de solução já é bastante difundida em instituições públicas o que comprova sua eficácia.

A solução de “Firewall de Próxima Geração” permite a gerência centralizada e correlação dos logs, atendendo a este requisito, uma das principais demandas do projeto;

O firewall de próxima geração possui todas as características levantadas pelo IFSul como necessidades deste projeto.

Cabe ressaltar algumas vantagens e desvantagens das soluções analisadas durante este estudo:

A Solução Unified Threat Management (UTM):

Para atender as necessidades do IFSul, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível nas localidades do IFSul envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e só possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes; Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução; Outro ponto elencado como uma das necessidades desta solução é a integração da solução com a base de usuários existentes neste órgão. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory;

E por fim, com o intuito de proteger os investimentos do IFSul para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução Composição de soluções de segurança: A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante; Por contar com um quantitativo de servidores reduzido para a administração da rede, a DTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações do IFSul;

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta em custo operacional elevado, bem como alto custo de renovação de contrato;

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade;

6.1.2 - Descrição da solução a ser contratada

6.1.3 - Bens e serviços que compõem a Solução		
ID	BEM/SERVIÇO	QUANTITATIVOS
1	FIREWALL TIPO 1 COM LICENÇA DE FILTRO URL, LICENÇAS DE PROTEÇÃO CONTRA AMEAÇAS CONHECIDAS E DESCONHECIDAS E SUPORTE/GARANTIA DE 36 MESES	2
2	FIREWALL TIPO 2 COM LICENÇA DE FILTRO URL, LICENÇAS DE PROTEÇÃO CONTRA AMEAÇAS CONHECIDAS E DESCONHECIDAS E SUPORTE/GARANTIA DE 36 MESES	4
3	FIREWALL TIPO 3 COM LICENÇA DE FILTRO URL, LICENÇAS DE PROTEÇÃO CONTRA AMEAÇAS CONHECIDAS E DESCONHECIDAS E SUPORTE/GARANTIA DE 36 MESES	10
4	FIREWALL TIPO 4 COM LICENÇA DE FILTRO URL, LICENÇAS DE PROTEÇÃO CONTRA AMEAÇAS CONHECIDAS E DESCONHECIDAS E SUPORTE/GARANTIA DE 36 MESES	12
5	SOFTWARE DE GESTÃO CENTRALIZADA PARA NGFW COM SUPORTE/GARANTIA DE 3 ANOS	1
6	SOFTWARE DE RELATORIA/LOGS CENTRALIZADA PARA NGFW COM SUPORTE/GARANTIA DE 3 ANOS	4
7	BANCO DE HORAS – SUPORTE TÉCNICO	180h

Benefícios a serem alcançados	
1.	Maior visibilidade do trafego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
2.	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização de recursos
3.	Geração de relatórios dos acessos realizados por IP, grupo ou usuário nas seguintes formas: diários, semanal, mensal ou periodo selecionado;
4.	Criação de políticas de proteção da rede de computadores contra ataques de hackers através do bloqueio de programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;

5.	Proteção do ambiente de rede contra worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
6.	Regras de bloqueio e liberação de portas de serviços TCP e UDP por grupo ou usuário;
7.	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações
8.	Administração centralizada de todos os firewalls para melhor gestão de logs e visualização de informações do tráfego da rede (relatórios).

7 - Declaração de viabilidade da contratação

A declaração da viabilidade da contratação expressa nesta seção apresenta a justificativa da solução escolhida, abrangendo a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

Nesse sentido, o planejamento em tela almeja os seguintes resultados:

Economia no valor da aquisição em função do ganho de escala;
Eficiência com a diminuição do custo administrativo em função da redução da fragmentação de processos licitatórios por unidades do IFSul;
Efetividade com a padronização dos produtos e oferta de uma solução que objetiva maior produtividade e gestão centralizada da solução;
Eficácia com o atendimento das necessidades das unidades que cadastraram suas necessidades de contratação de solução de firewall;
Além disso, frisa-se que a presente contratação atende adequadamente às demandas de negócio formuladas, os benefícios a serem alcançados são adequados, os custos previstos são compatíveis.
Considerando as informações do presente estudo, entende-se que a presente contratação se configura tecnicamente VIÁVEL.

8 - Aprovação e Assinaturas

Conforme o § 2º do Art. 11 da Instrução Normativa SGD/ME nº 94, de 2022, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TI:

8.1 - Integrante Técnico

O presente planejamento foi elaborado em harmonia com a Instrução Normativa SGD/ME nº 94, de 2022 - Secretaria do Governo Digital do Ministério da Economia, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da aquisição.

Declaração válida com assinatura eletrônica do Integrante Técnico: Igor Born Machado

8.2 - Integrante Requisitante

O presente planejamento atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área requisitante

priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a aquisição proposta.

Declaração válida com assinatura eletrônica do Integrante Requisitante: Eduardo da Silva Moller

8.3 - Aprovação da autoridade máxima da área de TI

O presente planejamento atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados e s definições técnicas atendem as necessidades da demanda.

Declaração válida com assinatura eletrônica da Autoridade da Área de TI: Carla Simone Guedes Pires

23 de julho de 2024

APÊNDICE I

1. **DESCRITIVO TÉCNICO DOS PRODUTOS**
    1. **REQUISITOS ESPECÍFICOS – ITEM 1 – FIREWALL DE BORDA TIPO 1 COM LICENCIAMENTO PARA ATIVAÇÃO DE FUNCIONALIDADES DE PROTEÇÃO PARA 36 MESES**
        a. **Deve suportar, no mínimo, 155 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, considerando pacotes de 512 bytes**
        b. **Deve suportar, no mínimo, 24.5 Gbps de throughput IPS**
        c. **Deve suportar, no mínimo, 54 Gbps de throughput de VPN IPSec**
        d. **Deve suportar, no mínimo, 9 Gbps de throughput de VPN SSL**
        e. **Deve suportar, no mínimo, 16 Gbps de throughput de Inspeção SSL**
        f. **Deve suportar, no mínimo, 72 Gbps de throughput de Controle de Aplicação**
        g. **Deve suportar, no mínimo, 19 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.**
        h. **Suporte a, no mínimo, 15 milhões de conexões simultâneas;**
        i. **Deve suportar o gerenciamento de no mínimo 500 Pontos de Acesso Wi-Fi do mesmo fabricante em modo Tunel, ou até 1000 em modo "Bridge", com saída local na unidade;**
        j. **Deve suportar o gerenciamento de no mínimo 75 Switches do mesmo fabricante por equipamento;**
        k. **Suporte a, no mínimo, 690 mil novas conexões por segundo**
        l. **Estar licenciado para, ou suportar sem o uso de licença, 1800 túneis de VPN IPSEC Site-to-Site simultâneos**
        m. **Estar licenciado para, ou suportar sem o uso de licença, 45.000 túneis de clientes VPN IPSEC simultâneos**
        n. **Estar licenciado para, ou suportar sem o uso de licença, 9.000 clientes de VPN SSL simultâneos**
        o. **Caso seja necessário fornecimento de licenças para prover o uso de VPN para a quantidade de usuários solicitada, a licença deverá operar em caráter perpétuo**
        p. **Possuir ao menos 14 interfaces 1Gbps RJ-45**
        q. **Possuir ao menos 8 interfaces 1Gbps SFP**
        r. **Possuir ao menos 2 interfaces SFP+ 10 Gigabit**
        s. **Possuir ao menos 4 interfaces SFP28 25 Gigabit**
        t. **Deverá possuir interface USB 3.0 para exportação de backups;**
        u. **Deverá possuir interface do tipo console para utilização de CLI**
        v. **Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance**
        w. **Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance**
        x. **Possuir no máximo 1 RU de altura**
        y. **Deverá ser fornecido com fonte de alimentação interna redundante com suporte a hot-swap;**

    2. **REQUISITOS ESPECÍFICOS – ITEM 2 – FIREWALL DE BORDA TIPO 2 COM LICENCIAMENTO PARA ATIVAÇÃO DE FUNCIONALIDADES DE PROTEÇÃO PARA 36 MESES**
        a. **Deve suportar, no mínimo, 132 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, considerando pacotes de 512 bytes**
        b. **Deve suportar, no mínimo, 13.2 Gbps de throughput IPS**
        c. **Deve suportar, no mínimo, 54 Gbps de throughput de VPN IPSec**
        d. **Deve suportar, no mínimo, 4 Gbps de throughput de VPN SSL**
        e. **Deve suportar, no mínimo, 8.5 Gbps de throughput de Inspeção SSL**
        f. **Deve suportar, no mínimo, 30 Gbps de throughput de Controle de Aplicação**
        g. **Deve suportar, no mínimo, 10 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.**
        h. **Suporte a, no mínimo, 8 milhões de conexões simultâneas;**
        i. **Deve suportar o gerenciamento de no mínimo 500 Pontos de Acesso Wi-Fi do mesmo fabricante em modo Tunel, ou até 1000 em modo "Bridge", com saída local na unidade;**

j. **Deve suportar o gerenciamento de no mínimo 80 Switches do mesmo fabricante por equipamento;**
k. **Suporte a, no mínimo, 500 mil novas conexões por segundo**
l. **Estar licenciado para, ou suportar sem o uso de licença, 1.600 túneis de VPN IPSEC Site-to-Site simultâneos**
m. **Estar licenciado para, ou suportar sem o uso de licença, 40.000 túneis de clientes VPN IPSEC simultâneos**
n. **Estar licenciado para, ou suportar sem o uso de licença, 7.500 clientes de VPN SSL simultâneos**
o. **Caso seja necessário fornecimento de licenças para prover o uso de VPN para a quantidade de usuários solicitada, a licença deverá operar em caráter perpétuo**
p. **Possuir ao menos 14 interfaces 1Gbps RJ-45**
q. **Possuir ao menos 6 interfaces 1Gbps SFP**
r. **Possuir ao menos 4 interfaces 25Gbps SFP28**
s. **Possuir ao menos 4 interfaces 10Gbps SFP+**
t. **Deverá possuir interface USB 3.0 para exportação de backups;**
u. **Deverá possuir interface do tipo console para utilização de CLI**
v. **Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance**
w. **Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance**
x. **Possuir no máximo 1 RU de altura**
y. **Deverá ser fornecido com fonte de alimentação interna redundante com suporte a hot-swap;**

3. **REQUISITOS ESPECÍFICOS – ITEM 3 – FIREWALL DE BORDA TIPO 3 COM LICENCIAMENTO PARA ATIVAÇÃO DE FUNCIONALIDADES DE PROTEÇÃO PARA 36 MESES**
   a. **Deve suportar, no mínimo, 76 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, considerando pacotes de 512 bytes**
   b. **Deve suportar, no mínimo, 11 Gbps de throughput IPS**
   c. **Deve suportar, no mínimo, 50 Gbps de throughput de VPN IPSec**
   d. **Deve suportar, no mínimo, 3 Gbps de throughput de VPN SSL**
   e. **Deve suportar, no mínimo, 8 Gbps de throughput de Inspeção SSL**
   f. **Deve suportar, no mínimo, 26 Gbps de throughput de Controle de Aplicação**
   g. **Deve suportar, no mínimo, 8 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.**
   h. **Suporte a, no mínimo, 7 milhões de conexões simultâneas;**
   i. **Deve suportar o gerenciamento de no mínimo 250 Pontos de Acesso Wi-Fi do mesmo fabricante em modo Tunel, ou até 500 em modo "Bridge", com saída local na unidade;**
   j. **Deve suportar o gerenciamento de no mínimo 60 Switches do mesmo fabricante por equipamento;**
   k. **Suporte a, no mínimo, 450 mil novas conexões por segundo**
   l. **Estar licenciado para, ou suportar sem o uso de licença, 1.500 túneis de VPN IPSEC Site-to-Site simultâneos**
   m. **Estar licenciado para, ou suportar sem o uso de licença, 35.000 túneis de clientes VPN IPSEC simultâneos**
   n. **Estar licenciado para, ou suportar sem o uso de licença, 3.000 clientes de VPN SSL simultâneos**

o. **Caso seja necessário fornecimento de licenças para prover o uso de VPN para a quantidade deusuários solicitada, a licença deverá operar em caráter perpétuo**
p. **Possuir ao menos 15 interfaces 1Gbps RJ-45**
q. **Possuir ao menos 6 interfaces 1Gbps SFP**
r. **Possuir ao menos 8 interfaces 10Gbps SFP+**
s. **Deverá possuir interface USB 3.0 para exportação de backups;**
t. **Deverá possuir interface do tipo console para utilização de CLI**
u. **Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos(Contextos) por appliance**
v. **Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance**
w. **Possuir no máximo 1 RU de altura**
x. **Deverá ser fornecido com fonte de alimentação interna redundante com suporte a hot-swap;**

4. **REQUISITOS ESPECÍFICOS – ITEM 4 – FIREWALL DE BORDA TIPO 4 COM LICENCIAMENTO PARAATIVAÇÃO DE FUNCIONALIDADES DE PROTEÇÃO PARA 36 MESES**
   a. **Deve suportar, no mínimo, 36 Gbps com a funcionalidade de firewall habilitada para tráfegoIPv4 e IPv6, considerando pacotes de 512 bytes**
   b. **Deve suportar, no mínimo, 5 Gbps de throughput IPS**
   c. **Deve suportar, no mínimo, 32 Gbps de throughput de VPN IPSec**
   d. **Deve suportar, no mínimo, 1.2 Gbps de throughput de VPN SSL**
   e. **Deve suportar, no mínimo, 3 Gbps de throughput de Inspeção SSL**
   f. **Deve suportar, no mínimo, 6 Gbps de throughput de Controle de Aplicação**
   g. **Deve suportar, no mínimo, 2.5 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.**
   h. **Suporte a, no mínimo, 3 milhões de conexões simultâneas;**
   i. **Deve suportar o gerenciamento de no mínimo 50 Pontos de Acesso Wi-Fi do mesmo fabricanteem modo Tunel, ou até 100 em modo "Bridge", com saída local na unidade;**
   j. **Deve suportar o gerenciamento de no mínimo 30 Switches do mesmo fabricante por equipamento;**
   k. **Suporte a, no mínimo, 120 mil novas conexões por segundo**
   l. **Estar licenciado para, ou suportar sem o uso de licença, 1.500 túneis de VPN IPSEC Site-to-Sitesimultâneos**
   m. **Estar licenciado para, ou suportar sem o uso de licença, 15.000 túneis de clientes VPN IPSECsimultâneos**
   n. **Estar licenciado para, ou suportar sem o uso de licença, 500 clientes de VPN SSL simultâneos**
   o. **Caso seja necessário fornecimento de licenças para prover o uso de VPN para a quantidade deusuários solicitada, a licença deverá operar em caráter perpétuo**
   p. **Possuir ao menos 16 interfaces 1Gbps RJ-45**
   q. **Possuir ao menos 6 interfaces 1Gbps SFP**
   r. **Possuir ao menos 4 interfaces 10Gbps SFP+**
   s. **Deverá possuir interface USB 3.0 para exportação de backups;**
   t. **Deverá possuir interface do tipo console para utilização de CLI**
   u. **Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos(Contextos) por appliance**
   v. **Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance**

w. **Possuir no máximo 1 RU de altura**
x. **Deverá ser fornecido com fonte de alimentação interna redundante;**

5. **REQUISITOS EM COMUM PARA OS ITENS 1, 2, 3, 4 E 5**
   a. **O Firewall deverá suportar e estar licenciado para o uso das diversas ferramentas de segurança incluídas em um Next Generation Firewall, como Antivírus, IPS, Filtragem Web, Controle de Aplicações, Proteção contra Botnets, Proteção contra Malwares Avançados e Antispam de Gateway.**
   b. **O projeto deverá contemplar serviço de instalação, configuração e treinamento de toda a solução;**
   c. **Todas as soluções deverão ser fornecidas com 36 meses de garantia pelos fabricantes, namodalidade NBD (Next Business Day);**
   d. **O fabricante ofertado deve estar posicionado no quadrante "Leader" do quadrante mágico doGartner de 2023 ou mais recente, na categoria Network Firewalls;**
   e. **CARACTERÍSTICAS GERAIS DE FUNCIONALIDADES**
      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. **Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;**
      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;**
      4. **A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;**
      5. **A gestão do equipamento deve ser compativel através da interface de gestão Web no mesmo dispositivo de proteção da rede;**
      6. **Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;**
      7. **Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;**
      8. **Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;**
      9. **Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);**
      10. **Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;**
      11. **Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;**
      12. **Os dispositivos de proteção de rede devem suportar sFlow;**
      13. **Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;**
      14. **Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;**
      15. **Deve suportar NAT dinâmico (Many-to-1);**
      16. **Deve suportar NAT dinâmico (Many-to-Many);**
      17. **Deve suportar NAT estático (1-to-1);**
      18. **Deve suportar NAT estático (Many-to-Many);**
      19. **Deve suportar NAT estático bidirecional 1-to-1;**
      20. **Deve suportar Tradução de porta (PAT);**
      21. **Deve suportar NAT de Origem;**
      22. **Deve suportar NAT de Destino;**
      23. **Deve suportar NAT de Origem e NAT de Destino simultaneamente;**

24. **Deve poder combinar NAT de origem e NAT de destino na mesma política**
25. **Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemasde roteamento assimétrico;**
26. **Deve suportar NAT64 e NAT46;**
27. **Deve implementar o protocolo ECMP;**
28. **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;**
29. **Enviar log para sistemas de monitoração externos, simultaneamente;**
30. **Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;**
31. **Proteção anti-spoofing;**
32. **Suportar otimização do tráfego entre dois equipamentos;**
33. **Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);**
34. **Para IPv6, deve suportar roteamento estático e dinâmico (RIPng, OSPFv3, BGP4+);**
35. **Suportar OSPF graceful restart;**
36. **Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados darede;**
37. **Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade dotráfego;**
38. **Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade dotráfego;**
39. **Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;**
40. **Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modotransparente;**
41. **Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;**
42. **Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 ecom no mínimo 3 equipamentos no cluster;**
43. **A configuração em alta disponibilidade deve sincronizar: Sessões;**
44. **A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, masnão limitado as políticas de Firewall, NAT, QOS e objetos de rede;**
45. **A configuração em alta disponibilidade deve sincronizar: Associações de Segurança dasVPNs;**
46. **A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;**
47. **O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;**
48. **Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;**
49. **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;**
50. **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;**
51. **O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;**
52. **Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente**

dentrode cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

53. O console de administração deve suportar pelo menos inglês, espanhol e português.
54. A solução deve oferecer suporte à integração nativa de equipamentos de proteção de email, firewall de aplicativos, proxy, cache e ameaças avançadas.
55. 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.

f. FUNCIONALIDADES DE CONTROLE POR POLÍTICAS

1. Deverá suportar controles por zona de segurança;
2. Controles de políticas por porta e protocolo;
3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos deaplicações (baseados em características e comportamento das aplicações) e categorias deaplicações;
4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
5. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering nomínimo) diretamente às políticas de segurança versus via perfis;
6. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;
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.
8. Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF);
9. Deve suportar o protocolo padrão da indústria VXLAN;
10. Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política defirewall
11. Deve possuir base com objetos de endereço IP, de serviços da internet como Google eOffice 365, atualizados dinamicamente pela solução
12. A solução deve oferecer suporte à integração nativa com a solução de sandbox, proteçãode email e firewall de aplicativos da Web.

g. FUNCIONALIDADES DE CONTROLE DE APLICAÇÃO

1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
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;
3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar econtrolar as aplicações e os ataques que utilizam táticas evasivas via comunicações

criptografadas, tais como Skype e utilização da rede Tor;

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;**
6. **Identificar o uso de táticas evasivas via comunicações criptografadas;**
7. **Atualizar a base de assinaturas de aplicações automaticamente;**
8. **Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IPde origem, usuários e grupos;**
9. **Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;**
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;**
11. **O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;**
12. **Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindogranularidade de controle/políticas para os mesmos;**
13. **Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;**
14. **Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;**
15. **Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindogranularidade de controle/políticas para os mesmos;**
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);**
17. **Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;**
18. **Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;**
19. **Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente**

h. **FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS**

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. **Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos(Antivírus e Anti-Spyware);**
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 ofabricante;**
4. **Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado emalta disponibilidade;**
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 dedestino, serviço e a combinação de todos esses itens;**
6. **Deve permitir o bloqueio de vulnerabilidades;**

7. **Deve incluir proteção contra-ataques de negação de serviços;**
8. **Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise de decodificação deprotocolo;**
9. **Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise para detecção deanomalias de protocolo;**
10. **Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation;**
11. **Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes deTCP;**
12. **Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados;**
13. **Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood,etc;**
14. **Detectar e bloquear a origem de portscans;**
15. **Bloquear ataques efetuados por worms conhecidos;**
16. **Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;**
17. **Possuir assinaturas para bloqueio de ataques de buffer overflow;**
18. **Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;**
19. **Identificar e bloquear comunicação com botnets;**
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;**
21. **Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;**
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;**
23. **Os eventos devem identificar o país de onde partiu a ameaça;**
24. **Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;**
25. **Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis emaliciosos;**
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;**
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;**

i. **FUNCIONALIDADES DE FILTRO DE URL**

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. **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;**
3. **Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;**

4. **Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;**
5. **Possuir pelo menos 60 categorias de URLs;**
6. **Deve possuir a função de exclusão de URLs do bloqueio, por categoria;**
7. **Permitir a customização de página de bloqueio;**
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);**
9. **Além do Explicit Web Proxy, suportar proxy Web transparente;**

j. **FUNCIONALIDADES DE IDENTIFICAÇÃO DE USUÁRIOS**

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. **Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos deusuários;**
3. **Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos deusuários, 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;**
4. **Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;**
5. **Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;**
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 deautenticação residente no firewall (Captive Portal);**
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;**
8. **Deve implementar a criação de grupos customizados de usuários no firewall, baseado ematributos do LDAP/AD;**
9. **Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;**
10. **Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;**

k. **FUNCIONALIDADES DE QOS E TRAFFIC SHAPING**

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. **Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;**
3. **Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;**
4. **Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;**
5. **Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas**

nãolimitado a Skype, Bittorrent, YouTube e Azureus;

6. **Suportar a criação de políticas de QoS e Traffic Shaping por porta;O QoS deve possibilitar a definição de tráfego com banda garantida;**
7. **O QoS deve possibilitar a definição de tráfego com banda máxima;**
8. **O QoS deve possibilitar a definição de fila de prioridade;**
9. **Suportar marcação de pacotes Diffserv, inclusive por aplicação;**
10. **Suportar modificação de valores DSCP para o Diffserv;**
11. **Suportar priorização de tráfego usando informação de Type of Service;**
12. **Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;**

l. **FUNCIONALIDADES DE FILTRO DE DADOS**

1. **Permitir a criação de filtros para arquivos e dados pré-definidos;**
2. **Os arquivos devem ser identificados por extensão e tipo;**
3. **Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF etc.) identificados sobre aplicações (HTTP, FTP, SMTP etc.);**
4. **Suportar identificação de arquivos compactados ou a aplicação de políticas sobre oconteúdo desses tipos de arquivos;**
5. **Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;**
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;**

m. **FUNCIONALIDADES DE ZTNA**

1. **A solução deverá permitir a implementação futura de ZTNA através do licenciamento dos Endpoints, permitindo a ativação das seguintes funcionalidades:**
    1. **Deverá permitir ao administrador a solicitação enforcement de identificação do usuário no login, de modo que o usuário necessite realizar uma confirmação de identidade através de no mínimo:**
        1. **Informação pessoal do sistema operacional;**
        2. **LinkedIn;**
        3. **Google;**
        4. **SalesForce;**
    2. **Deverá permitir aplicar perfis de segurança baseado em status de serviços do endpoint, permitindo que seja atribuído um perfil de acesso para os endpoints baseado em no mínimo:**
        1. **DHCP Server: Atribui um perfil de segurança se o endpoint estiver conectadoa um servidor DCHP específico**
        2. **DNS Server: Atribui um perfil de segurança se o endpoint estiver conectado aum servidor DNS específico**
        3. **Conexão ao Servidor: Atribui um perfil de segurança se o endpoint estiver online e com sua versão atualizada de acordo com o servidor de gerenciamento**
        4. **Local IP/Subnet: Atribui um perfil de segurança se o endpoint estiver em umrange de IPs específico**
        5. **Default Gateway: Atribui um perfil de segurança se o endpoint estiver enviando informações para um gateway de internet específico, permitindo também a configuração de endereço MAC do Gateway.**

6. **Ping Server: Atribui um perfil de segurança se o endpoint conseguir enviar um ping para um servidor específico de rede**
7. **VPN Tunnel: Atribui um perfil de segurança se o endpoint estiver acessando a rede através de um Tunel de VPN, deve ser permitida a escolha de túnel deVPN para cada perfil**

3. **Deve permitir a atribuição de usuários ou grupos de usuários a políticas de acesso;**

n. **GEO LOCALIZAÇÃO**

1. **Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado Pais/Países sejam bloqueados;**
2. **Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;**
3. **Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticasutilizando as mesmas;**

o. **FUNCIONALIDADES DE VPN**

1. **Suportar VPN Site-to-Site e Cliente-To-Site;**
2. **Suportar IPSec VPN;**
3. **Suportar SSL VPN;**
4. **A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;**
5. **A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;**
6. **A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);**
7. **A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);**
8. **Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper,Palo Alto Networks, Fortinet, SonicWall;**
9. **Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;**
10. **Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica dasolução, facilitando o processo de troubleshooting;**
11. **Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentrodo túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;**
12. **Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtrode URL para tráfego dos clientes remotos conectados na VPN SSL;**
13. **Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;**
14. **Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;**
15. **Deverá manter uma conexão segura com o portal durante a sessão;**
16. **O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);**
17. **Deve suportar Auto-Discovery Virtual Private Network (ADVPN)**
18. **Deve suportar agregação de túneis IPSec**
19. **Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPSec**
20. **A VPN IPSec deve suportar Forward Error Correction (FEC)**
21. **Deve suportar TLS 1.3 em VPN SSL**

p. **FUNCIONALIDADES DE SD-WAN**

1. **Deve implementar balanceamento de link por hash do IP de origem;**
2. **Deve implementar balanceamento de link por hash do IP de origem e destino;**

3. **Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definiro percentual de tráfego que será escoado por cada um dos links.**
4. **Deve implementar balanceamento de link por custo configurado do link.**
5. **Deve suportar o balanceamento de, no mínimo, 256 links;**
6. **Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas deVLAN e túneis IPSec**
7. **Deve implementar balanceamento de links sem a necessidade de criação de zonas ou usode instâncias virtuais;**
8. **Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN,monitorados pela checagem de saúde**
9. **Deve suportar Zero-Touch Provisioning**
10. **Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes**
11. **Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência ejitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado**
12. **A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links.**
13. **A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS**
14. **Suportar UDP Hole Punching em arquitetura ADVPN**
15. **A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, paraavaliação mais precisa de links que possuem QoE configurado**
16. **As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações,grupos de usuários, endereço IP de destino e Protocolo.**
17. **Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda depacotes) para que determinado link seja escolhido pelo SD-WAN**
18. **Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima deum link não seja detectada pela checagem de saúde do link**

q. **FUNCIONALIDADES DE WIRELESS CONTROLLER**

1. **Deverá administrar e controlar de maneira centralizada os pontos de acesso wireless domesmo fabricante da solução ofertada;**
2. **Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;**
3. **Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;**
4. **A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;**
5. **O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;**
6. **A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;**
7. **Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;**
8. **O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e**

controlador wireless. Neste modo todos os pacotes devem ser tunelados até o controlador wireless;

9. **Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;**
10. **Deve permitir o gerenciamento de pontos de acesso conectados remotamente através delinks 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;**
11. **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 aomesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;**
12. **A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;**
13. **A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das subredes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados locamente na interface do ponto de acesso;**
14. **A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;**
15. **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;**
16. **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;**
17. **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 deacesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acessonão autorizados;**
18. **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;**
19. **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;**
20. **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;**
21. **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;

22. **A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;**
23. **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;**
24. **A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;**
25. **Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;**
26. **A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;**
27. **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;**
28. **A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie asdecisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;**
29. **A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;**
30. **A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;**
31. **A solução deve implementar técnicas de Call Admission Control para limitar o número dechamadas simultâneas;**
32. **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;**
33. **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 primariamenteem 5GHz através do recurso conhecido como Band Steering;**
34. **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;**
35. **A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestruturawireless, melhorando assim o consumo de Airtime;**
36. **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;

37. **A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;**
38. **A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;**
39. **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;**
40. **A solução deve implementar recurso de web filtering para controle de websites acessadosna rede wireless. Deve possuir uma base de conhecimento para categorização dos sites epermitir configurar quais categorias de sites serão permitidos e bloqueados para cada perfil de usuário e SSID;**
41. **A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de Inspeção SSL 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 degarantia da solução;**
42. **A base de reconhecimento de aplicações através de Inspeção SSL deve identificar com, nomínimo, 1500 (mil e quinhentas) aplicações;**
43. **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 Inspeção SSL;**
44. **A solução deve ainda, através da técnica de Inspeção SSL, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;**
45. **"A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:**
46. **- Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);**
47. **- Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;**
48. **- ASLEAP;**
49. **- Null Probe Response / Null SSID Probe Response;**
50. **- Long Duration;**
51. **- Ataques contra Wireless Bridges;**
52. **- Weak WEP;**
53. **- Invalid MAC OUI."**
54. **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 deauthentication;**
55. **A solução deve implementar mecanismos de proteção contra-ataques do tipo ARP Poisoning na rede wireless;**
56. **A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;**
57. **Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;**
58. **Deve implementar autenticação administrativa através do protocolo RADIUS;**
59. **Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos**

de autenticação: WPA (TKIP) e WPA2 (AES);

60. **Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;**
61. **A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;**
62. **Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição delimite quanto ao número de conexões simultâneas para cada chave criada;**
63. **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;**
64. **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;**
65. **A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;**
66. **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 dosusuários enquanto estes não informar as credenciais válidas para acesso à rede;**
67. **A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;**
68. **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;**
69. **A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;**
70. **A solução deve permitir que a página de autenticação seja hospedada em servidor externo;**
71. **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;**
72. **A solução deve garantir que usuários se autentiquem em captive portal que faça uso de endereço IPv6;**
73. **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;**
74. **Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;**
75. **A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;**
76. **A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;**
77. **A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;**
78. **A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;**

79. **A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;**
80. **A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;**
81. **A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;**
82. **A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;**
83. **A solução deve permitir que softwares de gerenciamento realizem consultas diretamentenos pontos de acesso via protocolo SNMP;**
84. **A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet -like MIB);**
85. **A solução deve permitir a captura de pacotes na rede wireless e exportá-los em arquivos no formato. pcap;**
86. **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;**
87. **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;**
88. **A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;**
89. **A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;**
90. **A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;**
91. **A solução deve possuir ferramentas de diagnósticos e debug;**
92. **A solução deve suportar comunicação com elementos externos através de APIs;**
93. **A solução deverá ser compatível e gerenciar pontos de acesso e switches do mesmo fabricante;**
94. **Os serviços de instalação deverão contemplar:**
    1. **Consultoria para diagramação e arquitetura de rede, de forma que seja sugerida amelhor topologia de acordo com as boas práticas de mercado;**
    2. **Instalação física dos Firewalls;**
    3. **Migração das configurações atuais, quando houver;**
    4. **Configuração de Alta Disponibilidade nos Firewalls e integração com a rede atual;**
    5. **Ativação de recursos no Firewall, como:**
        1. **Antivírus**
        2. **WebFilter**
        3. **Application Control**
        4. **DNS Filter**
        5. **SSL Inspection para navegação web**
        6. **SSL Inspection para servidores publicados**
        7. **IPS**
    6. **Configurações de redes e rotas para os dispositivos de rede;**
    7. **Configurações de autenticação e integração com o Active Directory do ÓRGÃOLICITANTE;**
    8. **Integração dos Switches com os Firewalls Concentradores para gestão centralizada;**

9. **Configuração de domínios de Spanning Tree e Root Bridge;**
10. **Configuração de VLANs;**
11. **Treinamento completo de uso da solução para 6 alunos, de forma teórica e hands-on de no mínimo 12 horas, distribuído em três dias;**
    1. **O treinamento deve conter ementa referente à utilização das soluções de Firewall, Relatoria e logs, e Gerenciamento centralizado, a ser fornecida neste certame;**
12. **O treinamento deverá ser realizado por técnico certificado pelo fabricante, o certificado deverá ser anexado nas documentações de habilitação do ÓRGÃO LICITANTE;**
13. **O ÓRGÃO LICITANTE será responsável por prover o espaço para realização dotreinamento.**

6. **SOLUÇÃO DE RELATORIA E CENTRALIZAÇÃO DE LOGS**
   a. **A solução deve ser baseada em máquina virtual do mesmo fabricante da solução de NGFW e SD-WAN e ter como objetivo a coleta, armazenamento e análise automatizada de registros em modo centralizado de todos os equipamentos a partir de uma única console de administração;**
   b. **Poderá ser entregue em formato appliance virtual, a ser instalado no ambiente de VMs da IFSul;**
   c. **Deverá estar devidamente licenciada para suportar a coleta de, no mínimo, 25 GB de logs diários;**
   d. **Caso a solução seja entregue como appliance virtual, este deve suportar:**
      1. **Deve ser compatível com os hypervisor VMWare ESXi, Hyper-V e KVM;**
      2. **Não deverá existir limite para o número de vCPUs no appliance virtual;**
      3. **Não deverá existir limite para a expansão da memória RAM no appliance virtual;**
      4. **Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;**
      5. **Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;**
      6. **Realizar o backup das configurações para permitir o retorno de uma configuração salva;**
      7. **Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuraçãoem um determinado dia e hora;**
      8. **Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;**
      9. **A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;**
      10. **Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito;**
      11. **Realizar agregação via pontuação, para geração de um veredito sobre máquinas comprometidas na rede e atividades suspeitas;**
      12. **Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes etc.;**
      13. **Deve oferece um portal do cliente fácil de usar, permitindo acesso às capacidades seguras de SD-WAN, como monitoramento e modelos SD-WAN, políticas e objetos, painéis analíticos, visualizações e relatórios, auditoria e recursos adicionais, como documentaçãoe links;**

14. **Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;**
15. **Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;**
16. **Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;**
17. **Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;**
18. **Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;**
19. **Deve possuir mecanismos de remoção automática para logs antigos;**
20. **Permitir importação e exportação de relatórios**
21. **Deve ter a capacidade de criar relatórios no formato HTML, PDF, XML e CSV;**
22. **Deve permitir exportar os logs no formato CSV;**
23. **Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;**
24. **Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores daplataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;**
25. **A solução deve ter relatórios predefinidos;**
26. **Deve permitir o envio automático dos logs para um servidor FTP externo a solução;**
27. **Deve ter a capacidade de personalizar a capa dos relatórios obtidos;**
28. **Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos,incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;**
29. **Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidosem uma lista diferente dos logs relacionados ao tráfego de dados;**
30. **Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas etabelas;**
31. **Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelosrelatórios em tempo real;**
32. **Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;**
33. **Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;**
34. **Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;**
35. **Permitir o envio por e-mail relatórios automaticamente;**
36. **Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;**
37. **Permitir a programação da geração de relatórios, conforme calendário definido peloadministrador;**
38. **Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cadadispositivo gerenciado;**
39. **Deve permitir o uso de filtros nos relatórios;**
40. **Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens,alinhamento, quebras de página, fontes, cores, entre outros;**
41. **Permitir especificar o idioma dos relatórios criados;**
42. **Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais emlogs, gravidade do evento, entre outros;**
43. **Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;**

44. **Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;**
45. **Possibilidade de exibir 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;**
46. **Deve fornecer as informações da quantidade de logs armazenados e as estatisticas do tempo restante armazenado;**
47. **Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;**
48. **Deve permitir visualizar em tempo real os logs recebidos;**
49. **Deve permitir o encaminhamento de log no formato syslog;**
50. **Deve permitir o encaminhamento de log no formato CEF (Common Event Format);**
51. **Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;**
52. **Deve ser capaz de visualizar alertas de surtos e baixar automaticamente manipuladoresde eventos e relatórios relacionados;**
53. **Deve permitir gerar alertas de eventos a partir de logs recebidos;**
54. **Deverá possuir licenciamento perpétuo, incluindo suporte do fabricante pelo períodomínimo de 36 meses;**
55. **Os serviços de instalação deverão contemplar:**
    1. **Implementação da solução em máquina virtual fornecida pelo ÓRGÃO LICITANTE;**
    2. **Integração com a solução de firewall deste certame para envio de logs à solução;**
    3. **Configuração de servidor SMTP para disparo de alertas e relatórios;**
    4. **Criação de 2 relatórios personalizados de acordo com as necessidades de cada campus da IFSul, visando recebimento recorrente de informações que apoiem a tomada de decisão dos campi;**
    5. **Criação de thresholds de alerta;**
    6. **Separação da visibilidade de logs em domínios administrativos por campus;**
    7. **Repasse de conhecimento;**

7. **SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO**
    a. **Deve ser do tipo appliance virtual (VM), a ser instalado em ambiente disponibilizado pelo IFSul;**
    b. **Deve estar licenciado para gerenciar no mínimo 20 dispositivos não sendo necessário licenciar ambos os equipamentos em caso de Cluster HA. Caso seja necessário licenciar gestão para os 2equipamentos do cluster, deverão ser fornecidas licenças para gestão de 40 dispositivos.**
    c. **Deverá suportar sua implementação em:**
        1. **VMware ESXi 6.0+;**
        2. **Microsoft Hyper-V 2008 R2/2012/2012 R2/2016;**
        3. **Citrix XenServer 6.0+ e Open Source Xen 4.1+**
        4. **KVM**
        5. **Nutanix AHV**
        6. **Amazon Web Services (AWS)**
        7. **Microsoft Azure.**
        8. **Google Cloud (GPC)**
        9. **Oracle Cloud Infrastructure (OCI)**
    d. **Não deve possuir limite na quantidade de múltiplas vCPU**
    e. **Não deve possuir limite para suporte a expansão de memória RAM**
    f. **Deve suportar alta disponibilidade**

g. **Funcionalidades gerais:**

1. **Deve ter a capacidade de permitir o provisionamento e o monitoramento da configuração SD-WAN de todos os dispositivos gerenciados a partir de um único console.**
2. **Como parte da visibilidade SD-WAN dos dispositivos gerenciados centralmente, a soluçãodeve ter visibilidade do status do link, desempenho do aplicativo, utilização da largura debanda e conformidade com o SLA objetivo.**
3. **Deve ter a capacidade de automatizar fluxos de trabalho e configurações para dispositivos gerenciados em um único console**
4. **A solução deve ter o recurso de Multi-tenancy para separar os dados de gerenciamento da infraestrutura lógica ou geograficamente e permitir a implantação do zerotouch para orápido provisionamento em massa.**
5. **A solução deve poder executar backups de configuração automáticos em até 5 nós, contendo atualizações de todos os dispositivos gerenciados.**
6. **Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de um único console e exibir sua localização geográfica em um mapa.**
7. **A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança.**
8. **Permitir a integração de trocas e compartilhamento de dados com terceiros por meio do pxGrid, OCI, ESXi.**
9. **Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site dofabricante em listas de end-of-life e end-of-sale;**
10. **O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e APIaberta;**
11. **Permitir acesso concorrente de administradores;**
12. **Possuir interface baseada em linha de comando para administração da solução de gerência**
13. **Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;**
14. **Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;**
15. **Definição de perfis de acesso à console com permissões granulares como: acesso deescrita, acesso de leitura, criação de usuários, alteração de configurações;**
16. **Gerar alertas automáticos via Email**
17. **Gerar alertas automáticos via SNMP**
18. **Gerar alertas automáticos via Syslog**
19. **Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia ehora.**
20. **Deve ser permitido ao administrador transferir os backups para um servidor FTP.**
21. **Deve ser permitido ao administrador transferir os backups para um servidor SCP**
22. **Deve ser permitido ao administrador transferir os backups para um servidor SFTP**
23. **As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante**
24. **Deve ser permitido aos administradores se autenticarem nos servidores de gerênciaatravés de contas de usuários LOCAIS**
25. **Deve ser permitido aos administradores se autenticarem nos servidores de**

gerênciaatravés de base externa TACACS

26. **Deve ser permitido aos administradores se autenticarem nos servidores de gerênciaatravés de usuários de base externa LDAP**
27. **Deve ser permitido aos administradores se autenticarem nos servidores de gerênciaatravés de base externa RADIUS**
28. **Deve ser permitido aos administradores se autenticarem nos servidores de gerênciaatravés de Certificado Digital X.509 (PKI)**
29. **Deve suportar sincronização do relógio interno via protocolo NTP.**
30. **Deve registrar as ações efetuadas por quaisquer usuários**
31. **Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução,na língua portuguesa ou inglesa, com apresentação de boa qualidade.**
32. **Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência**
33. **Deve permitir habilitar e desabilitar, para cada interface de rede da solução de gerência,permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet**
34. **Deve permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado**
35. **A solução de gerência deve permitir criar administradores que tenham acesso à todas as instâncias de virtualização**

h. **Funcionalidades de gestão de firewalls:**
i. **O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;**
j. **O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus eAnti-Spyware;**
k. **O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;**
l. **Permitir localizar quais regras um objeto está sendo utilizado;**
m. **Permitir criação de regras que fiquem ativas em horário definido;**
n. **A solução deve permitir o repositório de assinaturas de antivírus, IPS, filtragem da Web e filtragem de email para otimizar a velocidade e o download centralizado de dispositivos gerenciados**
o. **Deve ter a capacidade de exibir os resultados da auditoria de segurança dos dispositivos gerenciados**
p. **Permitir backup das configurações e rollback de configuração para a última configuração salva;**
q. **Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);**
r. **Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;**
s. **Deve permitir que todos os firewalls sejam controlados de forma centralizada utilizando apenas um servidor de gerência.**
t. **A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.**
u. **A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances.**
v. **Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas.**

w. **Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas elas somente sejam aplicadas após aprovação de outro administrador**

x. **Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos**

1. **Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importadosquando o mesmo for adicionado à solução de gerência**
2. **Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horáriodo sistema e firmware.**
3. **Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos**
4. **Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração**
5. **Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos**
6. **Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência**
7. **Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada**
8. **Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ougrupos de dispositivos**
9. **Deve permitir criar regras de NAT64 e NAT46 de forma centralizada**
10. **Permitir criar regras anti DoS de forma centralizada**
11. **Permitir criar os objetos que serão utilizados nas políticas de forma centralizada**
12. **Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia**
13. **Deve permitir o uso de DDNS em VPNs de forma centralizada**
14. **Deve permitir o gerenciamento de pontos de acesso proprietários de forma centralizada**
15. **Deve permitir o gerenciamento centralizado de switches proprietários**
16. **Deve permitir o gerenciamento centralizado de perfis de segurança de software de endpoint proprietários**
17. **Deverá possuir licenciamento perpétuo, incluindo suporte do fabricante pelo períodomínimo de 36 meses;**
18. **Os serviços de instalação deverão contemplar:**
    1. **Implementação da solução em máquina virtual fornecida pelo ÓRGÃO LICITANTE;**
    2. **Integração com a solução de firewall deste certame para sua gerência centralizada através da solução;**
    3. **Separação da visibilidade através domínios administrativos, permitindo que cada unidade possua visibilidade apenas às informações e gerência do seu câmpus, e a reitoria possua acesso à configuração e gerência de todos os campi;**
    4. **Criação de templates de configuração para aplicação automática de políticas em determinados campi;**
    5. **Repasse de conhecimento;**

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA SUL-RIO-GRANDENSE

Anexo II

PREGÃO ELETRÔNICO Nº 20/2024

PROCESSO Nº 23163.002283.2024-42

MODELO DE PROPOSTA DE PREÇOS

ITEM	DESCRIÇÃO	UNID.	QUANT.	VALOR UNIT. R$	VALOR TOTAL R$

Prazo de validade da proposta: no mínimo de 60 (sessenta) dias a contar da data de abertura da Proposta de Preços.

Declaração: nos preços cotados estão incluídas todas as despesas tais como frete (CIF), impostos, taxas, seguros, tributos e demais encargos de qualquer natureza incidentes sobre o objeto do Pregão.

Licitante: Razão Social, CNPJ, endereço completo, número do telefone, fax e e-mail, bem como, número da conta corrente, nome do banco e agência onde deseja

_____,_____ de 2024.

_____
(assinatura e carimbo da empresa)

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA SUL-RIO-GRANDENSE

Anexo III

PREGÃO ELETRÔNICO Nº 20/2024

PROCESSO Nº 23163.002283.2024-42

ATA DE REGISTRO DE PREÇOS

O Instituto Federal Sul-rio-grandense, com sede na Rua Gonçalves Chaves, 3218, na cidade de Pelotas/RS, inscrito(a) no CNPJ/MF sob o nº 10.729.992/0001-46, neste ato representado pelo Diretor de Planejamento Ernesto Monteiro Perez, nomeado pela Portaria nº 1.734 de 03 de julho de 2017, publicada no Diário Oficial da União de 04 de julho de 2017, inscrito no CPF sob o nº 001.589.000-73, portador da Carteira de Identidade nº 1073533191, considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS, publicada no Diário Oficial da União de __/__/2024 RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no Edital de licitação, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021, no Decreto n.º 11.462, de 31 de março de 2023, e em conformidade com as disposições a seguir:

1. DO OBJETO

1.1. Aquisição de solução de segurança TIC , a ser utilizada nas 15 (quinze) unidades do instituto Federal Sul-rio-grandense, quantidades e exigências estabelecidas neste Edital e seus anexos.

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:

RAZÃO SOCIAL:
CNPJ:
ENDEREÇO:
FONE:
E-MAIL:
REPRESENTANTE:

ITEM do TR	ESPECIFICAÇÃO	MARCA E MODELO	UNID.	QUANT.	VALOR UNITÁRIO R$

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

3. ÓRGÃO(S) GERENCIADOR E PARTICIPANTE(S)

3.1. O Instituto Federal Sul-rio-grandense define o ÓRGÃO GERENCIADOR e os ÓRGÃOS PARTICIPANTES conforme segue:

GERENCIADOR		UG
Reitoria do Instituto Federal Sul-rio-grandense	158126 PARTICIPANTES	UG
Instituto Federal Sul-rio-grandense Campus Bagé		151879
Instituto Federal Sul-rio-grandense Campus Camaquã		151878
Instituto Federal Sul-rio-grandense Campus Charqueadas		158340
Instituto Federal Sul-rio-grandense Campus Gravataí		155143
Instituto Federal Sul-rio-grandense Campus Jaguarão		158126
Instituto Federal Sul-rio-grandense Campus Lajeado		155144
Instituto Federal Sul-rio-grandense Campus Passo Fundo		158338
Instituto Federal Sul-rio-grandense Campus Pelotas		158467
Instituto Federal Sul-rio-grandense Campus Pelotas CAVG		151895
Instituto Federal Sul-rio-grandense Campus Santana do Livramento		154773
Instituto Federal Sul-rio-grandense Campus Sapiranga		155146
Instituto Federal Sul-rio-grandense Campus Sapucaia		158339
Instituto Federal Sul-rio-grandense Campus Venâncio Aires		151964

3.2 São órgãos e entidades públicas participantes do registro de preços em seus quantitativos:

	Item 1	Item 2	Item 3	Item 4	Item 5	Item 6	Item 7
Reitoria	2				4	1	180
Passo Fundo			2				
Santana do Livramento			2				
Sapiranga				2			
Sapucaia				2			
Camaquã			2				
Gravataí				2			
Pelotas		2					
Pelotas-CAVG				2			
Venâncio Aires			2				
Bagé				2			

Charqueadas			2				
Lajeado				2			
Jaguarão				2			

3.3 Endereço dos participantes:

Campus	Endereço
Reitoria	Rua Gonçalves Chaves, nº 3218, Centro. Pelotas/RS. CEP 96015-560;
Instituto Federal Sul-rio-grandense **Campus Bagé**	Av. Leonel de Moura Brizola, 2501 Bairro Pedra Branca - Bagé/RS CEP: 96.418-400
Instituto Federal Sul-rio-grandense **Campus Camaquã**	Rua Ana Gonçalves da Silva, 901 Bairro Olaria Camaquã/RS CEP: 96180-000
Instituto Federal Sul-rio-grandense **Campus Gravataí**	Rua Men de Sá, 800 Bairro Bom Sucesso/Gravataí-RS CEP: 94.135-300;
Instituto Federal Sul-rio-grandense **Campus Jaguarão**	Rua Corredor das Tropas, 801- Jaguarão/RS CEP 96.300-000;
Instituto Federal Sul-rio-grandense **Campus Lajeado**	Rua João Goulart, 2150 - Bairro Olarias Lajeado/RS - CEP 95.900-000;
Instituto Federal Sul-rio-grandense **Campus Passo Fundo**	Estrada Perimetral Leste, 150 Passo Fundo/RS - CEP 99.064-440;
Instituto Federal Sul-rio-grandense **Campus Pelotas**	Praça Vinte de Setembro, 455 Centro - Pelotas/RS - CEP 96.015-360;

Instituto Federal Sul-rio-grandense **Campus Pelotas Visconde da Graça (CAVG)**	Av. Ildelfonso Simões Lopes, 2791 Bairro Arco-Íris - Pelotas/RS - CEP 96.060-290;
Instituto Federal Sul-rio-grandense **Campus Santana do Livramento**	Rua Paul Harris, 410 Centro Santana do Livramento/RS CEP: 97574-360
Instituto Federal Sul-rio-grandense **Campus Sapiranga**	Av. Carlos Gilberto Weiss, 155 Bairro Oeste Sapiranga/RS CEP: 93800-000
Instituto Federal Sul-rio-grandense **Campus Sapucaia do Sul**	Av. Copacabana, 100 - Bairro Piratini - Sapucaia do Sul/RS - CEP 93.216-120;
Instituto Federal Sul-rio-grandense **Campus Santana do Livramento**	Rua Paul Harris, 410 Centro Santana do Livramento/RS CEP: 97574-360
Instituto Federal Sul-rio-grandense **Campus Venâncio Aires**	Av. das Indústrias, 1865 Bairro Universitário Venâncio Aires/RS CEP: 95800-000

4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

4.1. Durante a vigência da ata, os órgãos e as entidades da Administração Pública federal, estadual, distrital e municipal que não participaram do procedimento de IRP poderão aderir à ata de registro de preços na condição de não participantes, observados os seguintes requisitos:

4.1.1. apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

4.1.2. demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei nº 14.133, de 2021; e

4.1.3. consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.

4.2. A autorização do órgão ou entidade gerenciadora apenas será realizada após a aceitação da adesão pelo fornecedor.

4.2.1. O órgão ou entidade gerenciadora poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.

4.3. Após a autorização do órgão ou da entidade gerenciadora, o órgão ou entidade não participante deverá efetivar a aquisição ou a contratação solicitada em até noventa dias, observado o prazo de vigência da ata.

4.4. O prazo de que trata o subitem anterior, relativo à efetivação da contratação, poderá ser prorrogado excepcionalmente, mediante solicitação do órgão ou da entidade não participante aceita pelo órgão ou pela entidade gerenciadora, desde que respeitado o limite temporal de vigência da ata de registro de preços.

4.5. O órgão ou a entidade poderá aderir a item da ata de registro de preços da qual seja integrante, na qualidade de não participante, para aqueles itens para os quais não tenha quantitativo registrado, observados os requisitos do item 4.1.

Dos limites para as adesões

4.6. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o gerenciador e para os participantes.

4.7. O quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o gerenciador e os participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.

4.8. Para aquisição emergencial de medicamentos e material de consumo médico-hospitalar por órgãos e entidades da Administração Pública federal, 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 4.7.

4.9. A adesão à ata de registro de preços por órgãos e entidades da Administração Pública estadual, distrital e municipal poderá ser exigida para fins de transferências voluntárias, não ficando sujeita ao limite de que trata o item 4.7, desde que seja destinada à execução descentralizada de programa ou projeto federal e comprovada a compatibilidade dos preços registrados com os valores praticados no mercado na forma do art. 23 da Lei nº 14.133, de 2021.

Vedação a acréscimo de quantitativos

4.10. É vedado efetuar acréscimos nos quantitativos fixados na ata de registro de preços.

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

5.1. A validade da Ata de Registro de Preços será de 1 (um) ano, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

5.1.1. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida no próprio instrumento contratual e observará no momento da contratação e a cada exercício financeiro a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro.

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

5.2. A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de instrumento contratual, emissão de nota de empenho de despesa, autorização de compra ou outro instrumento hábil, conforme o art. 95 da Lei nº 14.133, de 2021.

5.2.1. O instrumento contratual de que trata o item 5.2. deverá ser assinado no prazo de validade da ata de registro de preços.

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

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

5.4.1. Serão registrados na ata os preços e os quantitativos do adjudicatário, devendo ser observada a possibilidade de o licitante oferecer ou não proposta em quantitativo inferior ao máximo previsto no edital e se obrigar nos limites dela;

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

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

5.4.2.2. Mantiverem sua proposta original.

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

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

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

5.7. A habilitação dos licitantes que comporão o cadastro de reserva a que se refere o item 5.4.2.2 somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

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

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

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

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

5.9.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante ou fornecedor convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela Administração.

5.10. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no 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, observando o item 5.7 e subitens, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

5.12. Na hipótese de nenhum dos licitantes que trata o item 5.4.2.1, aceitar a contratação nos termos do item anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

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

5.12.2. 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 Administração 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, de 2021;

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

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

6.1.3.1. No caso do reajustamento, 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, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado.

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

7.1.2. Na hipótese prevista no item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado e não convocará os licitantes ou fornecedores que tiveram seu registro cancelado.

7.1.3. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora 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, o gerenciador comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços para que avaliem a conveniência e a oportunidade de diligenciarem negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

7.2. Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao gerenciador a

alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.

7.2.1. Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou a planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.

7.2.2. Não hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão ou entidade gerenciadora e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, nos termos do item 9.1, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

7.2.3. Na hipótese de cancelamento do registro do fornecedor, nos termos do item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados, observado o disposto no item 5.7.

7.2.4. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, nos termos do item 9.4, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.

7.2.5. Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto no item 7.2 e no item 7.2.1, o órgão ou entidade gerenciadora atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

7.2.6. O órgão ou entidade gerenciadora comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços sobre a efetiva alteração do preço registrado, para que avaliem a necessidade de alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 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 pelo órgão ou entidade gerenciadora entre os órgãos ou as entidades participantes e não participantes do registro de preços.

8.2. O remanejamento somente poderá ser feito:

8.2.1. De órgão ou entidade participante para órgão ou entidade participante; ou

8.2.2. De órgão ou entidade participante para órgão ou entidade não participante.

8.3. O órgão ou entidade gerenciadora que tiver estimado as quantidades que pretende contratar será considerado participante para efeito do remanejamento.

8.4. Na hipótese de remanejamento de órgão ou entidade participante para órgão ou entidade não participante, serão observados os limites previstos no art. 32 do Decreto nº 11.462, de 2023.

8.5. Competirá ao órgão ou à entidade gerenciadora autorizar o remanejamento solicitado, com a redução do quantitativo inicialmente informado pelo órgão ou pela entidade participante, desde que haja prévia anuência do órgão ou da entidade que sofrer redução dos quantitativos informados.

8.6. Caso o remanejamento seja feito entre órgãos ou entidades dos Estados, do Distrito Federal ou de Municípios distintos, caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente do remanejamento dos itens.

8.7. Na hipótese da compra centralizada, não havendo indicação pelo órgão ou pela entidade gerenciadora, dos quantitativos dos participantes da compra centralizada, nos termos do item 8.3, a distribuição das quantidades para a execução descentralizada será por meio do remanejamento.

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

9.1. O registro do fornecedor será cancelado pelo gerenciador, quando o fornecedor:

9.1.1. Descumprir as condições da ata de registro de preços, sem motivo justificado;

9.1.2. Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;

9.1.3. Não aceitar manter seu preço registrado, na hipótese prevista no artigo 27, § 2º, do Decreto nº 11.462, de 2023; ou

9.1.4. Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021.

9.1.4.1. Na hipótese de aplicação de sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021, caso a penalidade aplicada ao fornecedor não ultrapasse o prazo de vigência da ata de registro de preços, o órgão ou a entidade gerenciadora poderá, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

9.2. O cancelamento de registros nas hipóteses previstas no item 9.1 será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos os princípios do contraditório e da ampla defesa.

9.3. Na hipótese de cancelamento do registro do fornecedor, o órgão ou a entidade gerenciadora poderá convocar os licitantes que compõem o cadastro de reserva, observada a ordem de classificação.

9.4. O cancelamento dos preços registrados poderá ser realizado pelo gerenciador, em determinada ata de registro de preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:

9.4.1. Por razão de interesse público;

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

9.4.3. Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado tornar-se superior ou inferior ao preço registrado, nos termos do artigos 26, § 3º e 27, § 4º, ambos do Decreto nº 11.462, de 2023.

10. DAS PENALIDADES

10.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas *no edital ou no aviso de contratação direta*.

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

10.2. É da competência do gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço (art. 7º, inc. XIV, do Decreto nº 11.462, de 2023), exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos ou entidade participante, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 8º, inc. IX, do Decreto nº 11.462, de 2023).

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

11. CONDIÇÕES GERAIS

11.1. As condições gerais de execução do objeto, tais como os prazos para entrega e recebimento, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, ANEXO II ao Edital.

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

Local e data

Assinaturas

Representante legal do órgão gerenciador e representante(s) legal(is) do(s) fornecedor(s) registrado(s)