FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

SEÇÃO DE ADMINISTRAÇÃO FINANÇAS E CONTRATOS - SIn/SeAFC/SIn

Rod. Washington Luís km 235 - SP-310, s/n - Bairro Monjolinho, São Carlos/SP, CEP 13565-905

Telefone: (16) 3351-8146 - http://www.ufscar.br

Edital nº 1/2021/SIn/SeAFC/SIn

EDITAL DE LICITAÇÃO

UASG: 156403
PREGÃO ELETRÔNICO Nº 03/2021
PROCESSO SEI N° 23112.017883/2021-68

Torna-se público, para conhecimento dos interessados, que a Fundação Universidade Federal de São Carlos, por meio da Secretaria Geral de Informática, sediada à Rodovia Washington Luís Km 235 SP-310, CEP 13565-905, São Carlos-SP, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, com critério de julgamento MENOR PREÇO, nos termos da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto nº 7.746, de 05 de junho de 2012, do Decreto 9.507, de 21 de setembro de 2018, do Decreto nº 7.174, de 12 de maio de 2010, do Decreto nº 7892, de 23 de janeiro e 2013, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, da Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010, das Instruções Normativas SEGES/MP nº 05, de 26 de maio de 2017 e nº 03, de 26 de abril de 2018, da Lei Complementar n° 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto n° 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993, e as exigências estabelecidas neste Edital.

Data da sessão: 16/11/2021

Horário: 09:00 horas (Horário de Brasília)

Local: Portal de Compras do Governo Federal – https://www.gov.br/compras/pt-br/sistemas/comprasnet-siasg

1. **DO OBJETO**

1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para aquisição da solução de firewall para a Universidade Federal de São Carlos, com 5 (cinco) anos de suporte, garantia, licenças de proteção e instalação, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será dividida em um único grupo formada por 5 (cinco) itens, devendo o licitante ofertar proposta para todos os itens que o compõe. **Bens e serviços que compõem a solução:**

Grupo	ID	CÓDIGO CATMAT/CATSER	DESCRIÇÃO	QUANTIDADE	UNIDADE
1	1	CATMAT - 133132	FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 05 ANOS - SÃO CARLOS COM SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO.	1	unidade
	2	CATMAT -133132	FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 05 ANOS - ARARAS E SOROCABA COM SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO.	2	unidade
	3	CATMAT -133132	FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 05 ANOS - LAGOA DO SINO COM SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO.	1	unidade
	4	CATSER - 27464	SOFTWARE DE GESTÃO CENTRALIZADA COM SUPORTE E GARANTIA DE 05 ANOS	1	unidade
	5	CATSER - 16837	TREINAMENTO OFICIAL DE FIREWALL	4	unidade

1.3. O critério de julgamento adotado será o menor preço do grupo, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

1.4. Cada serviço ou produto do lote deverá estar discriminado em itens separados nas propostas de preço, de modo a permitir a identificação do seu preço individual na composição do preço global, e eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam as normas técnicas brasileiras - NTB.

1.5. Havendo divergências entre a descrição do objeto constante neste Edital e a descrição do objeto constante no site Portal de Compras do Governo Federal, “SIASG” ou Nota de Empenho, prevalecerá, sempre, a descrição constante do Termo de Referência, Anexo deste Edital.

2. **DOS RECURSOS ORÇAMENTÁRIOS**

2.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento da União para o exercício de 2021, na classificação abaixo:

Gestão/Unidade: 15266/156403

Fonte: 8100000000

Programa de Trabalho: 170326

Elemento de Despesa: 449052-37, 449040-06 e 449040-03

PI: N20RKG01SCN

3. **DO CREDENCIAMENTO**

3.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

3.2. O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio https://www.gov.br/compras/pt-br/sistemas/comprasnet-siasg,, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.

3.3. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

3.4. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assumir 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 da senha, ainda que por terceiros.

3.5. É de responsabilidade do cadastrado 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 que se tornem desatualizados.

3.5.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

4. DA PARTICIPAÇÃO NO PREGÃO

4.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.

4.1.1. Os licitantes deverão utilizar o certificado digital para acesso ao Sistema.

4.2. Não poderão participar desta licitação os interessados:

4.2.1. proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente em especial o art. 34 da Instrução Normativa SEGES/MPDG nº 03, de 26 de abril de 2018;

4.2.2. que não atendam às condições deste Edital e seu(s) anexo(s);

4.2.3. estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

4.2.4. que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

4.2.5. que estejam sob falência, concurso de credores, concordata ou insolvência, em processo de dissolução ou liquidação;

4.2.6. entidades empresariais que estejam reunidas em consórcio;

4.2.7. organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário);

4.2.8. instituições sem fins lucrativos (parágrafo único do art. 12 da Instrução Normativa/SEGES nº 05/2017)

4.2.8.1. É admissível a participação de organizações sociais, qualificadas na forma dos arts. 5º a 7º da Lei 9.637/1998, desde que os serviços objeto desta licitação se insiram entre as atividades previstas no contrato de gestão firmado entre o Poder Público e a organização social (Acórdão nº 1.406/2017- TCU-Plenário), mediante apresentação do Contrato de Gestão e dos respectivos atos constitutivos.

4.2.9. sociedades cooperativas, considerando a vedação contida no art. 10 da Instrução Normativa SEGES/MP nº 5, de 2017, bem como o disposto no Termo de Conciliação firmado entre o Ministério Público do Trabalho e a AGU.

4.3. Nos termos do art. 5º do Decreto nº 9.507, de 2018, é vedada a contratação de pessoa jurídica na qual haja administrador ou sócio com poder de direção, familiar de:

a) detentor de cargo em comissão ou função de confiança que atue na área responsável pela demanda ou contratação; ou

b) de autoridade hierarquicamente superior no âmbito do órgão contratante.

4.3.1. Para os fins do disposto neste item, considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau (Súmula Vinculante/STF nº 13, art. 5º, inciso V, da Lei nº 12.813, de 16 de maio de 2013 e art. 2º, inciso III, do Decreto n.º 7.203, de 04 de junho de 2010);

4.4. Nos termos do art. 7° do Decreto n° 7.203, de 2010, é vedada, ainda, a utilização, na execução dos serviços contratados, de empregado da futura Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança neste órgão contratante.

4.5. Como condição para participação no Pregão, a licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:

4.5.1. que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49;

4.5.1.1. nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;

4.5.1.2. 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.

4.5.2. que está ciente e concorda com as condições contidas no Edital e seus anexos.

4.5.3. que cumpre plenamente os requisitos de habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

4.5.4. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

4.5.5. que 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;

4.5.6. que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.

4.5.7. que não possui, em sua cadeia produtiva, 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;

4.5.8. que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

4.5.9. que cumpre os requisitos do Decreto n. 7.174, de 2010, estando apto a usufruir dos critérios de preferência.

4.5.9.1. a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto no Decreto nº 7.174, de 2010.

4.6. A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

5.2. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

5.3. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

5.4. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

5.5. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.6. Até a abertura da sessão, os licitantes poderão retirar ou substituir as propostas apresentadas.

5.7. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

5.8. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances

6. **DO PREENCHIMENTO DA PROPOSTA**

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

6.1.1. Valor unitário e total do item;

6.1.2. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência.

6.2. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

6.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços, apurados mediante o preenchimento do modelo de Planilha de Custos e Formação de Preços, conforme anexo deste Edital;

6.3.1. A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1° do artigo 57 da Lei n° 8.666, de 1993.

6.3.2. Caso o eventual equívoco no dimensionamento dos quantitativos se revele superior às necessidades da contratante, a Administração deverá efetuar o pagamento seguindo estritamente as regras contratuais de faturamento dos serviços demandados e executados, concomitantemente com a realização, se necessário e cabível, de adequação contratual do quantitativo necessário, com base na alínea "b" do inciso I do art. 65 da Lei n. 8.666/93 e nos termos do art. 63, §2° da IN SEGES/MPDG n. 5/2017.

6.4. A empresa é a única responsável pela cotação correta dos encargos tributários. Em caso de erro ou cotação incompatível com o regime tributário a que se submete, serão adotadas as orientações a seguir:

6.4.1. cotação de percentual menor que o adequado: o percentual será mantido durante toda a execução contratual;

6.4.2. cotação de percentual maior que o adequado: o excesso será suprimido, unilateralmente, da planilha e haverá glosa, quando do pagamento, e/ou redução, quando da repactuação, para fins de total ressarcimento do débito.

6.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses, devendo o licitante ou contratada apresentar ao pregoeiro ou à fiscalização, a qualquer tempo, comprovação da adequação dos recolhimentos, para os fins do previsto no subitem anterior.

6.6. Independentemente do percentual de tributo inserido na planilha, no pagamento dos serviços, serão retidos na fonte os percentuais estabelecidos na legislação vigente.

6.7. 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 os serviços 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.

6.8. 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.

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

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

6.10.1. 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.

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

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

7.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital ou contenham vícios insanáveis, ilegalidades, ou não apresentem as especificações exigidas no Termo de Referência.

7.2.1. Também será desclassificada a proposta que identifique o licitante.

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

7.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

7.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

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

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

7.5.1. O lance deverá ser ofertado pelo valor Total do item.

7.6. Os licitantes poderão oferecer lances sucessivos, contendo cada lance no máximo 02 (duas) casas decimais, relativas à parte dos centavos, sob a pena de exclusão do lance, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

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

7.8. 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 100 (cem) reais

7.9. Será adotado para o envio de lances no pregão eletrônico o Modo de Disputa “Aberto e Fechado”, em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

7.10. 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.

7.11. 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.

7.11.1. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

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

7.12.1. 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, *observando-se, após, o item anterior.*.

7.13. 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.

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

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

7.16. 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.

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

7.18. O Critério de julgamento adotado será o menor preço, conforme definido neste Edital e seus anexos.

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

7.20. 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 LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

7.21. 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.

7.22. A melhor classificada nos termos do item 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.

7.23. Caso a microempresa ou a empresa de pequeno porte melhor 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.

7.24. 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.

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

7.26. Havendo eventual empate entre propostas, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens produzidos:

7.26.1. prestados por empresas brasileiras;

7.26.2. prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.26.3. prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

7.27. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas ou os lances empatados.

7.28. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das prevista deste Edital.

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

7.28.2. O pregoeiro solicitará ao licitante melhor classificado que, no prazo de 02 (duas) horas, 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.

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

7.30. Será assegurado o direito de preferência previsto no seu artigo 3º, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010.

7.30.1. As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

8. DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

8.1. Encerrada a etapa de negociação, 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 parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 10.024/2019.

8.2. A análise da exequibilidade da proposta de preços deverá ser realizada com o auxílio da Planilha de Custos e Formação de Preços, a ser preenchida pelo licitante em relação à sua proposta final, conforme anexo deste Edital.

8.3. A Planilha de Custos e Formação de Preços deverá ser encaminhada pelo licitante exclusivamente via sistema, no prazo de 2 horas, contado da solicitação do Pregoeiro, com os respectivos valores adequados ao lance vencedor e será analisada pelo Pregoeiro no momento da aceitação do lance vencedor.

8.4. A inexequibilidade dos valores referentes a itens isolados da Planilha de Custos e Formação de Preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais.

8.5. Será desclassificada a proposta ou o lance vencedor, nos termos do item 9.1 do Anexo VII-A da In SEGES/MPDG n. 5/2017, que:

8.5.1. não estiver em conformidade com os requisitos estabelecidos neste edital;

8.5.2. contenha vício insanável ou ilegalidade;

8.5.3. não apresente as especificações técnicas exigidas pelo Termo de Referência;

8.5.4. apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018-TCU – Plenário), desconto menor do que o mínimo exigido, ou que apresentar preço manifestamente inexequível.

8.5.4.1. Quando o licitante não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:

8.5.4.1.1 for insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

8.5.4.1.2 apresentar um ou mais valores da planilha de custo que sejam inferiores àqueles fixados em instrumentos de caráter normativo obrigatório, tais como leis, medidas provisórias e convenções coletivas de trabalho vigentes.

8.6. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MPDG N. 5, de 2017, para que a empresa comprove a exequibilidade da proposta.

8.7. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela análise da planilha de custos, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

8.8. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

8.8.1. Na hipótese de necessidade de suspensão de sessão pública para a realização de diligências, com vista ao saneamento das propostas, a sessão pública

somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata.

8.9. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de 02 (duas) horas, sob pena de não aceitação da proposta.

8.9.1. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

8.9.2. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se as destacam-se as planilhas de custo readequadas com o valor final ofertado.

8.10. Todos os dados informados pelo licitante em sua planilha deverão refletir com fidelidade os custos especificados e a margem de lucro pretendida.

8.11. O Pregoeiro analisará a compatibilidade dos preços unitários apresentados na Planilha de Custos e Formação de Preços com aqueles praticados no mercado em relação aos insumos e também quanto aos salários das categorias envolvidas na contratação;

8.12. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo licitante, no prazo indicado pelo Pregoeiro, desde que não haja majoração do preço.

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

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

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

8.14. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

8.15. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.

8.16. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

9. DA HABILITAÇÃO

9.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);

c) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa e Inelegibilidade mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php).

d) Lista de Inidôneos e o Cadastro Integrado de Condenações por Ilícitos Administrativos - CADICON, mantidos pelo Tribunal de Contas da União - TCU;

9.1.1. Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas das alíneas “b”, “c” e “d” acima pela Consulta Consolidada de Pessoa Jurídica do TCU (https://certidoesapf.apps.tcu.gov.br/)

9.1.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

9.1.2.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

9.1.2.1.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

9.1.2.1.2. O licitante será convocado para manifestação previamente à sua desclassificação.

9.1.3. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

9.1.4. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.2. Caso atendidas as condições de participação, a habilitação do licitante será verificada por meio do SICAF, nos documentos por ele abrangidos, em relação à habilitação jurídica, à regularidade fiscal e à qualificação econômica financeira, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

9.2.1. O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o terceiro dia útil anterior à data prevista para recebimento das propostas;

9.2.2. É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

9.2.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

9.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de **no prazo de duas (02) horas**, sob pena de inabilitação.

9.4. 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.

9.5. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

9.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

9.6.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

9.7. Ressalvado o disposto no item 6.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação:

9.8. **Habilitação jurídica:**

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

9.8.2. Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

9.8.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

9.8.4. inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

9.8.5. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

9.8.6. decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

9.8.7. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva;

9.9. **Regularidade fiscal e trabalhista:**

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

9.9.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

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

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

9.9.5. prova de inscrição no cadastro de contribuintes municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.9.6. prova de regularidade com a Fazenda Municipal do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

9.9.7. caso o licitante seja considerado isento dos tributos municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Municipal do seu domicílio ou sede, ou outra equivalente, na forma da lei;

9.10.**Qualificação Econômico-Financeira:**

9.10.1. certidão negativa de falência expedida pelo distribuidor da sede do licitante;

9.10.2. balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

9.10.2.1.no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

9.10.2.2.é admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

9.10.3. comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidospela aplicação das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

9.10.4. As empresas, , que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10% (dez por cento) do valor total estimado da contratação ou do item pertinente.

9.11. **Qualificação Técnica:**

9.11.1. Os critérios de Qualificação Técnica estão previstos no Termo de Referência, anexo a este edital.

9.12. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

9.13. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

9.13.1. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

9.14. Caso a proposta mais vantajosa seja ofertada por microempresa, empresa de pequeno porte ou sociedade cooperativa equiparada, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

9.15. A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

9.16. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

9.17. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

9.18. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.19. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

10. **DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA**

10.1 A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de 02 (duas) horas, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

10.1.1. ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.

10.1.2. *apresentar a planilha de custos e formação de preços, devidamente ajustada ao lance vencedor, em conformidade com o modelo anexo a este instrumento convocatório.*

10.1.3. conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.

10.2. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

10.2.1. Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

10.3. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

10.3.1. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

10.4. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

10.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante

10.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

11. **DOS RECURSOS**

11.1. O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal e trabalhista da licitante, se for o caso, concederá o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

11.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

11.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

11.2.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

11.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três (03) dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três (03) dias, que começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

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

11.4. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

12. **DA REABERTURA DA SESSÃO PÚBLICA**

12.1. A sessão pública poderá ser reaberta:

12.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

12.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

12.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

12.2.1. A convocação se dará por meio do sistema eletrônico ("chat"), e-mail, de acordo com a fase do procedimento licitatório.

12.2.2. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

13. **DA ADJUDICAÇÃO E HOMOLOGAÇÃO**

13.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

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

14. **DA GARANTIA DE EXECUÇÃO**

14.1. Será exigida a prestação de garantia na presente contratação, conforme regras constantes do Termo de Referência.

15. **DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE**

15.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

15.2. O adjudicatário terá o **prazo de 05 (cinco) dias úteis**, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

15.2.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite da Adjudicatária, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado ou aceito **no prazo de 05 (cinco) dias úteis**, a contar da data de seu recebimento.

15.2.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

15.3. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

15.3.1. referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;

15.3.2. a contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

15.3.3. a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.

15.4. O prazo de vigência da contratação é de 12 meses, prorrogável conforme previsto no Termo de Referência - item 10.

15.5. Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

15.5.1. Nos casos em que houver necessidade de assinatura do instrumento de contrato, e o fornecedor não estiver inscrito no SICAF, este deverá proceder ao seu cadastramento, sem ônus, antes da contratação.

15.5.2. Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no edital e anexos.

15.6. Na assinatura do contrato, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da ata de registro de preços.

15.7. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato ou a ata de registro de preços.

16. DO REAJUSTAMENTO EM SENTIDO GERAL

16.1. As regras acerca do reajustamento em sentido geral do valor contratual são as estabelecidas no Termo de Referência, anexo a este Edital.

17. DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

17.1. Os critérios de recebimento e aceitação do objeto e de fiscalização estão previstos no Termo de Referência, anexo a este Edital.

18. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

18.1. As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência, anexo a este Edital.

19. DO PAGAMENTO

19.1. As regras acerca do pagamento são as estabelecidas no Termo de Referência, anexo a este Edital.

20. DAS SANÇÕES ADMINISTRATIVAS

20.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

20.1.1. Não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

20.1.2. Apresentar documentação falsa;

20.1.3. Deixar de entregar os documentos exigidos no certame;

20.1.4. Ensejar o retardamento da execução do objeto;

20.1.5. Não mantiver a proposta;

20.1.6. Cometer fraude fiscal;

20.1.7. Comportar-se de modo inidôneo.

20.2. As sanções do item acima também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente.

20.3. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

20.4. O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

20.4.1. Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;
20.4.2. Multa de 20% (vinte por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;
20.4.3. 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;
20.4.4. Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;
20.4.5. 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;

20.5. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

20.6. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

20.7. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

20.8. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

20.9. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

20.10 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

20.11. 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.

20.12. As penalidades serão obrigatoriamente registradas no SICAF.

20.13. As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.

21. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

21.1. Até 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.

21.2. A impugnação poderá ser realizada por forma eletrônica, pelo e-mail, compras@sin.ufscar.br ou por petição dirigida ou protocolada no endereço Rodovia Washington Luís Km235 SP-310, Cep 13565-905, São Carlos-SP , Secretária de Informática.

21.3. Caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos, decidir sobre a impugnação no prazo de até dois (02) dias úteis contados da data de recebimento da impugnação.

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

21.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.

21.6. O pregoeiro responderá aos pedidos de esclarecimentos no prazo de dois dias úteis, contado da data de recebimento do pedido, e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos.

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

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

21.8. As informações e/ou esclarecimentos serão prestados pelo Pregoeiro através do site https://www.gov.br/compras/pt-br/, ficando todos os licitantes obrigados a acessá-lo para obtenção das informações prestadas pelo Pregoeiro.

21.9. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.

22. DAS DISPOSIÇÕES GERAIS

22.1. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

22.2. 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.

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

22.4.22.5. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

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

22.6. 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.

22.7. 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.

22.8. 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.

22.9. 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.

22.10. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as do Termo de Referência;

22.11.O Edital está disponibilizado, na íntegra, no endereço eletrônico https://www.gov.br/compras/pt-br/, e também no http://www.sin.ufscar.br, ademais, ainda poderão ser lidos e/ou obtidos na Secretaria de Informática do Campus São Carlos - Rodovia Washington Luís km 235- São Carlos-SP, nos dias úteis, no horário das 8 horas às 12 horas e das 14 horas às 17h45, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

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

1. ANEXO I - Termo de Referência
2. ANEXO II – Minuta de Termo de Contrato;

ASSINATURAS E CIÊNCIAS

Nome Completo	Cargo/Função	Lotação
Erick Lazaro Melo	Analista de TI / Secretario Geral de Informática	Secretaria Geral de Informática
Antonio Aparecido Rosalem	Analista de TI / Pregoeiro	Seção de Administração Finanças e Contratos

Documento assinado eletronicamente por **Antonio Aparecido Rosalem**, **Analista de Tecnologia da Informação**, em 26/10/2021, às 15:03, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Erick Lazaro Melo**, **Secretário(a) Geral**, em 26/10/2021, às 15:05, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufscar.br/autenticacao, informando o código verificador **0521240** e o código CRC **30C65175**.

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENADORIA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO - CITI/SIn

Rod. Washington Luís km 235 - SP-310, s/n - Bairro Monjolinho, São Carlos/SP, CEP 13565-905

Telefone: (16) 33518204 - http://www.ufscar.br

TR nº 7/2021/CITI/SIn

Termo de Referência (TR)

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
14/10/2021	1.0	Primeira versão do TR	Marcio R Falvo
26/10/2021	2.0	Correções referente ao parecer nº 00126/2021/CONS/PFFUFSCAR/PGF/AGU	Equipe de planejamento

1. OBJETO DA CONTRATAÇÃO

Aquisição da solução de firewall para a Universidade Federal de São Carlos - UFSCar com 5 anos de suporte, garantia, licenças de proteção e instalação.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. Bens e serviços que compõem a solução

Grupo	ID	CÓDIGO CATMAT/CATSER	DESCRIÇÃO	QUANTIDADE	UNIDADE
1	1	CATMAT - 133132	FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 05 ANOS - SÃO CARLOS COM SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO.	1	unidade
	2	CATMAT -133132	FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 05 ANOS - ARARAS E SOROCABA COM SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO.	2	unidade
	3	CATMAT -133132	FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 05 ANOS - LAGOA DO SINO COM SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO.	1	unidade
	4	CATSER - 27464	SOFTWARE DE GESTÃO CENTRALIZADA COM SUPORTE E GARANTIA DE 05 ANOS	1	unidade
	5	CATSER - 16837	TREINAMENTO OFICIAL DE FIREWALL	4	unidade

3. JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

A adoção de uma nova solução de firewall na UFSCar é necessária para assegurar a continuidade da segurança na comunicação de dados tanto externamente (internet), quanto entre os ativos de tecnologia dentro da rede dos Campus, melhorar o nível de qualidade e segurança dos serviços das aplicações internas da Universidade e impedir o uso da infraestrutura de rede da Universidades para fins adversos ao objetivo institucional (Exemplo: na utilização da capacidade computacional da instituição para fins criminosos, mineração ou armazenamento e acesso a conteúdo ilícito, ou originar ataques cibernéticos, ou ser vítima de ataques cibernéticos).

Outros pontos que fortalecem a necessidade de uma nova solução de firewall é a necessidade do cumprimento legal. O primeiro ponto é instituído pelo Marco Civil da Internet - Lei nº 12.965/2014, onde os logs das conexões de acesso a internet devem ser retidos pelo período de 1 ano. O segundo ponto é a necessidade da garantia da integridade e da confidencialidade dos dados dos usuários em conformidade com a Lei Geral de Proteção de Dados nº 13.709/2018. Neste sentido, temos a **necessidade de aquisição de solução de firewall, com visão de médio prazo - 5 anos, para os quatro (4) Campi da UFSCar - São Carlos, Araras, Sorocaba e Lagoa do Sino.**

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**PDI <2018-2022>**
1	Objetivo estratégico 4.5: Proteção e segurança de dados e transformação digital a) Atendimento aos requisitos da LGPD e as políticas do PDA até 2022.

ALINHAMENTO AO PDTIC <2019-2021>			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
INF4	Definir políticas e regras de controle de acesso a redes	**M1**	Padronizar regras bloqueio do firewall
		M2	Melhorar política de controle de acesso para serviços e sistemas
		M3	Unificar método de autenticação para serviços e sistemas

ALINHAMENTO AO PLANO ANUAL DE CONTRATAÇÕES	
ID	**PAC <2021>**
1	3.2 Serviços - Item 10: Informática - Suporte Técnico (Software, e quipamentos); 3.5 Solução de TIC - Item 1: Serviços de Garantia de Equipamentos de TIC.

3.3. Estimativa da demanda

3.3.1. A aquisição da solução de firewall de próxima geração é detalhada pelos itens de 1 a 5 da tabela desse Termo de Referência constante no item 2.1. Os quantitativos foram definidos para atender as necessidades de cada um dos quatro Campus UFSCar provendo a gestão unificada da solução, o que impacta diretamente na gestão do serviço. Além disso, foi considerado a garantia de 5 anos devido a criticidade da solução ser alta por tratar-se de item ligado a segurança e dar suporte no cumprimento das legislações vigentes, como: Marco Civil da Internet - Lei nº 12.965/2014 e Lei Geral de Proteção de Dados nº 13.709/2018.

3.3.2. O escopo dos itens que fazem parte da solução serão descritos a seguir:

3.3.2.1. **Grupo 1: Item 1 - FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 05 ANOS - SÃO CARLOS**

Características técnicas mínimas:
1. A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, *spywares* e *malwares* desconhecidos (*Zero Day*), IPS, filtro de URL e recursos de

VPN;

2. O *hardware* e *software* que executem as funcionalidades de proteção de rede devem ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

3. O equipamento fornecido deve ser próprio para montagem em rack 19", incluindo *kit* tipo trilho para adaptação, se necessário, e cabos de alimentação;

4. Deve possuir *throughput* de, no mínimo, 7.8 (sete ponto oito) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;

5. Deve possuir *throughput* de, no mínimo, 3.7 (três ponto sete) Gbps com as funcionalidades de controle de aplicação, IPS, antivírus e *anti-spyware* habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os *throughput* aferidos com tráfego HTTP ou *blend* de protocolos definidos pelo fabricante como tráfego real;

6. Deve suportar, no mínimo, 2.000.000 (dois milhões) de conexões simultâneas;

7. Deve suportar, no mínimo, 90.000 (noventa mil) de novas conexões por segundo;

8. Deve possuir, no mínimo, 12 (doze) interfaces físicas de rede de 1 Gbps do tipo RJ-45;

9. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1/10 Gbps do tipo SFP/SFP+. Caso o equipamento não possua interfaces do tipo SPF/SFP+ serão aceitos equipamentos que possuam, no mínimo, 8 (oito) interfaces físicas de rede de 1 Gbps do tipo SFP mais 8 (oito) interfaces físicas de rede de 10 Gbps do tipo SFP+;

10. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 40 Gbps do tipo QSFP+;

11. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento;

12. Deve possuir, no mínimo, 1 (uma) interface física dedicada para o recurso de alta disponibilidade;

13. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;

14. Para as 4 interfaces de 40Gbps - QSFP+ deve acompanhar os *transceivers* de 40G para conexões acima de 100m. Também deve acompanhar 2 transceivers de 40G para conexões acima de 100m adicionais, totalizando 6 *transceivers* de 40G para conexões acima de 100m.

15. Para as 8 interfaces de rede de 1/10 Gbps - SFP/SFP+ ou 10 Gbps - SFP+ deve acompanhar os *transceivers* de 10G para conexões acima de 100m. Caso as interfaces sejam apenas de 10 Gbps - SFP+, para as 8 interfaces do tipo 1Gbps - SFP também deve acompanhar os *transceivers* de 1G para conexões superiores a 100m.

16. Deve possuir disco do tipo *Solid State Divre* (SSD) de, no mínimo, 240 (duzentos e quarenta) GB de armazenamento do sistema operacional e registro de *logs*;

17. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento;

18. Deve suportar, no mínimo, 2.000 (dois mil) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;

19. Deve suportar, no mínimo, 2.000 (dois mil) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;

20. Deve possuir suporte a criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 1.000 (hum mil) VLANs;

21. Deve implementar o protocolo LLDP – Link Layer Discovery Protocol;

22. Deve possuir o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um *link* agrupado virtualmente (LAG – Link Aggregation Group);

23. Deve possuir o recurso de NAT – *Network Address Translation* nas modalidades de NAT estático 1 para 1, NAT dinâmico 1 para vários e NAT dinâmico vários para vários. Este recurso deve ser aplicado tanto para o endereço de origem quanto para endereço de destino. Deve possuir também NAT64 para tradução entre endereços IPv6 e IPv4 e NPTv6 (*Network Prefix Translation*) para tradução de um prefixo IPv6 para outro prefixo IPv6 prevenindo problemas de roteamento assimétrico;

24. Deve suportar a criação de rotas estáticas e os protocolos de roteamento estático e dinâmico RIPv2, OSPFv2 e OSPFv3 incluindo OSPF *graceful restart* e BGP;

25. Deve implementar o protocolo ECMP – *Equal Cost Multiple Path* para balanceamento de carga entre *links* baseados no *hash* do endereço IP de origem, no *hash* do endereço IP de origem e de destino, pela técnica conhecida como *round-robin* e com base no peso ou prioridade atribuído a cada *link*. Deve suportar o balanceamento entre, no mínimo 4 (quatro) *links*;

26. Deve permitir o envio de *logs* para sistemas de monitoração externos utilizando o padrão *syslog*, bem como o envio de forma segura através do protocolo SSL/TLS;

27. Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo;

28. Deve implementar controle por políticas/regras de *firewall* capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego;

29. A identificação do país deve ser através do código do país, por exemplo, BR, USA, UK, RUS, etc e também através de geolocalização possibilitando a criação de regiões geográficas;

30. Deve permitir configurar o agendamento das políticas/regras de *firewall* para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;

31. Deve possuir a capacidade para realizar a decriptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A decriptografia deve ser realizada com base em políticas/regras de acordo com a origem e destino do tráfego;

32. Deve possuir recurso de QoS – *Quality of Service* com suporte a DSCP – *Differentiated Services Code Point*. Deve permitir também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda devem ser baseadas no endereço IP de origem e destino, no usuário e na aplicação;

33. Deve possuir a capacidade de reconhecer, no mínimo, 3.000 (três mil) aplicações diferentes tais como redes sociais, compartilhamento de arquivos, e-mail, atualização de *softwares*, acesso remoto, VoIP, áudio e vídeo, *peer-to-peer*, sistemas de mensagem instantânea, etc, sendo esta uma lista não exaustiva;

34. O reconhecimento da aplicação se dará, independentemente de porta e protocolo, através de, no mínimo, os seguintes métodos: baseado na assinatura da aplicação conhecida pelo fabricante da solução de *firewall*, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado;

35. Deve permitir a criação de assinaturas personalizadas para o reconhecimento de aplicações proprietárias na própria interface gráfica do equipamento sem a necessidade de intervenção do fabricante;

36. Deve permitir a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permitir a troca de mensagens de texto e bloquear a transferência de arquivos por dentro da aplicação;

37. Deve permitir bloquear sessões TCP que utilizarem variações do *three-way handshake* como *four-way* e o *five-way split handshake*, prevenindo assim possíveis tráfegos maliciosos;

38. Deve permitir bloquear conexões que contenham dados no *payload* dos pacotes TCP SYN e TCP SYN-ACK durante o *three-way handshake*;

39. A solução de *firewall* deve possuir funcionalidades de IPS, antivírus e *anti-spyware* que permita o bloqueio de vulnerabilidades e *exploits* conhecidos e proteção contra vírus e *spywares* baseado em assinaturas de ameaças conhecidas;

40. Deve ser possível a criação de assinaturas customizadas de ameaças;

41. Deve permitir realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3. Será permitido o uso de *appliance* externo para o bloqueio de vírus caso a solução de *firewall* ofertada não realize nativamente a inspeção em algum dos protocolos solicitados;

42. Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;

43. Deve possuir proteção contra ataques de negação de serviço (DoS) capaz de impedir ataques de SYN *Flood*, ICMP *Flood,* UDP *Flood*, etc e deve também bloquear *port scans*, bloquear ataques de *buffer overflow* e identificar e bloquear comunicação com *botnets*;

44. Para cada ameaça detectada pela solução deve ser realizado o registro nos *logs* do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego);

45. A solução de *firewall* deve possuir funcionalidade para análise de *malwares* não conhecidos (*Malware Zero Day*) onde o dispositivo envia o arquivo de forma automática para análise na "*cloud*" ou em um *appliance* instalado na rede local onde o arquivo será executado e simulado em um ambiente controlado (*sandbox*);

46. Caso seja fornecido um *appliance* local para análise de malwares não conhecidos ele deve possuir, no mínimo, 28 (vinte e oito) ambientes controlados (*sandbox*) independentes para execução simultânea de arquivos suspeitos;

47. Caso seja necessário licença de sistema operacional e *software* para execução de arquivos no ambiente controlado (*sandbox*) as mesmas devem ser fornecidas em sua totalidade para o seu perfeito funcionamento;

48. O resultado da análise de *malwares* não conhecidos deve ter a capacidade de categorizar o arquivo analisado como, no mínimo, um arquivo malicioso, um arquivo não malicioso e um arquivo não malicioso, mas com características indesejáveis que deixam o sistema operacional lento ou que alteram parâmetros do sistema;

49. A análise de *malwares* não conhecidos deve ser realizada em arquivos trafegados na internet através dos protocolos HTTP, HTTPS e FTP bem como em arquivos trafegados entre servidores de arquivos utilizando o protocolo SMB. A análise também deve ser realizada em arquivos anexos em *e-mails* e *links* HTTP e HTTPS presentes no corpo de *e-mails* trafegados utilizando os protocolos SMTP e POP3. A análise do *link* HTTP e HTTPS presente no corpo do *e-mail* deve identificar se o *website* é um hospedeiro de *exploits* ou atividade de *phishing*;

50. Deve suportar a análise dos arquivos em ambientes controlados (*sandbox*) com, no mínimo, os sistemas operacionais MS Windows XP, MS Windows 7, MS Windows 10, MacOS e Linux;

51. A análise de *malwares* não conhecidos em ambiente controlado (*sandbox*) deve ser realizada em arquivos tipo executáveis, DLLs, arquivos compactados RAR e 7-ZIP, arquivos do pacote MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos PDF, arquivos JAVA (.jar e class), arquivos DMG e PKG, arquivos ELF e arquivos APK;

52. Deve atualizar a base de assinaturas para bloqueio dos *malwares* identificados no ambiente controlado (*sandbox*) dentro de, no máximo, 5 (cinco) minutos;

53. A solução de *firewall* deve possuir funcionalidade de filtro URL que permita a criação de políticas/regras para controle do acesso a *websites* baseado em categorias de URL devendo o fabricante da solução disponibilizar a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL devem ser com base no usuário e grupos de usuários e por endereços IP e faixas de endereços IP;

54. A funcionalidade de filtro URL deve possuir categoria específica para classificar domínios recém registrados com menos de 30 dias;

55. Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;

56. Deve permitir a customização da página de bloqueio exibida ao usuário quando o mesmo tentar realizar um acesso a um *website* pertencente a uma categoria de URLs bloqueada;

57. Deve possuir recurso para proteger contra o roubo de credenciais de usuário e senha, identificadas através da integração com o *Active Directory*, submetidas em sites não corporativos. Deve ser possível definir em quais *websites* é permitido ou bloqueado o envio das credenciais baseado na categoria de URL a qual o *website* pertencer. Caso o usuário tente submeter suas credenciais de usuário e senhas pertencentes ao *Active Directory* em um *website* não autorizado deve ser exibido no *web browser* do mesmo uma página de bloqueio informando que o uso de tais credenciais no *website* específico não está autorizado;

58. A solução de *firewall* deve possuir recurso que permita bloquear a transferência de arquivos baseado na extensão dos mesmos e também definir por qual aplicação a transferência do arquivo está bloqueada, por exemplo, bloquear a transferência de arquivos .exe através de *web browser.* Deve permitir bloquear, no mínimo, arquivo com as extensões .exe, .bat, .dll, .pif e .torrent;

59. A solução de *firewall* deve possuir integração com LDAP, MS *Active Directoy* e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas/regras baseadas por usuários e grupo de usuários;

60. A integração com MS *Active Directory* para identificação dos usuários da rede deve ser realizada sem a necessidade de instalação de um agente no Controlador de Domínio e nem nas estações dos usuários;

61. A solução de *firewall* deve possuir recurso de portal de autenticação prévia (*Captive Portal*) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de *software* cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;

62. A solução de *firewall* deve possuir o recurso de VPN – *Virtual Private Network* dos tipos *site-to-site* e *client-to-site* e suportar IPSEc – *Internet Protocol Security* e SSL – *Secure Sockets Layer*;

63. O recurso de VPN IPSec deve suportar os algoritmos de criptografia 3DES, AES 128, AES 192 e AES 256, os algoritmos de autenticação MD5 e SHA 1, o algoritmo IKEv1 e IKEv2 e os algoritmos de troca de chaves Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 e Grupo 14 e suportar também a autenticação através de certificados IKE PKI;

64. O recurso de VPN SSL deve permitir que o usuário remoto se conecte através de um *software* cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo;

65. Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS *Active Directory*, TACACS+, RADIUS, SAML e através de base de usuários local no equipamento da solução de firewall. Deve suportar também a autenticação via certificado e OTP – One Time Password;

66. Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional MS Windows 8, MS Windows 10 e MacOS;

67. A solução de firewall deve possuir console de gerenciamento do equipamento acessada através de interface gráfica *web* permitindo realizar as configurações da solução como criar e administrar as políticas/regras de firewall e controle de aplicações, criar e administrar as políticas de IPS, antivírus e *anti-spyware*, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de logs de eventos e demais configurações;

68. Deve suportar a autenticação dos usuários administradores que se conectam à interface de gerenciamento do equipamento via LDAP, MS *Active Directory*, RADIUS e através de base de usuários local no equipamento da solução de firewall;

69. Deve ser possível criar perfis de acesso à interface de gerenciamento com permissões granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros;

70. Deve permitir realizar o *backup* das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;

71. A interface de gerenciamento do equipamento deve possuir recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regras (*shadowing*) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve possuir também recurso para análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão da mesma para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente. É permitido o uso de *appliance* externo para realização da análise das políticas;

72. Deve ser possível através de interface de gerenciamento do equipamento a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuário específicos incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados;

73. Deve ser possível gerar relatório de visibilidade e uso das aplicações do tipo SaaS – *Software as a Service* mostrando os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso a aplicação SaaS e o consumo da aplicação SaaS pelo usuário;

74. Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU;

75. Deve ser possível configurar o envio de alertas do sistema via *e-mail*;

76. Deve suportar o monitoramento via SNMPv3;

77. O sistema operacional a ser instalado no equipamento que compõe a solução deverá ser fornecido em sua versão mais atualizada, não sendo aceito sistema operacional de uso genérico;

78. Por cada equipamento que compõe a solução de segurança, entende-se o *hardware* e as licenças de softwares necessárias para o seu funcionamento;

79. Na data do certame, nenhum dos equipamentos ofertados poderão estar listados no site do fabricante em listas de *end-of-life* e *end-of-sale*;

80. Durante o período de vigência do contrato de garantia todos os componentes da solução de *firewall*, incluindo o equipamento, o sistema operacional do mesmo, as licenças necessárias para atender as funcionalidades e recursos solicitados, os softwares clientes de VPN e demais itens necessários para o perfeito funcionamento devem estar cobertos por garantia e suporte técnico do fabricante da solução em caso de problema;

81. A solução de *firewall* deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e dos demais software e das assinaturas de proteção da solução.

Serviço de Instalação:

1. A contratada deverá prestar serviços de instalação e configuração do item 1 do grupo 1, que compreendem, entre outros, os seguintes procedimentos:
    1. Reunião de alinhamento para criação do escopo do projeto previamente a instalação;
    2. Instalação física de todos os equipamentos (*hardware*) e licenças (*softwares*) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);
    3. Análise da topologia e arquitetura da rede, considerando todos os equipamentos já existentes e instalados;
    4. Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;
    5. Migração das regras de *firewall* existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;
    6. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;
    7. Configuração do sistema de firewall, VPN, IPS, Filtro URL, Antivírus e a*nti-malware* de acordo com as exigências levantadas;
2. Toda a configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos *firewall* afim de garantir a melhor eficiência da solução durante o período de vigência das licenças;
3. Configuração do sistema de gerenciamento centralizado considerando adição dos novos *appliance*;
4. Repasse de informação das configurações realizadas no formato *hands-on* de 4 horas para a equipe responsável pelo projeto por parte da contratante após validação da migração;

3.3.2.2. **Grupo 1: Item 2 - FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 05 ANOS - ARARAS E SOROCABA**

Características técnicas mínimas:

1. A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, *spywares* e *malwares* desconhecidos (*Zero Day*), IPS, filtro de URL e recursos de VPN;
2. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

3. O equipamento deve ser fornecido com *kit* que permita a sua montagem em *rack* 19";
4. Deve possuir *throughput* de, no mínimo, 1.6 (um ponto seis) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;
5. Deve possuir *throughput* de, no mínimo, 850 (oitocentos e cinquenta) Mbps com as funcionalidades de controle de aplicação, IPS, antivírus e *anti-spyware* habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os *throughput* aferidos com tráfego HTTP ou *blend* de protocolos definidos pelo fabricante como tráfego real;
6. Deve suportar, no mínimo, 190.000 (cento e noventa mil) conexões simultâneas;
7. Deve suportar, no mínimo, 35.000 (trinta e cinco mil) novas conexões por segundo;
8. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1 Gbps do tipo RJ-45;
9. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento;
10. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;
11. Deve possuir, no mínimo, 128 (cento e vinte e oito) GB de armazenamento interno para o sistema operacional e registro de *logs*;
12. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento;
13. Deve suportar, no mínimo, 800 (oitocentos) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;
14. Deve suportar, no mínimo, 200 (duzentos) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;
15. Deve possuir suporte a criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 1.000 (hum mil) VLANs;
16. Deve implementar o protocolo LLDP – *Link Layer Discovery Protocol*;
17. Deve possuir o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um *link* agrupado virtualmente (LAG – *Link Aggregation Group*);
18. Deve possuir o recurso de NAT – *Network Address Translation* nas modalidades de NAT estático 1 para 1, NAT dinâmico 1 para vários e NAT dinâmico vários para vários. Este recurso deve ser aplicado tanto para o endereço de origem quanto para endereço de destino. Deve possuir também NAT64 para tradução entre endereços IPv6 e IPv4 e NPTv6 (*Network Prefix Translation*) para tradução de um prefixo IPv6 para outro prefixo IPv6 prevenindo problemas de roteamento assimétrico;
19. Deve suportar a criação de rotas estáticas e os protocolos de roteamento estático e dinâmico RIPv2, OSPFv2 e OSPFv3 incluindo OSPF *graceful restart* e BGP;
20. Deve implementar o protocolo ECMP – *Equal Cost Multiple Path* para balanceamento de carga entre *links* baseados no *hash* do endereço IP de origem, no *hash* do endereço IP de origem e de destino, pela técnica conhecida como *round-robin* e com base no peso ou prioridade atribuído a cada *link*. Deve suportar o balanceamento entre, no mínimo 4 (quatro) *links*;
21. Deve permitir o envio de *logs* para sistemas de monitoração externos utilizando o padrão *syslog*, bem como o envio de forma segura através do protocolo SSL/TLS;
22. Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo;
23. Deve implementar controle por políticas/regras de *firewall* capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego;
24. A identificação do país deve ser através do código do país, por exemplo, BR, USA, UK, RUS, etc e também através de geolocalização possibilitando a criação de regiões geográficas;
25. Deve permitir configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;
26. Deve possuir a capacidade para realizar a decriptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A decriptografia deve ser realizada com base em políticas/regras de acordo com a origem e destino do tráfego;
27. Deve possuir recurso de QoS – *Quality of Service* com suporte a DSCP – *Differentiated Services Code Point*. Deve permitir também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda devem ser baseadas no endereço IP de origem e destino, no usuário e na aplicação;
28. Deve possuir a capacidade de reconhecer, no mínimo, 3.000 (três mil) aplicações diferentes tais como redes sociais, compartilhamento de arquivos, *e-mail*, atualização de *softwares*, acesso remoto, VoIP, áudio e vídeo, *peer-to-peer*, sistemas de mensagem instantânea, etc, sendo esta uma lista não exaustiva;
29. O reconhecimento da aplicação se dará, independentemente de porta e protocolo, através de, no mínimo, os seguintes métodos: baseado na assinatura da aplicação conhecida pelo fabricante da solução de *firewall*, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado;
30. Deve permitir a criação de assinaturas personalizadas para o reconhecimento de aplicações proprietárias na própria interface gráfica do equipamento sem a necessidade de intervenção do fabricante;
31. Deve permitir a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permitir a troca de mensagens de texto e bloquear a transferência de arquivos por dentro da aplicação;
32. Deve permitir bloquear sessões TCP que utilizarem variações do *three-way handshake* como *four-way* e o *five-way split handshake*, prevenindo assim possíveis tráfegos maliciosos;
33. Deve permitir bloquear conexões que contenham dados no *payload* dos pacotes TCP SYN e TCP SYN-ACK durante o *three-way handshake*;
34. A solução de firewall deve possuir funcionalidades de IPS, antivírus e *anti-spyware* que permita o bloqueio de vulnerabilidades e *exploits* conhecidos e proteção contra vírus e *spywares* baseado em assinaturas de ameaças conhecidas;
35. Deve ser possível a criação de assinaturas customizadas de ameaças;
36. Deve permitir realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3. Será permitido o uso de *appliance* externo para o bloqueio de vírus caso a solução de firewall ofertada não realize nativamente a inspeção em algum dos protocolos solicitados;
37. Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;
38. Deve possuir proteção contra ataques de negação de serviço (DoS) capaz de impedir ataques de SYN *Flood*, ICMP *Flood*, UDP *Flood*, etc e deve também bloquear *port scans*, bloquear ataques de buffer overflow e identificar e bloquear comunicação com *botnets*;

39. Para cada ameaça detectada pela solução deve ser realizado o registro nos *logs* do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego);

40. A solução de firewall deve possuir funcionalidade para análise de *malwares* não conhecidos (*Malware Zero Day*) onde o dispositivo envia o arquivo de forma automática para análise na "*cloud*" ou em um *appliance* instalado na rede local onde o arquivo será executado e simulado em um ambiente controlado (*sandbox*);

41. Caso seja fornecido um *appliance* local para análise de *malwares* não conhecidos ele deve possuir, no mínimo, 28 (vinte e oito) ambientes controlados (*sandbox*) independentes para execução simultânea de arquivos suspeitos;

42. Caso seja necessário licença de sistema operacional e *software* para execução de arquivos no ambiente controlado (*sandbox*) as mesmas devem ser fornecidas em sua totalidade para o seu perfeito funcionamento;

43. O resultado da análise de *malwares* não conhecidos deve ter a capacidade de categorizar o arquivo analisado como, no mínimo, um arquivo malicioso, um arquivo não malicioso e um arquivo não malicioso, mas com características indesejáveis que deixam o sistema operacional lento ou que alteram parâmetros do sistema;

44. A análise de *malwares* não conhecidos deve ser realizada em arquivos trafegados na internet através dos protocolos HTTP, HTTPS e FTP bem como em arquivos trafegados entre servidores de arquivos utilizando o protocolo SMB. A análise também deve ser realizada em arquivos anexos em *e-mails* e *links* HTTP e HTTPS presentes no corpo de *e-mails* trafegados utilizando os protocolos SMTP e POP3. A análise do *link* HTTP e HTTPS presente no corpo do *e-mail* deve identificar se o *website* é um hospedeiro de *exploits* ou atividade de *phishing*;

45. Deve suportar a análise dos arquivos em ambientes controlados (*sandbox*) com, no mínimo, os sistemas operacionais MS Windows XP, MS Windows 7, MS Windows 10, MacOS e Linux;

46. A análise de *malwares* não conhecidos em ambiente controlado (*sandbox*) deve ser realizada em arquivos tipo executáveis, DLLs, arquivos compactados RAR e 7-ZIP, arquivos do pacote MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos PDF, arquivos JAVA (.jar e class), arquivos DMG e PKG, arquivos ELF e arquivos APK;

47. Deve atualizar a base de assinaturas para bloqueio dos *malwares* identificados no ambiente controlado (sandbox) dentro de, no máximo, 5 (cinco) minutos;

48. A solução de *firewall* deve possuir funcionalidade de filtro URL que permita a criação de políticas/regras para controle do acesso a *websites* baseado em categorias de URL devendo o fabricante da solução disponibilizar a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL devem ser com base no usuário e grupos de usuários e por endereços IP e faixas de endereços IP;

49. A funcionalidade de filtro URL deve possuir categoria específica para classificar domínios recém registrados com menos de 30 dias;

50. Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;

51. Deve permitir a customização da página de bloqueio exibida ao usuário quando o mesmo tentar realizar um acesso a um *website* pertencente a uma categoria de URLs bloqueada;

52. Deve possuir recurso para proteger contra o roubo de credenciais de usuário e senha, identificadas através da integração com o *Active Directory*, submetidas em sites não corporativos. Deve ser possível definir em quais *websites* é permitido ou bloqueado o envio das credenciais baseado na categoria de URL a qual o *website* pertencer. Caso o usuário tente submeter suas credenciais de usuário e senhas pertencentes ao *Active Directory* em um *website* não autorizado deve ser exibido no *web browser* do mesmo uma página de bloqueio informando que o uso de tais credenciais no *website* específico não está autorizado;

53. A solução de *firewall* deve possuir recurso que permita bloquear a transferência de arquivos baseado na extensão dos mesmos e também definir por qual aplicação a transferência do arquivo está bloqueada, por exemplo, bloquear a transferência de arquivos .exe através de *web browser*. Deve permitir bloquear, no mínimo, arquivo com as extensões .exe, .bat, .dll, .pif e .torrent;

54. A solução de *firewall* deve possuir integração com LDAP, MS *Active Directoy* e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas/regras baseadas por usuários e grupo de usuários;

55. A integração com MS *Active Directory* para identificação dos usuários da rede deve ser realizada sem a necessidade de instalação de um agente no Controlador de Domínio e nem nas estações dos usuários;

56. A solução de *firewall* deve possuir recurso de portal de autenticação prévia (*Captive Portal*) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de *software* cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;

57. A solução de *firewall* deve possuir o recurso de VPN – *Virtual Private Network* dos tipos *site-to-site* e *client-to-site* e suportar IPSEc – *Internet Protocol Security* e SSL – *Secure Sockets Layer*;

58. O recurso de VPN IPSec deve suportar os algoritmos de criptografia 3DES, AES 128, AES 192 e AES 256, os algoritmos de autenticação MD5 e SHA 1, o algoritmo IKEv1 e IKEv2 e os algoritmos de troca de chaves Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 e Grupo 14 e suportar também a autenticação através de certificados IKE PKI;

59. O recurso de VPN SSL deve permitir que o usuário remoto se conecte através de um software cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo;

60. Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS Active Directory, TACACS+, RADIUS, SAML e através de base de usuários local no equipamento da solução de firewall. Deve suportar também a autenticação via certificado e OTP – *One Time Password*;

61. Deve ser disponibilizado o *software* cliente de VPN do mesmo fabricante da solução de *firewall* ofertada compatível para instalação em computadores com sistema operacional MS Windows 8, MS Windows 10 e MacOS;

62. A solução de *firewall* deve possuir console de gerenciamento do equipamento acessada através de interface gráfica *web* permitindo realizar as configurações da solução como criar e administrar as políticas/regras de firewall e controle de aplicações, criar e administrar as políticas de IPS, antivírus e *anti-spyware*, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de *logs* de eventos e demais configurações;

63. Deve suportar a autenticação dos usuários administradores que se conectam à interface de gerenciamento do equipamento via LDAP, MS *Active Directory*, RADIUS e através de base de usuários local no equipamento da solução de *firewall*;

64. Deve ser possível criar perfis de acesso à interface de gerenciamento com permissões granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros;

65. Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;

66. A interface de gerenciamento do equipamento deve possuir recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regras (*shadowing*) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve possuir também recurso para análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão da mesma para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente. É permitido o uso de *appliance* externo para realização da análise das políticas;

67. Deve ser possível através de interface de gerenciamento do equipamento a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças

vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuário específicos incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados;

68. Deve ser possível gerar relatório de visibilidade e uso das aplicações do tipo SaaS – *Software as a Service* mostrando os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso a aplicação SaaS e o consumo da aplicação SaaS pelo usuário;
69. Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU;
70. Deve ser possível configurar o envio de alertas do sistema via *e-mail*;
71. Deve suportar o monitoramento via SNMPv3;
72. O sistema operacional a ser instalado no equipamento que compõe a solução deverá ser fornecido em sua versão mais atualizada, não sendo aceito sistema operacional de uso genérico;
73. Por cada equipamento que compõe a solução de segurança, entende-se o *hardware* e as licenças de *softwares* necessárias para o seu funcionamento;
74. Na data do certame, nenhum dos equipamentos ofertados poderão estar listados no site do fabricante em listas de *end-of-life* e *end-of-sale*;
75. Durante o período de vigência do contrato de garantia todos os componentes da solução de *firewall*, incluindo o equipamento, o sistema operacional do mesmo, as licenças necessárias para atender as funcionalidades e recursos solicitados, os *softwares* clientes de VPN e demais itens necessários para o perfeito funcionamento devem estar cobertos por garantia e suporte técnico do fabricante da solução em caso de problema;
76. A solução de *firewall* deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais *software* e das assinaturas de proteção da solução.

Serviço de Instalação:

1. A contratada deverá prestar serviços de instalação e configuração do item 2 do grupo 1, que compreendem, entre outros, os seguintes procedimentos:
    1. Reunião de alinhamento para criação do escopo do projeto previamente a instalação;
    2. Instalação física de todos os equipamentos (*hardware*) e licenças (*softwares*) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante. Quando aplicável, considerar instalação em modo alta disponibilidade (ativo/passivo);
    3. Análise da topologia e arquitetura da rede, considerando todos os equipamentos já existentes e instalados;
    4. Análise do acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;
    5. Migração das regras de *firewall* existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;
    6. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;
    7. Configuração do sistema de *firewall*, VPN, IPS, Filtro URL, antivírus e *anti-malware* de acordo com as exigências levantadas;
2. Toda a configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos *firewall* afim de garantir a melhor eficiência da solução durante o período de vigência das licenças;
3. Configuração do sistema de gerenciamento centralizado considerando adição dos novos *appliance*;
4. Repasse de informação das configurações realizadas no formato *hands-on* de 4 horas para a equipe responsável pelo projeto por parte da contratante após validação da migração;

3.3.2.3. **Grupo 1: Item 3 - FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 05 ANOS - LAGOA DO SINO**

Características técnicas mínimas:

1. A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, *spywares* e *malwares* desconhecidos (*Zero Day*), IPS, filtro de URL e recursos de VPN;
2. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
3. Deve possuir *throughput* de, no mínimo, 1 (um) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;
4. Deve possuir *throughput* de, no mínimo, 500 (quinhentos) Mbps com as funcionalidades de controle de aplicação, IPS, antivírus e *anti-spyware* habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os *throughput* aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;
5. Deve suportar, no mínimo, 60.000 (setenta mil) conexões simultâneas;
6. Deve suportar, no mínimo, 11.000 (onze mil) novas conexões por segundo;
7. Deve possuir, no mínimo, 7 (sete) interfaces físicas de rede de 1 Gbps do tipo RJ-45;
8. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento;
9. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;
10. Deve possuir, no mínimo, 64 (sessenta e quatro) GB de armazenamento interno para o sistema operacional e registro de logs;

11. Deve possuir fonte de alimentação elétrica capaz de operar entre 120 à 240 VAC;

12. Deve suportar, no mínimo, 200 (duzentos) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;

13. Deve suportar, no mínimo, 200 (duzentos) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;

14. Deve possuir suporte a criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 1.000 (hum mil) VLANs;

15. Deve implementar o protocolo LLDP – *Link Layer Discovery Protocol*;

16. Deve possuir o recurso de agregação de *links* conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um *link* agrupado virtualmente (LAG – *Link Aggregation Group*);

17. Deve possuir o recurso de NAT – *Network Address Translation* nas modalidades de NAT estático 1 para 1, NAT dinâmico 1 para vários e NAT dinâmico vários para vários. Este recurso deve ser aplicado tanto para o endereço de origem quanto para endereço de destino. Deve possuir também NAT64 para tradução entre endereços IPv6 e IPv4 e NPTv6 (*Network Prefix Translation*) para tradução de um prefixo IPv6 para outro prefixo IPv6 prevenindo problemas de roteamento assimétrico;

18. Deve suportar a criação de rotas estáticas e os protocolos de roteamento estático e dinâmico RIPv2, OSPFv2 e OSPFv3 incluindo OSPF *graceful restart* e BGP;

19. Deve implementar o protocolo ECMP – *Equal Cost Multiple Path* para balanceamento de carga entre *links* baseados no hash do endereço IP de origem, no hash do endereço IP de origem e de destino, pela técnica conhecida como *round-robin* e com base no peso ou prioridade atribuído a cada *link*. Deve suportar o balanceamento entre, no mínimo 4 (quatro) *links*;

20. Deve permitir o envio de *logs* para sistemas de monitoração externos utilizando o padrão *syslog*, bem como o envio de forma segura através do protocolo SSL/TLS;

21. Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo;

22. Deve implementar controle por políticas/regras de *firewall* capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego;

23. A identificação do país deve ser através do código do país, por exemplo, BR, USA, UK, RUS, etc e também através de geolocalização possibilitando a criação de regiões geográficas;

24. Deve permitir configurar o agendamento das políticas/regras de *firewall* para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;

25. Deve possuir a capacidade para realizar a decriptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A decriptografia deve ser realizada com base em políticas/regras de acordo com a origem e destino do tráfego;

26. Deve possuir recurso de QoS – *Quality of Service* com suporte a DSCP – *Differentiated Services Code Point*. Deve permitir também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda devem ser baseadas no endereço IP de origem e destino, no usuário e na aplicação;

27. Deve possuir a capacidade de reconhecer, no mínimo, 3.000 (três mil) aplicações diferentes tais como redes sociais, compartilhamento de arquivos, e-mail, atualização de softwares, acesso remoto, VoIP, áudio e vídeo, *peer-to-peer*, sistemas de mensagem instantânea, etc, sendo esta uma lista não exaustiva;

28. O reconhecimento da aplicação se dará, independentemente de porta e protocolo, através de, no mínimo, os seguintes métodos: baseado na assinatura da aplicação conhecida pelo fabricante da solução de *firewall*, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado;

29. Deve permitir a criação de assinaturas personalizadas para o reconhecimento de aplicações proprietárias na própria interface gráfica do equipamento sem a necessidade de intervenção do fabricante;

30. Deve permitir a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permitir a troca de mensagens de texto e bloquear a transferência de arquivos por dentro da aplicação;

31. Deve permitir bloquear sessões TCP que utilizarem variações do *three-way handshake* como *four-way* e o *five-way split handshake*, prevenindo assim possíveis tráfegos maliciosos;

32. Deve permitir bloquear conexões que contenham dados no payload dos pacotes TCP SYN e TCP SYN-ACK durante o three-way handshake;

33. A solução de *firewall* deve possuir funcionalidades de IPS, antivírus e *anti-spyware* que permita o bloqueio de vulnerabilidades e *exploits* conhecidos e proteção contra vírus e *spywares* baseado em assinaturas de ameaças conhecidas;

34. Deve ser possível a criação de assinaturas customizadas de ameaças;

35. Deve permitir realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3. Será permitido o uso de *appliance* externo para o bloqueio de vírus caso a solução de *firewall* ofertada não realize nativamente a inspeção em algum dos protocolos solicitados;

36. Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;

37. Deve possuir proteção contra ataques de negação de serviço (DoS) capaz de impedir ataques de SYN *Flood*, ICMP *Flood*, UDP *Flood*, etc e deve também bloquear *port scans*, bloquear ataques de *buffer overflow* e identificar e bloquear comunicação com *botnets*;

38. Para cada ameaça detectada pela solução deve ser realizado o registro nos *logs* do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego);

39. A solução de *firewall* deve possuir funcionalidade para análise de *malwares* não conhecidos (*Malware Zero Day*) onde o dispositivo envia o arquivo de forma automática para análise na "cloud" ou em um appliance instalado na rede local onde o arquivo será executado e simulado em um ambiente controlado (*sandbox*);

40. Caso seja fornecido um *appliance* local para análise de *malwares* não conhecidos ele deve possuir, no mínimo, 28 (vinte e oito) ambientes controlados (*sandbox*) independentes para execução simultânea de arquivos suspeitos;

41. Caso seja necessário licença de sistema operacional e *software* para execução de arquivos no ambiente controlado (*sandbox*) as mesmas devem ser fornecidas em sua totalidade para o seu perfeito funcionamento;

42. O resultado da análise de *malwares* não conhecidos deve ter a capacidade de categorizar o arquivo analisado como, no mínimo, um arquivo malicioso, um arquivo não malicioso e um arquivo não malicioso, mas com características indesejáveis que deixam o sistema operacional lento ou que alteram parâmetros do sistema;

43. A análise de malwares não conhecidos deve ser realizada em arquivos trafegados na internet através dos protocolos HTTP, HTTPS e FTP bem como em arquivos trafegados entre servidores de arquivos utilizando o protocolo SMB. A análise também deve ser realizada em arquivos anexos em *e-mails* e *links* HTTP e HTTPS presentes no corpo de *e-mails* trafegados utilizando os protocolos SMTP e POP3. A análise do *link* HTTP e HTTPS presente no corpo do *e-mail* deve identificar se o *website* é um hospedeiro de *exploits* ou atividade de *phishing*;

44. Deve suportar a análise dos arquivos em ambientes controlados (*sandbox*) com, no mínimo, os sistemas operacionais MS Windows XP, MS Windows 7, MS

Windows 10, MacOS e Linux;

45. A análise de *malwares* não conhecidos em ambiente controlado (*sandbox*) deve ser realizada em arquivos tipo executáveis, DLLs, arquivos compactados RAR e 7-ZIP, arquivos do pacote MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos PDF, arquivos JAVA (.jar e class), arquivos DMG e PKG, arquivos ELF e arquivos APK;

46. Deve atualizar a base de assinaturas para bloqueio dos malwares identificados no ambiente controlado (*sandbox*) dentro de, no máximo, 5 (cinco) minutos;

47. A solução de *firewall* deve possuir funcionalidade de filtro URL que permita a criação de políticas/regras para controle do acesso a *websites* baseado em categorias de URL devendo o fabricante da solução disponibilizar a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL devem ser com base no usuário e grupos de usuários e por endereços IP e faixas de endereços IP;

48. A funcionalidade de filtro URL deve possuir categoria específica para classificar domínios recém registrados com menos de 30 dias;

49. Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;

50. Deve permitir a customização da página de bloqueio exibida ao usuário quando o mesmo tentar realizar um acesso a um *website* pertencente a uma categoria de URLs bloqueada;

51. Deve possuir recurso para proteger contra o roubo de credenciais de usuário e senha, identificadas através da integração com o *Active Directory*, submetidas em sites não corporativos. Deve ser possível definir em quais websites é permitido ou bloqueado o envio das credenciais baseado na categoria de URL a qual o *website* pertencer. Caso o usuário tente submeter suas credenciais de usuário e senhas pertencentes ao *Active Directory* em um *website* não autorizado deve ser exibido no *web browser* do mesmo uma página de bloqueio informando que o uso de tais credenciais no *website* específico não está autorizado;

52. A solução de *firewall* deve possuir recurso que permita bloquear a transferência de arquivos baseado na extensão dos mesmos e também definir por qual aplicação a transferência do arquivo está bloqueada, por exemplo, bloquear a transferência de arquivos .exe através de *web browser*. Deve permitir bloquear, no mínimo, arquivo com as extensões .exe, .bat, .dll, .pif e .torrent;

53. A solução de *firewall* deve possuir integração com LDAP, MS *Active Directoy* e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas/regras baseadas por usuários e grupo de usuários;

54. A integração com MS *Active Directory* para identificação dos usuários da rede deve ser realizada sem a necessidade de instalação de um agente no Controlador de Domínio e nem nas estações dos usuários;

55. A solução de *firewall* deve possuir recurso de portal de autenticação prévia (*Captive Portal*) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de *software* cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;

56. A solução de *firewall* deve possuir o recurso de VPN – *Virtual Private Network* dos tipos *site-to-site* e *client-to-site* e suportar IPSEc – *Internet Protocol Security* e SSL – *Secure Sockets Layer*;

57. O recurso de VPN IPSec deve suportar os algoritmos de criptografia 3DES, AES 128, AES 192 e AES 256, os algoritmos de autenticação MD5 e SHA 1, o algoritmo IKEv1 e IKEv2 e os algoritmos de troca de chaves Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 e Grupo 14 e suportar também a autenticação através de certificados IKE PKI;

58. O recurso de VPN SSL deve permitir que o usuário remoto se conecte através de um *software* cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo;

59. Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS *Active Directory*, TACACS+, RADIUS, SAML e através de base de usuários local no equipamento da solução de *firewall*. Deve suportar também a autenticação via certificado e OTP – *One Time Password*;

60. Deve ser disponibilizado o *software* cliente de VPN do mesmo fabricante da solução de *firewall* ofertada compatível para instalação em computadores com sistema operacional MS Windows 8, MS Windows 10 e MacOS;

61. A solução de *firewall* deve possuir console de gerenciamento do equipamento acessada através de interface gráfica *web* permitindo realizar as configurações da solução como criar e administrar as políticas/regras de *firewall* e controle de aplicações, criar e administrar as políticas de IPS, antivírus e *anti-spyware*, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de *logs* de eventos e demais configurações;

62. Deve suportar a autenticação dos usuários administradores que se conectam à interface de gerenciamento do equipamento via LDAP, MS *Active Directory*, RADIUS e através de base de usuários local no equipamento da solução de *firewall*;

63. Deve ser possível criar perfis de acesso à interface de gerenciamento com permissões granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros;

64. Deve permitir realizar o *backup* das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;

65. A interface de gerenciamento do equipamento deve possuir recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regras (*shadowing*) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve possuir também recurso para análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão da mesma para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente;

    1. É permitido o uso de *appliance* externo para realização da análise das políticas;

66. Deve ser possível através de interface de gerenciamento do equipamento a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuário específicos incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados;

67. Deve ser possível gerar relatório de visibilidade e uso das aplicações do tipo SaaS – *Software as a Service* mostrando os riscos para a segurança do ambiente, tais como a entrega de *malwares* através de aplicativos SaaS com a informação do usuário responsável pelo acesso a aplicação SaaS e o consumo da aplicação SaaS pelo usuário;

68. Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU;

69. Deve ser possível configurar o envio de alertas do sistema via *e-mail*;

70. Deve suportar o monitoramento via SNMPv3;

71. O sistema operacional a ser instalado no equipamento que compõe a solução deverá ser fornecido em sua versão mais atualizada, não sendo aceito sistema operacional de uso genérico;

72. Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de *softwares* necessárias para o seu funcionamento;

73. Na data do certame, nenhum dos equipamentos ofertados poderão estar listados no site do fabricante em listas de *end-of-life* e *end-of-sale*;

74. Durante o período de vigência do contrato de garantia todos os componentes da solução de *firewall*, incluindo o equipamento, o sistema operacional do mesmo, as licenças necessárias para atender as funcionalidades e recursos solicitados, os *softwares* clientes de VPN e demais itens necessários para o perfeito funcionamento devem estar cobertos por garantia e suporte técnico do fabricante da solução em caso de problema;

75. A solução de *firewall* deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais *software* e das assinaturas de proteção da solução.

Serviço de Instalação:

1. A contratada deverá prestar serviços de instalação e configuração do item 3 do grupo 1, que compreendem, entre outros, os seguintes procedimentos:
    1. Reunião de alinhamento para criação do escopo do projeto previamente a instalação;
    2. Instalação física de todos os equipamentos (*hardware*) e licenças (*softwares*) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);
    3. Análise da topologia e arquitetura da rede, considerando todos os equipamentos já existentes e instalados;
    4. Análise do acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;
    5. Migração das regras de *firewall* existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;
    6. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;
    7. Configuração do sistema de *firewall*, VPN, IPS, Filtro URL, antivírus e *anti-malware* de acordo com as exigências levantadas;
2. Toda a configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos *firewall* afim de garantir a melhor eficiência da solução durante o período de vigência das licenças;
3. Configuração do sistema de gerenciamento centralizado considerando adição dos novos *appliance*;
4. Repasse de informação das configurações realizadas no formato *hands-on* de 4 horas para a equipe responsável pelo projeto por parte da contratante após validação da migração;

3.3.2.4. **Grupo 1: Item 4 - SOFTWARE DE GESTÃO CENTRALIZADA COM SUPORTE E GARANTIA DE 05 ANOS**

Características técnicas mínimas:

1. Deve ser fornecido solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos de *firewall*;
2. A solução de gerenciamento centralizado deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos de *firewall* gerenciados pela solução, além de consolidar os registros de eventos (*logs*) e relatórios de todos os equipamentos que compõem a solução de proteção de rede;
3. Deve ser homologado totalmente compatível com os itens 1, 2 e 3 especificadas para permitir o gerenciamento centralizado e armazenamento de *logs* dos mesmos, estando devidamente licenciado para este fim;
4. Deve permitir o controle sobre todos os equipamentos de *firewall* em uma única console, com administração de privilégios e funções;
5. O gerenciamento centralizado poderá ser entregue como *appliance* físico ou virtual. Caso seja entregue em *appliance* físico ele deve ser compatível com *rack* 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em *appliance* virtual deve ser compatível com VMware ESXi;
6. Deve permitir o armazenamento de *logs* sem limite de tempo nem limite da quantidade de *logs* diários a ser recebido ou armazenado. Caso seja necessário licenciamento adicional, deverá ser entregue licenciado com a maior capacidade suportada;
7. Deve permitir controle global de políticas para todos os equipamentos gerenciados pela solução;
8. Deve suportar organizar os equipamentos gerenciados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;
9. Deve implementar sistema de hierarquia entre os equipamentos gerenciados, onde seja possível aplicar configurações de forma granular em grupos de *firewall*;
10. Deve implementar a criação de perfis de usuários com acesso a solução de gerenciamento com definição exata de quais informações e de quais equipamento de *firewall* e grupos de equipamentos de *firewall* o usuário terá acesso referente a *logs* e relatórios;
11. Deve permitir a criação de objetos e políticas compartilhadas;
12. Deve consolidar *logs* e relatórios de todos os equipamentos de *firewall* gerenciados;
13. Deve permitir exportar o *backup* de configuração automaticamente via agendamento;
14. Deve permitir que a configuração dos *firewall* seja importada de forma automática na solução de gerenciamento centralizado e que possa ser usada em outros *firewall* e grupos de *firewall*;
15. Deve mostrar os status dos equipamentos de *firewall* em alta disponibilidade a partir da solução de gerenciamento centralizado;
16. A solução de gerenciamento centralizado e armazenamento de *logs* deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a atualização do software para obter novas funcionalidades e correções de *bugs*.

3.3.2.5. **Grupo 1: Item 5 - TREINAMENTO OFICIAL DE FIREWALL**

Características técnicas mínimas:

1. A contratada deverá disponibilizar um voucher individual para participação no treinamento oficial do fabricante do item Solução de Segurança de Rede *Firewall* ofertado;
2. O treinamento deve ser ministrado abrangendo teoria e prática de configuração e administração de solução de *firewall* de próxima geração, bem como assuntos teóricos relacionados;
3. Deve conter, no mínimo, a seguinte ementa:
    1. Arquitetura e plataforma;
    2. Configuração da solução;
    3. Políticas de segurança e NAT;
    4. Políticas de segurança baseada em aplicação;
    5. Identificação de aplicações;
    6. Identificação de usuário;
    7. Bloqueio de ameaças;
    8. Bloqueio de ameaças desconhecidas;
    9. Bloqueio de ameaças em de tráfego criptografado;
    10. Análise das informações de tráfego e ameaças detectadas;
    11. Demais assuntos pertinentes a solução;
4. A duração do curso será de 5 dias em horário comercial;
5. Deve ser emitido um único certificado de conclusão cobrindo todo o curso para o participante;
6. O treinamento deverá ser ministrado pelo próprio fabricante ou por um parceiro nacional, capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais;
7. O treinamento deve estar disponível na modalidade presencial nas instalações do fabricante ou da autorizada ou ministrado de forma remota;
8. O fabricante ou autorizada fornecerá os materiais didáticos para ministrar o curso;
9. Não será necessário considerar na proposta os custos de deslocamento, hospedagem e alimentação. Esses custos serão de responsabilidade da Contratante;

3.4. **Parcelamento da Solução de TIC**

O objeto do certame não será parcelado, pois a solução deve ser na totalidade de um único fabricante para que seja completamente interoperável e de baixa complexidade operacional, de manutenção e de atualização. Soluções que envolvem mais de um fabricante exigem maior esforço da equipe técnica, pois trabalham com sintaxes diferentes, tem *softwares* diferentes. Além disso, a integração dessas soluções é mais trabalhosa e muito mais sujeita a falhas de interoperabilidade. Esses fatos prejudicam em um eventual incidente a correlação das informações e por consequência comprometem a disponibilidade da equipe e segurança das redes e das informações.

Caso seja desconsiderado o agrupamento dos itens e adotado o critério de julgamento e de adjudicação de menor preço unitário, não há como garantir que as partes da solução sejam compatíveis entre si, de forma a comprometer o conjunto indissociável do objeto.

Somente a execução de forma integrada dos itens licitados garante a segurança adequada das informações, a interoperabilidade da solução durante toda a vida útil do equipamento por tratar-se de *hardware* e *softwares* de mesma natureza e portanto garante uma gestão simplificada, menor esforço técnico, maior segurança das redes de dados. Além disso, evita a transferência de responsabilidades entre fabricantes em casos de eventuais problemas causados por má interoperabilidade no caso desassociação dos itens.

As vantagens obtidas pelo agrupamento do objeto do certame em lote único são:

- Garantia de interoperabilidade dos itens durante toda a vida útil dos equipamentos;
- Menor esforço de gestão da equipe técnica;
- Maior segurança das informações e das redes e identificação de incidentes;
- Evita a isenção de responsabilidade por parte dos fabricantes em caso de problemas e necessidade de acionamento da garantia.

3.5. **Resultados e Benefícios a Serem Alcançados**

3.5.1. Melhorar o nível de segurança dos serviços das aplicações internas da Universidade;

3.5.2. Garantir a confiabilidade da segurança das informações e infraestrutura da Universidade;

3.5.3. Proteger a infraestrutura de TI contra ataques cibernéticos;

3.5.4. Auxiliar na criação de regras de acesso a infraestrutura de TI utilizando usuários e grupos como parâmetros.

4. **ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO**

4.1. **Requisitos de Negócio**

4.1.1. Preservação da integridade e da confidencialidade dos dados dos usuários, sejam eles docentes, discentes e técnicos administrativos em educação desta Universidade para conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018);

4.1.2. Assegurar a continuidade da segurança na comunicação de dados tanto externamente quanto entre os ativos de tecnologia dentro da rede dos campi;

4.1.3. Proteção da infraestrutura de tecnologia da informação de modo a impedir que seja utilizada para outros fins como, por exemplo, na utilização da capacidade computacional da instituição para fins não educacionais ou mesmo criminosos, como a mineração de bitcoins, armazenamento e acesso à conteúdo ilícito ou ser origem ou destino de ataques cibernéticos;

4.1.4. Auxiliar no comprimento da Marco Civil da Internet Lei nº 12.965/2014.

4.2. **Requisitos de Capacitação**

4.2.1. Deve ser apresentado atestado de capacidade técnica ou declaração emitida pelo fabricante do equipamento, comprovando que a licitante é apta a instalar, configurar, prestar suporte técnico e ministrar treinamentos das solução descrita no item 3.3.2 deste Termo de Referência;

4.2.2. A contratada deverá possuir, pelo menos, um técnico certificado pelo fabricante compatível com o objeto deste Termo de Referência;

4.2.2.1. A comprovação de vínculo profissional se fará com a apresentação de cópia da carteira de trabalho (CTPS) em que conste o licitante como contratante; do contrato

social do licitante em que conste o profissional como sócio; do contrato de prestação de serviços, sem vínculo trabalhista, regido pela legislação civil ou, ainda, de declaração de contratação futura do profissional, desde que acompanhada de declaração de anuência do profissional.

4.3. **Requisitos Legais**

4.3.1. Atender os requisitos estabelecidos na lei n° 8.666/93 e na IN n° 1 de 4 de abril de 2019.

4.3.2. Durante a vigência contratual, a CONTRATADA deverá manter as condições e os critérios técnicos de habilitação, conforme disposição legal.

4.3.3. A CONTRATADA deverá cumprir os requisitos legais estabelecidos em CONTRATO, bem como os requisitos técnicos descritos no Termo de Referência e seus respectivos anexos.

4.4. **Requisitos de Manutenção**

4.4.1. Os requisitos de **manutenção preventiva** corresponde a verificação do correto funcionamento da solução pela área responsável e acionamento da garantia para eventual serviço de **manutenção corretiva**.

4.4.2. A Contratada deve fornecer, durante todo o período de garantia, todas as atualizações relacionadas a ao *softwares, firmwares* e atualizações relacionadas a assinaturas de segurança e protocolos de segurança conforme disponibilizados pelo fabricante.

4.4.2.1. A CONTRATADA é responsável por fornecer todos os materiais e ferramentas necessários para execução das **manutenção corretivas**, sempre que necessário durante o período de garantia, mantendo a solução completamente funcional no que tange a *hardware*, *software*, licenciamento e atualizações. Os prazos devem ser seguidos conforme descritos no Acordo de Nível de Serviço;

4.4.2.2. A CONTRATADA deve custear todo o serviço de deslocamento do seu técnico para instalação e manutenções durante todo o período de garantia dos equipamentos, seguindo os prazos descritos no Acordo de Nível de Serviço;

4.4.2.3. Cabe a CONTRATADA seguir as orientações dos fabricantes descritas nos manuais dos equipamentos para a realização das **manutenções corretivas**;

4.4.2.4. Os materiais, peças e componentes de reposição devem ser idênticos aos substituídos, originais, novos e de primeiro uso. Em caso de impossibilidade da substituição pelo original, a CONTRATADA deverá apresentar justificativa técnica expressa a CONTRATANTE, e em caso de aceite da justificativa, a CONTRATADA deverá apresentar o componente de reposição com especificações idênticas ou superiores, novos e de primeiro uso.

4.4.2.5. As solicitações de **manutenção corretiva** e suporte técnico serão realizados por meio de chamados técnicos feitos diretamente à CONTRATADA quando constatado falha ou erro pela área responsável.

4.4.2.6. A CONTRATADA deverá disponibilizar, obrigatoriamente, um ou mais canais de comunicação para registro e gestão dos chamados técnicos.

4.4.2.7. A CONTRATADA deverá disponibilizar um sistema de monitoramento e controle dos chamados técnicos, ou relatórios dos chamados abertos contendo todo acompanhamento do chamado e solução dada.

4.4.2.8. Não haverá limites para quantidades de chamados técnicos abertos.

4.4.2.9. Cada chamado técnico deverá conter, no mínimo, as seguintes informações:

- Número de registro;
- Data e hora de abertura;
- Descrição da solicitação, incidente, falha ou erro;
- Data e hora de fechamento;
- Descrição da solução adotada.

4.4.2.10. Para cada chamado técnico aberto, deverá ser emitido e entregue o Relatório de Atendimento Corretivo, contendo as informações descritas no item anterior e os procedimentos realizados para solução do chamado.

4.4.2.11. O Relatório de Atendimento deverá ser assinado pelos técnicos da CONTRATADA e da CONTRATANTE.

4.4.2.12. O chamado técnico somente será finalizado após a entrega do Relatório de Atendimento, devidamente assinado pelas partes.

4.4.2.13. Os chamados técnicos deverão ser solucionados conforme os prazos descritos no Acordo de Nível de Serviço.

4.5. **Requisitos Temporais**

4.5.1. **Garantia e Suporte:**

4.5.1.1. Deve possuir garantia do fabricante ou autorizada no Brasil com validade mínima de 60 (sessenta) meses;

4.5.1.2. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de *bugs*;

4.5.1.3. Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução;

4.5.1.4. Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição nos locais especificados neste edital, obedecendo a modalidade NBD (*Next Business Day*);

4.5.1.5. Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português ou *website* ou *e-mail* durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana), não existindo limite de chamado;

4.5.2. **Condições de Entrega**

4.5.2.1. O prazo de entrega dos produtos deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato;

4.5.2.2. A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada;

4.5.2.3. Para itens de *software*, poderá ser fornecido sem mídia de instalação, desde que seja indicado local para download do arquivo de instalação;

4.6. **Requisitos de Segurança e Privacidade**

4.6.1. Os serviços deverão ser prestados em conformidade com leis, normas e diretrizes de Governo relacionadas à Segurança da Informação e Comunicações, em especial a Instrução Normativa n° 01-GSI/PR e suas normas complementares, bem como a todos os normativos internos da CONTRATANTE que tratam do assunto, tais como a Política de Segurança da Informação da UFSCar.

4.6.2. A empresa CONTRATADA para prestar os serviços deverá credenciar junto à CONTRATANTE seus profissionais autorizados a operar presencialmente nos sítios da CONTRATANTE, e também aqueles que terão acesso aos sistemas corporativos.

4.6.3. A CONTRATADA deverá comprometer-se, por si e por seus funcionários, a aceitar e aplicar rigorosamente todas as normas e procedimentos de segurança definidos na Política de Segurança da Informação da CONTRATANTE – inclusive com a assinatura de termo apropriado de responsabilidade e manutenção do sigilo.

4.6.4. A CONTRATADA deverá comunicar a CONTRATANTE, com antecedência, qualquer ocorrência de transferência, remanejamento ou demissão de funcionários envolvidos diretamente na execução dos serviços de suporte à infraestrutura, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos da CONTRATANTE.

4.6.5. Todas as informações as quais a CONTRATADA ter acesso em função da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada sua reprodução, utilização ou divulgação a terceiros.

4.6.6. Os representantes, empregados e colaboradores da CONTRATADA deverão zelar pela manutenção do sigilo absoluto de dados, informações, documentos e especificações técnicas, que tenham conhecimento em razão dos serviços executados.

4.6.7. Todas as informações, imagens e documentos a serem manuseados e utilizados são de propriedade da CONTRATANTE e não poderão ser repassados, copiados, alterados ou absorvidos pela CONTRATADA sem expressa autorização da CONTRATANTE, de acordo com os termos constantes em termo de sigilo a ser firmado entre a CONTRATANTE e a CONTRATADA.

4.6.8. Cada profissional a serviço da CONTRATADA deverá estar ciente de que a estrutura computacional do órgão não poderá ser utilizada para fins particulares,

sendo que quaisquer ações que tramitem em sua rede poderão ser auditadas.

4.7. **Requisitos Sociais, Ambientais e Culturais**

4.7.1. Requisitos sociais:

4.7.1.1. Quando no ambiente da UFSCar, manter os seus prestadores de serviços sujeitos às suas normas disciplinares, porém sem qualquer vínculo empregatício com o órgão;

4.7.1.2. Respeitar as normas e procedimentos de controle e acesso às dependências da UFSCar;

4.7.2. Requisitos culturais:

4.7.2.1. O atendimento deve ser efetuado em língua portuguesa.

4.7.3. Requisitos Ambientais:

4.7.3.1. Sobre os critérios de sustentabilidade ambiental na contratação de serviços pela Administração Pública Federal, conforme Art. 6o da INSTRUÇÃO NORMATIVA No 1, de 19 de janeiro de 2010, da SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO, a CONTRATANTE exigirá que a empresa CONTRATADA adote as seguintes práticas de sustentabilidade na execução dos serviços:

a) Adotar medidas para evitar o desperdício de energia e água tratada, conforme instituído no Decreto no 48.138, de 8 de outubro de 2003;

b) Dar a destinação correta a baterias, óleos e filtros descartados no processo de manutenção, segundo disposto na Resolução CONAMA no 257, de 30 de junho de 1999;

c) Desenvolver ou adotar manuais de procedimentos de descarte de materiais potencialmente poluidores, tais como sobre pilhas e baterias dispostas para descarte que contenham em suas composições chumbo, cádmio, mercúrio e seus compostos, aos estabelecimentos que as comercializam ou à rede de assistência técnica autorizada pelas respectivas indústrias, para repasse aos fabricantes ou importadores;

d) Separar resíduos como papéis, plásticos, metais, vidros e orgânicos para empresas de coleta apropriadas, respeitando as Normas Brasileiras – NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos;

e) Separar e acondicionar em recipientes adequados para destinação específica as lâmpadas fluorescentes e frascos de aerossóis em geral, quando descartados;

f) Encaminhar os pneumáticos inservíveis abandonados ou dispostos inadequadamente, aos fabricantes para destinação final, ambientalmente adequada, tendo em vista que pneumáticos inservíveis abandonados ou dispostos inadequadamente constituem passivo ambiental, que resulta em sério risco ao meio ambiente e à saúde pública. Esta obrigação atende a Resolução CONAMA no 258, de 26 de agosto de 1999;

g) Fornecer aos empregados os equipamentos de segurança que se fizerem necessários para a execução de serviços;

h) Racionalizar o uso de substâncias potencialmente tóxicas/poluentes;

i) Substituição de substâncias tóxicas por outras atóxicas ou de menor toxicidade;

j) Capacitar periodicamente os empregados sobre boas práticas de redução de desperdícios/poluição;

k) Utilizar lavagem com água de reuso ou outras fontes, sempre que possível (águas de chuva, poços cuja água seja certificada de não contaminação por metais pesados ou agentes bacteriológicos, minas e outros); e

l) Promover a reciclagem e destinação adequada dos resíduos gerados nas atividades de limpeza, asseio e conservação.

4.7.3.2. No momento da assinatura do contrato, a comprovação do disposto acima poderá ser feita mediante apresentação de declaração da empresa, assinalando que cumpre os critérios ambientais exigidos. A CONTRATANTE poderá realizar diligências para verificar a adequação quanto às exigências.

4.8. **Requisitos de Arquitetura Tecnológica**

4.8.1. Todos os requisitos de arquitetura tecnológica, que é composta por: *hardware*, *software*, padrões de interoperabilidade, linguagens de programação, interfaces, dentre outros estão descritos no item 3.3.2 deste Termo de Referência.

4.8.2. Ressalta-se a necessidade destes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, necessitarem ser do mesmo fabricante e portanto serem agrupados em um único lote. Essa prática é amparada pelo disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas).

4.9. **Requisitos de Projeto e de Implementação**

4.9.1. Não se aplica ao objeto da contratação pois o escopo do serviço se delimita a garantia e suporte dos equipamentos da solução descrita neste Termo de Referência.

4.10. **Requisitos de Implantação**

4.10.1. A CONTRATADA deverá fazer a reunião de alinhamento com a CONTRATANTE para criação do escopo do projeto previamente a instalação. O prazo é de até 5 (cinco) dias após a entrega dos equipamentos.

4.10.2. Após a reunião e definição do escopo do projeto, que não deve ultrapassar o prazo de 10 (dez) dias úteis, será agendada a instalação dos equipamentos.

4.10.3. O prazo para instalação é de até 5 (cinco) dias após a definição do escopo do projeto.

4.11. **Requisitos de Garantia e Manutenção**

4.11.1. A CONTRATADA deverá prover garantia dos equipamentos e softwares constantes na solução durante toda a vigência do CONTRATO.

4.11.2. A garantia de todos os equipamentos e materiais fornecidos é total, e inclui a substituição de todas as peças, componentes e acessórios, sem qualquer tipo de faturamento adicional. Não serão aceitas alegações que o componente chegou ao final da vida útil prevista ou de que este era consumível.

4.11.3. A reposição de peças na garantia deverá utilizar apenas peças e componentes originais do fabricante do equipamento, salvo nos casos fundamentados por escrito e autorizados previamente pela Fiscalização.

4.12. **Requisitos de Experiência Profissional**

4.12.1. Para a prestação dos serviços, a CONTRATADA deverá ter experiência técnica comprovada, conforme requisitos de capacitação exigidos neste Termo de Referência.

4.13. **Requisitos de Formação de Equipe**

4.13.1. Os serviços deverão ser executados por profissionais qualificados, sendo esta qualificação aferida com base em cursos de formação e certificações oficiais, com experiência em diagnóstico proativo de problemas em ambientes complexos, e com a capacidade técnica necessária para atender a complexidade especificada no procedimento.

4.13.2. Durante a execução contratual, a CONTRATADA se obriga a manter as qualificações, certificações e habilidades dos seus colaboradores diretamente envolvidos na prestação dos serviços, conforme estabelecem os requisitos obrigatórios previstos neste Termo de Referência.

4.14. **Requisitos de Metodologia de Trabalho**

4.14.1. A metodologia de trabalho será baseada no conceito de delegação de responsabilidade, onde a CONTRATANTE é responsável pela gestão e fiscalização do contrato e pela atestação da aderência aos padrões de qualidade exigidos, e a CONTRATADA como responsável pela execução dos serviços e gestão dos seus recursos humanos.

4.14.2. A CONTRATADA deverá executar os serviços seguindo os processos, padrões e procedimentos descritos na Base de Conhecimento da CONTRATANTE.

4.14.3. A CONTRATADA deverá ter um canal de comunicação, e-mail ou central de atendimento 0800 ou um sistema de chamado para ser acionada pela CONTRATANTE em caso de ocorrência ou qualquer outra necessidade.

4.14.4. Os chamados para a prestação dos serviços serão feitos por intermédio de e-mail, telefone (0800) ou website (Central de Atendimento, Central de

Monitoramento ou outro sistema disponibilizado), a ser definido pela CONTRATANTE junto a CONTRATADA.

4.14.5. Durante a execução das tarefas, deverão ser observadas todas as boas práticas para garantir a disponibilidade dos sistemas e ambientes computacionais, a migração eficaz e transparente dos recursos, a execução de todas as análises e provas e a verificação do desempenho de todos os ativos de TI impactados pela atividade.

4.14.6. Todas as atividades devem estar de acordo com as especificações e melhores práticas dos fabricantes dos equipamentos/*softwares* e com as recomendações de organizações padronizadoras do segmento, desde que não entrem em conflito com os padrões, procedimentos e documentação definidos pela CONTRATANTE.

4.15. **Requisitos de Segurança da Informação e Privacidade**

4.15.1. A solução visa garantir a segurança da informação. Para isso, tem por objetivo:

4.15.2. Realizar controle de acesso aos serviços de TI da UFSCar;

4.15.3. Auxiliar na detecção de incidentes de segurança da informação;

4.15.4. Possibilitar o armazenamento dos logs para rastreabilidade dos eventos e manutenção de trilhas de auditoria;

4.16. **Outros Requisitos Aplicáveis**

4.16.1. Para o correto dimensionamento e elaboração de sua proposta, a licitante poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 09 horas às 17 horas.

4.16.2. O prazo para vistoria iniciará no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.

4.16.3. Para a vistoria, o licitante ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

4.16.4. A não realização da vistoria, quando facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus dos serviços decorrentes.

4.16.5. A licitante deverá declarar que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação assinando a Declaração de Vistoria Técnica (Anexo VI); OU

4.16.6. Caso a licitante decida não realizar a vistoria, deverá assinar a Declaração de Dispensa de Vistoria Técnica (Anexo VII).

5. RESPONSABILIDADES

5.1. **Deveres e responsabilidades da CONTRATANTE**

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

b) Encaminhar formalmente a demanda por meio de Ordem de Serviço, de acordo com os critérios estabelecidos no Termo de Referência;

c) Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

d) Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

e) Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato;

f) Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

g) Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da CONTRATADA, com base em pesquisas de mercado, quando aplicável;

h) 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;

i) Verificar, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e, posterior, recebimento definitivo;

5.2. **Deveres e responsabilidades da CONTRATADA**

a) Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

b) Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE;

c) Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

d) Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

e) Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

f) Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

g) Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados à Administração;

h) Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

i) Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da CONTRATANTE;

j) Não fazer uso das informações prestadas pela CONTRATANTE para fins diversos do estrito e absoluto cumprimento do contrato em questão;

k) **Para assinatura do contrato a CONTRATADA deve ter tido os requisitos de capacitação aprovados.**

5.3. **Deveres e responsabilidades do órgão gerenciador da ata de registro de preços**

Não se aplica ao objeto da contratação pois não haverá contratação por Sistema de Registro de Preços – SRP.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. **Rotinas de Execução:**

FIREWALLS

FIREWALLS
1. Auxiliar na elaboração do projeto de infraestrutura, destacando as melhores práticas de mercado; 2. Auxiliar durante todo o processo de instalação e configuração dos equipamentos; 3. Instalar as licenças constantes na solução; 4. Enviar atualizações de *firmware* e de *software*, sempre no dia útil posterior ao lançamento da atualização pelo fabricante, constando o roteiro para aplicação das atualizações; 5. Dar suporte para configurações e reparar, através de manutenções corretivas, qualquer problema de *hardware*, *firmware* e *software* dos equipamentos;
SOFTWARE DE GERENCIAMENTO CENTRALIZADO
1. Auxiliar durante todo o processo de instalação e configuração; 2. Instalar as licenças constantes na solução; 3. Enviar atualizações de *firmware* e de *software*, sempre no dia útil posterior ao lançamento da atualização pelo fabricante, constando o roteiro para aplicação das atualizações; 4. Dar suporte para configurações e reparar, através de manutenções corretivas, qualquer problema de *hardware* (quando for o caso), *firmware* e *software* dos equipamentos;

6.1.1. A CONTRATADA deve garantir o pleno funcionamento de todos os equipamentos e *softwares* da solução descrita neste Termo de Referência.

6.1.2. A CONTRATADA fica responsável em fornecer, sem nenhum ônus à CONTRATANTE, todas as peças de reposição bem como os materiais auxiliares necessários para a realização de serviços de manutenção preventiva/programada (atualizações, suporte, etc) e corretiva.

6.1.3. A CONTRATADA fica responsável em fornecer, sem nenhum ônus à CONTRATANTE, toda a mão de obra, os seus custos relacionados a deslocamento, estadia, trabalhista, ou qualquer outro relacionado ao cumprimento do objeto do contrato.

6.1.4. As omissões e divergências técnicas desta especificação devem ser tratadas considerando as definições e considerações das normativas e literatura relacionadas abaixo:

6.1.4.1. Todo e qualquer serviço realizado pela CONTRATADA deverá obedecer às Normas Regulamentadoras do Ministério do Trabalho – NR, aprovada pela Portaria 3214, de 08 de junho de 1978, relativas à Segurança e Medicina do Trabalho, em especial a NR-18 – condições e meio ambiente de trabalho na indústria da construção.

6.1.4.2. A CONTRATANTE poderá paralisar a execução dos serviços se a CONTRATADA não mantiver suas atividades dentro de padrões de segurança exigidos por lei.

6.1.4.3. Fica a CONTRATADA responsável pelo fornecimento e pela supervisão do uso pelos seus profissionais, de equipamentos de proteção individual (EPI's) estabelecido em norma regulamentadora do Ministério do Trabalho, tais como: uniformes, identificação profissional (crachá), capacetes de segurança, protetores faciais, óculos de segurança contra impactos, luvas e mangas de proteção, botas de borrachas, calçados de couro, cintos de segurança, máscaras, avental de raspa de couro e outros que se fizerem necessários.

6.1.4.4. O transporte, refeições, assistência médica e demais benefícios, bem como todos os custos trabalhistas para todos os seus funcionários deverão ser sempre providos pela CONTRATADA.

6.1.4.5. Todos os serviços deverão ser executados obedecendo rigorosamente as Normas Regulamentadoras de Segurança e Saúde no Trabalho, em especial:

- NR 1 – Disposições Gerais;
- NR 4 – Serviços Esp. Engenharia de Segurança e em Medicina do Trabalho;
- NR 6 – EPI - Equipamentos de Proteção Individual;
- NR 7 – Programa de Controle Médico de Saúde Ocupacional;
- NR 9 – Programa de Prevenção de Riscos Ambientais.

6.1.4.6. Para as atividades que envolva infraestrutura, deverá ser considerado como referência e fonte de consulta as seguintes:

- ABNT (Associação Brasileira de Normas Técnicas);
- ASTM - American Society will be Testing Materials;
- ANSI - American Standard National Institute – TIA 942/ TIA 568C;
- ASME - American Standards Mechanical Engineering;
- ASHRAE - American Society Heat. Refrig. Air Cond. Engineers;
- Recommendations of the manual "Industrial Ventilation";
- NFPA - National Fire Protection Association; e
- IEC - International Electrical Code;

6.1.5. Manutenção Corretiva:

a) Caberá à CONTRATADA apresentar soluções definitivas para os problemas apresentados dentro dos prazos e condições estabelecidos neste Termo de Referência.

b) Caberá à CONTRATADA emitir Relatório Técnico apontando a causa raiz dos problemas e as ações necessárias para sua solução.

c) No caso de constatação de defeito irreparável em qualquer um dos firewalls ou sistema de gerenciamento centralizado fornecidos e instalados, a CONTRATADA deverá avaliar a necessidade de sua substituição, emitindo Relatório Técnico.

d) Este Relatório Técnico deve ser conclusivo quanto ao impacto do defeito nas características construtivas dos mesmos e em seu nível de proteção, quando for o caso.

e) Havendo a necessidade comprovada de substituição integral do equipamento danificado, a CONTRATADA deverá substituí-lo em garantia.

f) Nenhum serviço de manutenção corretiva poderá ser executado pela CONTRATADA sem a autorização direta da CONTRATANTE, por meio de seus responsáveis indicados.

6.2. **Quantidade mínima de bens ou serviços para comparação e controle**

A quantidade mínima de serviços que deverão ser prestados pela CONTRATADA estão especificados na tabela:

ITEM	DESCRIÇÃO DA ATIVIDADE TÉCNICA	QUANTIDADE	MÉTRICA OU UNIDADE
1	ELABORAÇÃO DE PROJETO CONTEMPLANDO TODA A SOLUÇÃO	1	unid.
	INSTALAÇÃO DO FIREWALL	4	unid.
	INSTALAÇÃO DO SOFTWARE DE GERENCIAMENTO CENTRALIZADO	1	unid.
	CONFIGURAÇÃO DO FIREWALL	4	unid.
	CONFIGURAÇÃO DO SOFTWARE DE GERENCIAMENTO CENTRALIZADO	1	unid.
	INTEGRAÇÃO DA SOLUÇÃO AO AMBIENTE DA UFSCAR	4	unid.

ITEM	DESCRIÇÃO DA ATIVIDADE TÉCNICA	QUANTIDADE	MÉTRICA OU UNIDADE
	SUPORTE TÉCNICO	Sempre que necessário	unid.
	REPARO / SUBSTITUIÇÃO EM GARANTIA	Sempre que necessário	unid.

6.3. **Mecanismos formais de comunicação**

6.3.1. A Ordem de Serviço (OS) (Anexo I) será adota como mecanismo formal de comunicação para a troca de informações entre a CONTRATADA e a CONTRATANTE.

6.3.2. A abertura de cada Ordem de Serviço para execução dos serviços dar-se-a:

I -Por meio de abertura de Chamado Técnico, através do telefone ou e-mail, realizado pelo CONTRATANTE, ao identificar a ocorrência de falhas nos sistemas e equipamentos, para execução dos serviços de manutenção corretiva;

II -Por meio de abertura de Chamado Técnico, através do telefone ou e-mail, realizado pelo CONTRATANTE, ao necessitar de suporte técnico para realização de atividade técnica dentro do contexto da solução constante neste Termo de Referência.

6.3.3. Todos os serviços contratados, sejam programados, ou não, e os sob demanda, somente serão executados mediante abertura de uma Ordem de Serviço, conforme modelo constante no Anexo I d, numerada sequencialmente e que registre todos os fatos ocorridos.

6.3.4. Na Ordem de Serviço deve constar a Identificação do Profissional Técnico que cumpriu a OS, os serviços executados e os materiais entregues, o tempo inicial e final de execução dos serviços.

6.3.5. A demanda executada pela CONTRATADA nas OS(s) emitidas será classificada pelo Fiscal Técnico considerando os seguintes critérios:

ACEITA	Quando a Ordem de Serviço e o entregável forem recebidos integralmente e, após verificação da qualidade, serem aceitos não cabendo ajustes.
PENDENTE	Quando a demanda for atendida parcialmente e a pendência não afetar a operacionalização das atividades da CONTRATANTE relacionada à demanda. Neste caso, deverão ser observados os Acordos de Níveis de Serviços acordado neste Termo de Referência.
NÃO ACEITA	Quando a Ordem de Serviço e o entregável forem recebidos integralmente e, após verificação da qualidade, serem rejeitados cabendo ajustes ou retificações, observado o Acordo de Níveis de Serviços e sujeitando-se a CONTRATADA às sanções estabelecidas para o caso.
SUSPENSA	Quando a execução advier de uma solução de contorno e a Ordem de Serviço ficar aguardando a solução definitiva, até o prazo máximo, conforme previsto nos subitens 7.3

6.3.6. Após a validação pela CONTRATANTE, dos serviços executados e das peças e materiais entregues pela CONTRATADA, e não havendo pendências, a Ordem de Serviço será finalizada.

6.3.7. Ao término de cada Ordem de Serviço, a CONTRATADA deverá emitir, por escrito, Relatório Técnico discriminando:

a) número de identificação da Ordem de Serviço;

b) grau de severidade;

c) data e hora da chamada;

d) data e hora do atendimento;

e) motivo da chamada;

f) situação da chamada;

g) data e hora da conclusão;

h) serviços executados;

i) relação de materiais utilizados, quando for o caso;

j) identificação do equipamento com número de série, marca e modelo, quando for o caso;

k) identificação do técnico executante;

6.3.8. Cópia do Relatório Técnico deverá ser encaminhada para a equipe responsável pelo acompanhamento e fiscalização da CONTRATANTE, no prazo máximo de 48 (quarenta e oito) horas contados a partir da conclusão dos serviços.

6.4. **Manutenção de Sigilo e Normas de Segurança**

6.4.1. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.4.2. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e Termo de Ciência, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos ANEXOS II e III.

7. MODELO DE GESTÃO DO CONTRATO

7.1. **Critérios de Aceitação**

7.1.1. Somente serão aceitos equipamentos novos e sem uso. Não serão aceitos equipamentos re-manufaturados, NFR (Not For Resale) ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

7.1.2. Observadas as condições e prazos constantes neste Termo de Referência, o recebimento dos produtos/serviços será realizado de acordo com o art. 73 da Lei no 8.666/93 nos seguintes termos:

I -Provisoriamente, por ocasião da entrega pela CONTRATADA, para posterior verificação da conformidade do produto/serviços com a especificação;

II -Definitivamente, mediante Termo Circunstanciado, por comissão designada pela autoridade competente, após a instalação, configuração e verificação de sua conformidade com as especificações contidas na proposta apresentada e/ou neste Termo de Referência;

7.1.3. Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital. Em caso de dúvida ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnico certificado na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão (conforme itens 1.1.1 e 1.1.2, TC-006.806/2006-4, Acórdão nº 838/2006-TCU-2ª Câmara);

7.2. **Procedimentos de Teste e Inspeção**

7.2.1. Para a elaboração dos Termo de Recebimento Provisório (Anexo IV) e Termo de Recebimento Definitivo (Anexo V), será feita avaliação das especificações dos equipamentos, ou inspeção junto ao técnico da CONTRATADA para que este demonstre como foi executado o serviço e solucionada a falha.

7.3. **Níveis Mínimos de Serviço Exigidos**

7.3.1. Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição para a localidade da UFSCar onde o equipamento estiver instalado, obedecendo a modalidade NBD (*Next Business Day*);

7.4. **Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento**

7.4.1. Não se aplica, devido o contrato ser apenas para efeitos de atualização da solução e garantia dos equipamentos.

7.5. **Do Pagamento**

7.5.1. A apresentação da Nota Fiscal/Fatura pela CONTRATADA deverá ocorrer no prazo de 10 (dez) dias, contados a partir da autorização de faturamento emitida pelo CONTRATANTE. Sendo que o pagamento somente será autorizado após "Recebimento Definitivo" pelo(s) servidor(es) competente(s), condicionado este ato à verificação da conformidade dos serviços atestados em relação aos valores efetivamente faturados e após validação administrativa;

7.5.2. O pagamento será realizado em parcela única;

7.5.3. O pagamento será efetuado à CONTRATADA, no prazo de até 30 (trinta) dias após o recebimento da nota fiscal/fatura relativa aos valores executados e aprovados pelo CONTRATANTE, mediante a apresentação da Notas Fiscal/Fatura pela CONTRATADA, observado Art. 40 Inc. XIV, “a” da Lei 8.666/1993. A Nota Fiscal / Fatura será paga após ser devidamente atestada pelo Gestor do Contrato;

7.5.4. Será procedida consulta “ON LINE” junto ao SICAF antes de cada pagamento a ser efetuado à CONTRATADA, para verificação da situação da mesma relativa às condições de habilitação e qualificação exigidas na licitação;

7.5.5. Nenhum pagamento será efetuado à CONTRATADA enquanto estiver pendente de liquidação qualquer obrigação técnica ou financeira que lhe for imposta;

7.5.6. Havendo erro na Nota Fiscal/Fatura ou circunstância que impeça a liquidação da despesa, aquela será devolvida à CONTRATADA, no prazo de até cinco dias úteis, com as razões da devolução apresentadas formalmente, para as devidas retificações. O pagamento ficará pendente até que a CONTRATADA providencie as medidas corretivas necessárias. Nesta hipótese, o prazo para o pagamento iniciar-se-á após a regularização da situação e/ou reapresentação do documento fiscal, não acarretando qualquer ônus para o CONTRATANTE;

7.5.7. Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionado que o índice de compensação financeira devido pelo CONTRATANTE, entre a data prevista nesta cláusula e a correspondente ao efetivo adimplemento da parcela, terá a aplicação da seguinte fórmula:

EM = I x N x VP	
Onde	EM = Encargos Moratórios
	VP = Valor da Parcela
	N = Número de dias entre a data prevista para pagamento e a do efetivo adimplemento
	I = Índice de Compensação Financeira (0,00016438)
I = (TX/100)/365 = (6/100)/365 = 0,00016438	
Onde	I = Índice de Compensação Financeira
	Tx= Taxa (6,0%)

8. **ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO**

O valor estimado para aquisição e contratação da garantia e licenciamento pelo prazo de 5 (cinco) anos é de é de R$ 1.406.041,14 (Um milhão, quatrocentos e seis mil, quarenta e um reais e quatorze centavos).

9. **ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO**

9.1. Estimativa de impacto no orçamento do órgão ou entidade, com indicação das fontes de recurso

Item	Descrição	Qtd	Valor Unit.	Valor total
1	FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 05 ANOS - SÃO CARLOS COM SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO.	1	R$ 848.217,96	R$ 848.217,96
2	FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 05 ANOS - ARARAS E SOROCABA COM SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO.	2	R$ 139.328,10	R$ 278.656,21
3	FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 05 ANOS - LAGOA DO SINO COM SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO.	1	R$ 131.627,86	R$ 131.627,86
4	SOFTWARE DE GESTÃO CENTRALIZADA COM SUPORTE E GARANTIA DE 05 ANOS	1	R$ 94.656,21	R$ 94.656,21
5	TREINAMENTO OFICIAL DE FIREWALL	4	R$ 13.220,73	R$ 52.882,90
TOTAL GERAL				**R$ 1.406.041,14**

	ESTIMATIVA DO IMPACTO NO ORÇAMENTO			
GRUPO	**ITENS**	**DESCRIÇÃO**	**QTDE**	**VALOR MÁXIMO ESTIMADO**
1	1,2,3,4 e 5	Aquisição da solução de firewall para a Universidade Federal de São Carlos - UFSCar com 5 anos de suporte, garantia, licenças de proteção e instalação	1	**R$ 1.406.041,14**
	VALOR TOTAL ESTIMADO			**R$ 1.406.041,14**
	FONTE DE RECURSOS Deverá ser ratificada pelo setor competente da Universidade Federal de São Carlos, em momento oportuno			
	PROGRAMA:		2128 – Programa de Gestão e Manutenção do Poder Executivo	
	AÇÃO:		2000 – Administração da Unidade	
	PTRES:		174009	
	PLANO INTERNO:		C20004I018 – Ações de Informática	
	ELEMENTO DA DESPESA:		44905237 - Equipamentos de TIC - Ativos de Rede	
	VALOR TOTAL ESTIMADO:		R$ 1.406.041,14	

9.2. Cronograma de execução física e financeira, contendo o detalhamento das etapas ou fases da solução a ser contratada, com os principais serviços ou bens que a compõe, e a previsão de desembolso para cada uma delas.

CRONOGRAMA DE EXECUÇÃO FÍSICO-FINANCEIRA ITEM 1		
ID	**MARCO**	**PRAZO**
D	Recebimento provisório dos equipamentos	D
D1	Conferência técnica, elaboração do projeto, instalação e configuração	D1 = D + 28
D2	Recebimento definitivo e autorização de emissão da nota fiscal	D2 = D1 + 2
D3	Emissão de Nota fiscal e recebimento pela UFSCar	D3

D4	Pagamento	D4 = D3 + 30 dias corridos

10. **DA VIGÊNCIA DO CONTRATO**

10.1. O contrato vigorará por 60 (sessenta) meses, contados a partir da data da sua assinatura, podendo ser prorrogado por períodos iguais e sucessivos, limitado a <XXX> (<XXX>) meses, desde que haja preços e condições mais vantajosas para a Administração, nos termos do Inciso II, Art. 57, da Lei no 8.666, de 1993.

10.2. A prorrogação do contrato dependerá da verificação da manutenção da necessidade, economicidade e oportunidade da contratação, acompanhada de a realização de pesquisa de mercado que demonstre a vantajosidade dos preços contratados para a Administração.

11. **DO REAJUSTE DE PREÇOS**

Não se aplica.

12. **DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR**

12.1. **Regime, Tipo e Modalidade da Licitação**

12.1.1. O regime da execução do contrato é na forma de execução indireta, sob o regime de empreitada por preço global do serviço, e o tipo e critério de julgamento da licitação é o do tipo menor preço para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratação de bens e serviços de informática.

12.1.2. De acordo com o Art. 1º do Decreto nº 10.024, de 20 de setembro de 2019, esta licitação deve ser realizada na modalidade de Pregão, na forma eletrônica, com julgamento pelo critério de menor preço.

12.1.3. A fundamentação pauta-se na premissa que a aquisição de bens e serviços baseia-se em padrões de desempenho e qualidade objetivamente definidos no Termo de Referência, por meio de especificações reconhecidas e usuais do mercado, caracterizando-se como "serviço comum" conforme Inciso II, art. 3º, do Decreto nº 10.024, de 2019.

12.2. **Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência**

12.2.1. Será observada a aplicabilidade do Direito de Preferência previsto no Decreto nº 7.174/2010 e Lei Complementar nº 123/2006. Desde que as EPPs e MEs, atendam aos requisitos legais e aos itens que serão licitados. Na existência de decretos ou instrumentos congêneres vigentes que contemple a aplicabilidade de Margem de Preferência, o mesmo será observado também.

12.3. **Critérios de Qualificação Técnica para a Habilitação**

12.3.1. As exigências de habilitação jurídica e de regularidade fiscal e trabalhista estão disciplinadas no edital.

12.3.2. Os critérios de qualificação econômica a serem atendidos pelo fornecedor estão previstos no edital.

12.3.3. Comprovação de aptidão para prestação de serviços compatíveis com as características e quantidades do objeto da licitação, estabelecidas no Termo de Referência e no Edital, por meio de apresentação de atestados de desempenho anterior, fornecidos por pessoa jurídica de direito público ou privado, comprobatório da capacidade técnica para atendimento ao objeto da presente licitação, pelo período mínimo de 12 (doze) meses, compreendendo os requisitos abaixo de maior relevância:

12.3.3.1. Deve ser apresentado atestado de capacidade técnica ou declaração emitida pelo fabricante do equipamento, comprovando que a licitante é apta a comercializar, instalar, configurar e prestar suporte técnico da solução descrita no item 3.3.2 deste Termo de Referência. Além disso, deve ser disponibilizados pela licitante os *vouchers* para realização de treinamento oficial dado pelo fabricante dos equipamentos, conforme descrito no Item 3.3.2.5 deste Termo de Referência;

12.3.4. O atestado de capacidade técnica emitido pelo fabricante deverá ser impresso em papel timbrado e conter, no mínimo, as seguintes informações: identificação da pessoa jurídica e do responsável pela emissão do atestado; identificação da LICITANTE, constando o seu CNPJ e endereço completo; descrição clara da aptidão, devendo ser assinado por seus sócios, diretores, administradores, procuradores, gerentes ou servidor responsável, com expressa indicação de seu nome completo, cargo/função e meios de contato. As declarações de pessoa jurídica de direito privado deverão estar com firma reconhecida.

12.3.5. A administração se resguarda no direito de efetuar diligência junto à pessoa jurídica emissora do atestado, visando obter informação sobre a declaração.

12.3.6. Declaração de Vistoria Técnica (Anexo VI), assinada pelo servidor responsável, declarando ter conhecimento do ambiente objeto da contratação, condições físicas, estruturais, ambientais e locais de manutenção **OU** Declaração de Dispensa de Vistoria Técnica (Anexo VII), declarando que optou por não realizar a vistoria aos locais de execução dos serviços e que assume todo e qualquer risco por esta decisão.

13. **DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO**

A Equipe de Planejamento da Contratação foi instituída pela Portaria SIN nº 64/2021, de 14 de Setembro de 2021.

Conforme o §6º do art. 12 da IN SGD/ME nº 1, de 2019, o Termo de Referência ou Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC, e aprovado pela autoridade competente.

Integrante requisitante	Integrante técnico	Integrante administrativo
MARCIO RODRIGO FALVO	MARCELO PASTRE	ANTONIO APARECIDO ROSALEM
Analísta de T.I	Técnico de T.I	Analísta de T.I
Matrícula nº 1528060	Matrícula nº 1287300	Matrícula nº 0424689

Autoridade Máxima da Área de TIC

ERICK LAZARO MELO
Secretário Geral de Informática
Matrícula nº 1995470

Aprovo,

Autoridade Competente

ERICK LAZARO MELO
Ordenador de Despesa
Matrícula nº 1995470

Documento assinado eletronicamente por **Marcio Rodrigo Falvo**, **Coordenador(a)**, em 26/10/2021, às 11:36, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Marcelo Pastre**, **Analista de Tecnologia da Informação**, em 26/10/2021, às 11:41, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Antonio Aparecido Rosalem**, **Analista de Tecnologia da Informação**, em 26/10/2021, às 11:41, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Erick Lazaro Melo**, **Secretário(a) Geral**, em 26/10/2021, às 12:07, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufscar.br/autenticacao, informando o código verificador **0520917** e o código CRC **49BC762E**.

Referência: Caso responda a este documento, indicar expressamente o Processo nº 23112.017883/2021-68 SEI nº 0520917

Modelo de Documento: Adm: Aquis: Termo de Referência, versão de 02/Agosto/2019

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENADORIA DE INFRAESTRUTURA DE

TECNOLOGIA DA INFORMAÇÃO - CITI/SIn

ORDEM DE SERVIÇO

INTRODUÇÃO

<Por intermédio da Ordem de Serviço (OS) será solicitado formalmente à Contratada a prestação de serviço ou o fornecimento de bens relativos ao objeto do contrato.

O encaminhamento das demandas deverá ser planejado visando a garantir que os prazos para entrega final de todos os bens e serviços estejam compreendidos dentro do prazo de vigência contratual.

Referência: Art. 32 IN SGD Nº 1/2019.

1 – IDENTIFICAÇÃO			
Nº da OS	xxxx/aaaa	**Data de emissão**	<dd/mm/aaaa>
Contrato nº	xx/aaaa		
Objeto do Contrato	Prestação de Serviço de Instalação, configuração, suporte técnico e garantia da solução de Firewall da UFSCar.		
Contratada	<Nome da contratada>	**CNPJ**	99.999.999/9999-99
Preposto	<Nome do preposto>		
Início vigência	<dd/mm/aaaa>	**Fim vigência**	<dd/mm/aaaa>
ÁREA REQUISITANTE			
Unidade	Coordenadoria de Infraestrutura de TI - CITI		
Solicitante	<Nome do solicitante>	**E-mail**	xxxxxxxxxxxx

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENADORIA DE INFRAESTRUTURA DE

TECNOLOGIA DA INFORMAÇÃO - CITI/SIn

2 – ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES ESTIMADOS					
Item	**Descrição do bem ou serviço**	**Métrica**	**Valor unitário (R$)**	**Qtde/Vol.**	**Valor Total (R$)**
1					
...					
Valor total estimado da OS					

3 – <INSTRUÇÕES/ESPECIFICAÇÕES> COMPLEMENTARES
<Incluir instruções complementares à execução da OS>

4 – DATAS E PRAZOS PREVISTOS			
Data de Início:	<dd/mm/aaaa>	**Data do Fim:**	<dd/mm/aaaa>
CRONOGRAMA DE EXECUÇÃO/ENTREGA			

Item	**Tarefa/entrega**	**Início**	**Fim**
1		<dd/mm/aaaa>	<dd/mm/aaaa>
...		<dd/mm/aaaa>	<dd/mm/aaaa>

5 – ASSINATURA E ENCAMINHAMENTO DA DEMANDA

Autoriza-se a execução dos serviços correspondentes à presente OS, no período e nos quantitativos acima identificados.

_____

<Nome >

<Responsável pela demanda/ Fiscal Requisitante>

Matr.: <Nº da matrícula>

_____

<Nome >

Gestor do Contrato

Matr.: <Nº da matrícula>

SÃO CARLOS, xx de xxxxxxxxx de xxxx

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENADORIA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO - CITI/SIn

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO

O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não.

Referência: Art. 18, Inciso V, alínea "a" da IN SGD/ME Nº 1/2019.

Pelo presente instrumento o <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ n° <CNPJ>, doravante denominado **CONTRATANTE**, e, de outro lado, a Fundação Universidade Federal de São Carlos sediada em Rod. Washington Luís km 235 - SP-310 - São Carlos, CNPJ n° 45.358.058/0001-40, doravante denominada **CONTRATADA**;
CONSIDERANDO que, em razão do **CONTRATO N.º <nº do contrato>** doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**; CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção; CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da **CONTRATANTE**;
Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO,** doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 – OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

2 – CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

3 – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

4 – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5 – DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas

controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6 – VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

8 – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas

para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

9 – FORO

A CONTRATANTE elege o foro da cidade de São Carlos, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10 – ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

CONTRATADA	CONTRATANTE
_____ <Nome> <Qualificação>	_____ <Nome> **Matrícula:** xxxxxxxx

TESTEMUNHAS	
_____ <Nome> <Qualificação>	_____ <Nome> <Qualificação>

São Carlos, <dia> de <mês> de 202X.

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENADORIA DE INFRAESTRUTURA DE

TECNOLOGIA DA INFORMAÇÃO - CITI/SIn

TERMO DE CIÊNCIA

INTRODUÇÃO

O Termo de Ciência visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no Órgão/Entidade.

No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados.

Referência: Art. 18, Inciso V, alínea "b" da IN SGD/ME Nº 1/2019.

1 – IDENTIFICAÇÃO

CONTRATO Nº	xxxx/aaaa		
OBJETO	Prestação de Serviço de Instalação, configuração, suporte técnico e garantia da solução de Firewall da UFSCar.		
CONTRATADA	<nome da contratada>	**CNPJ**	xxxxxxxxxxxx
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	**MATR.**	xxxxxxxxxxxxx

2 – CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da Contratada		
Nome	**Matrícula**	**Assinatura**
<Nome do(a) Funcionário(a)>		
<Nome do(a) Funcionário(a)>		
…	…	…

São Carlos, <dia> de <mês> de 202X

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENADORIA DE INFRAESTRUTURA DE

TECNOLOGIA DA INFORMAÇÃO - CITI/SIn

TERMO DE RECEBIMENTO PROVISÓRIO

INTRODUÇÃO
O Termo de Recebimento Provisório declarará formalmente à Contratada que os serviços foram prestados ou que os bens foram recebidos para posterior análise das conformidades e qualidade, baseadas nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato. **Referência: Inciso XXI, Art. 2º, e alínea "a", inciso II, art. 33, da IN SGD/ME Nº 1/2019.**

1 – IDENTIFICAÇÃO

CONTRATO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OS	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTOS/BENS E VOLUMES DE EXECUÇÃO

SOLUÇÃO DE TIC

<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>

ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE
1	<Descrição igual ao da OS/OFB de abertura>	<Ex.: PF>	<n>
…			
TOTAL DE ITENS			

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENADORIA DE INFRAESTRUTURA DE

TECNOLOGIA DA INFORMAÇÃO - CITI/SIn

3 – RECEBIMENTO

Por este instrumento, atestamos, para fins de cumprimento do disposto no art. 33, inciso II, alínea "a", da IN SGD/ME nº 01/2019, atualizada pela IN SGD/ME nº 31/2021, que os serviços correspondentes à OS acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram recebidos provisoriamente na presente data e serão objetos de avaliação por parte da **CONTRATANTE** quanto à adequação da entrega às condições contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo destes serviços ocorrerá após a verificação dos requisitos e demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**.

4 – ASSINATURAS

FISCAL TÉCNICO

_____

<Nome do Fiscal Técnico do Contrato>

Matrícula: xxxxxx

São Carlos, <dia> de <mês> de 202x.

PREPOSTO

_____

<Nome do Preposto do Contrato>

Matrícula: xxxxxx

São Carlos, <dia> de <mês> de 202X.

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS COORDENADORIA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO - CITI/SIn

TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO
O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem aos requisitos estabelecidos e aos critérios de aceitação. **Referência: Alínea "f", inciso II, e alínea "d", inciso III, do art. 33, da IN SGD/ME Nº 1/2019.**

1 – IDENTIFICAÇÃO			
CONTRATO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OS	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTOS/BENS E VOLUMES DE EXECUÇÃO				
SOLUÇÃO DE TIC				
<descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>				
ITEM	**DESCRIÇÃO DO BEM OU SERVIÇO**	**MÉTRICA**	**QUANTIDADE**	**TOTAL**
1	<descrição igual à da OS de abertura>	<Ex.: PF>	<n>	<total>
…				
TOTAL DE ITENS				

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENADORIA DE INFRAESTRUTURA DE

TECNOLOGIA DA INFORMAÇÃO - CITI/SIn

3 – ATESTE DE RECEBIMENTO

Por este instrumento atestamos, para fins de cumprimento do disposto na alínea "f", inciso II, e alínea "d", inciso III, do art. 33, da IN SGD/ME Nº 1/2019, alterada pela IN SGD/ME nº 31/2021, que os serviços correspondentes à OS acima identificada foram prestados pela **CONTRATADA** e atendem às condições contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Termo de Referência do Contrato acima indicado.

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.

<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>.

Por conseguinte, o valor a liquidar correspondente à OS acima identificada monta em R$ <valor> (<valor por extenso>).

Referência: <Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy>.

5 – ASSINATURA

FISCAL TÉCNICO	FISCAL REQUISITANTE
_____ <Nome do Fiscal Técnico> **Matrícula:** xxxxxxxx São Carlos, <dia> de <mês> de 202X.	_____ <Nome do Fiscal Requisitante> **Matrícula:** xxxxxxxx São Carlos, <dia> de <mês> de 202X.

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENADORIA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO - CITI/SIn

DECLARAÇÃO DE VISTORIA TÉCNICA

Declaro para fins de participação no Pregão Eletrônico n°_____ Processo n°_____ que a empresa _____ (razão social da empresa Licitante), inscrita no CNPJ (CGC/MF) sob o n°_____ estabelecida à _____, na cidade de _____, por meio do(a) Sr.(a) _____, portador da cédula de identidade n° _____ tomou conhecimento de todas as informações e condições para o cumprimento das obrigações relativas ao objeto da licitação em epígrafe, por meio da vistoria nas instalações, bem assim nos locais onde serão executados os respectivos serviços mediante inspeções e coleta de informações de todos os dados e elementos que possam vir a influir no valor da proposta a ser oferecida na execução dos trabalhos pertinentes ao Edital e condições existentes. A empresa se dá por satisfeita com as informações obtidas acerca do Objeto desta licitação tendo analisado todo o instrumento convocatório e seus anexos e conferindo as informações, concordando com as condições existentes.

VISITA REALIZADA EM ___/___/2021, ÀS _____ HORAS

LOCAL E DATA: _____

_____ _____

Assinatura do Representante Legal Assinatura do Representante da UFSCar

ATENÇÃO: EMITIR EM PAPEL QUE IDENTIFIQUE A LICITANTE. A LICITANTE DEVERÁ TRAZER 2 (DUAS) VIAS.

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENADORIA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO - CITI/SIn

DECLARAÇÃO DE DISPENSA DE VISTORIA TÉCNICA

A (Empresa) _____ CNPJ nº _____ neste ato representada por _____(representante da empresa constando sua qualificação, inclusive qual função/cargo na empresa) DECLARAMOS que OPTAMOS por NÃO REALIZAR a VISTORIA aos locais de execução dos serviços e que ASSUMIMOS todo e qualquer risco por esta decisão e nos comprometemos a prestar fielmente os serviços nos termos do Edital e dos demais anexos que compõem o processo deste Pregão Eletrônico Nº_____/2021, Processo Administrativo _____ em _____ de _____ de 2021.

_____

Assinatura do representante legal

ATENÇÃO: EMITIR EM PAPEL QUE IDENTIFIQUE A LICITANTE. A LICITANTE DEVERÁ TRAZER 2 (DUAS) VIAS.

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENADORIA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO - CITI/SIn
Rod. Washington Luís km 235 - SP-310, s/n - Bairro Monjolinho, São Carlos/SP, CEP 13565-905
Telefone: (16) 33518204 - http://www.ufscar.br

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇO

Unidade Gestora: Coordenadoria de Infraestrutura de Tecnologia da Informação (CITI)

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº ...../...., QUE FAZEM ENTRE SI A UNIÃO, POR INTERMÉDIO DA FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS E A EMPRESA .....

A FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS - FUFSCar por intermédio do(a) ..... (órgão) contratante), com sede no(a) ....., na cidade de SÃO CARLOS/SP, inscrito(a) no CNPJ sob o nº ....., neste ato representado(a) pelo(a) ..... (cargo e nome), nomeado(a) pela Portaria nº ....., de ..... de ..... de 20..., publicada no DOU de ..... de ..... de ....., portador da Matrícula Funcional nº ....., doravante denominada CONTRATANTE, e o(a) ..... inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., em ..... doravante designada CONTRATADA, neste ato representada pelo(a) Sr.(a) ....., portador(a) da Carteira de Identidade nº ....., expedida pela (o) ....., e CPF nº ....., tendo em vista o que consta no Processo nº ..... e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 9.507, de 21 de setembro de 2018, do Decreto nº 7.174, de 12 de maio de 2010, da Instrução Normativa SGD/ME nº 1, de 4 de Abril de 2019 e da Instrução Normativa SEGES/MPDG nº 5, de 26 de maio de 2017 e suas alterações, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão nº ...../20...., mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto do presente instrumento é a contratação dos serviços de instalação, configuração, suporte técnico e garantia da solução de Firewall da Universidade Federal de São Carlos que serão prestados nas condições estabelecidas no Termo de Referência SEI nº 0510926.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

2. CLÁUSULA SEGUNDA – VIGÊNCIA

2.1. O prazo de vigência deste Termo de Contrato é aquele fixado no Edital, com início na data de ...../...../..... e encerramento em ...../...../.....

3. CLÁUSULA TERCEIRA – PREÇO

3.1. O valor global da contratação é de R$ ..... (.....).

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação. A CONTRATANTE pagará à CONTRATADA, pela execução do objeto deste Contrato, o valor global de R$ _____ .

4. CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 20...., na classificação abaixo:

Gestão/Unidade:
Fonte:
Programa de Trabalho:
Elemento de Despesa:
PI:

4.2. No(s) exercício(s) seguinte(s), as despesas correspondentes correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

5. CLÁUSULA QUINTA – PAGAMENTO

5.1. O prazo para pagamento à CONTRATADA e demais condições a ele referentes encontram-se definidos no Termo de Referência e no Anexo XI da IN SEGES/MPDG n. 5/2017.

6. CLÁUSULA SEXTA - REAJUSTAMENTO DE PREÇOS EM SENTIDO AMPLO.

6.1. As regras acerca do reajustamento de preços em sentido amplo do valor contratual (reajuste em sentido estrito e/ou repactuação) são as estabelecidas no Termo de Referência, anexo a este Contrato.

7. CLÁUSULA SÉTIMA – GARANTIA DE EXECUÇÃO

7.1. Será exigida a prestação de garantia na presente contratação, conforme regras constantes do Termo de Referência.

8. CLÁUSULA OITAVA – MODELO DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO

8.1. O modelo de execução dos serviços a serem executados pela CONTRATADA, os materiais que serão empregados, a disciplina do recebimento do objeto e a fiscalização pela CONTRATANTE são aqueles previstos no Termo de Referência, anexo do Edital.

9. CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

9.1. As obrigações da CONTRATANTE e da CONTRATADA são aquelas previstas no Termo de Referência, anexo do Edital.

10. CLÁUSULA DÉCIMA – SANSÕES ADMINISTRATIVAS

10.1. As sanções relacionadas à execução do contrato são aquelas previstas no Termo de Referência, anexo do Edital.

11. CLÁUSULA DÉCIMA PRIMEIRA –RECISÃO

11.1. O presente Termo de Contrato poderá ser rescindido:

11.1.1. por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo ao Edital;

11.1.2. amigavelmente, nos termos do art. 79, inciso II, da Lei nº 8.666, de 1993.

11.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

11.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

11.4. O termo de rescisão, sempre que possível, será precedido de Relatório indicativo dos seguintes aspectos, conforme o caso:

11.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

11.4.2. Relação dos pagamentos já efetuados e ainda devidos;

11.4.3. Indenizações e multas.

12. CLÁUSULA DÉCIMA SEGUNDA – VEDAÇÕES E PERMISSÕES

12.1. É vedado à CONTRATADA interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

12.2. É permitido à CONTRATADA caucionar ou utilizar este Termo de Contrato para qualquer operação financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020.

12.3. A cessão de crédito, a ser feita mediante celebração de termo aditivo, dependerá de comprovação da regularidade fiscal e trabalhista da cessionária, bem como da certificação de que a cessionária não se encontra impedida de licitar e contratar com o Poder Público, conforme a legislação em vigor, nos termos do Parecer JL-01, de 18 de maio de 2020.

12.4. A crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratada) pela execução do objeto contratual, com o desconto de eventuais multas, glosas e prejuízos causados à Administração, sem prejuízo da utilização de institutos tais como os da conta vinculada e do pagamento direto previstos na IN SEGES/ME nº 5, de 2017, caso aplicáveis.

13. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993, bem como do ANEXO X da IN/SEGES/MPDG nº 05, de 2017.

13.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

13.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14. CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS

14.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

15. CLÁUSULA DÉCIMA QUINTA – DA PUBLICAÇÃO

15.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666, de 1993.

16. **CLÁUSULA DÉCIMA SEXTA – FORO**

16.1. É eleito o Foro da ..... para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 55, §2º da Lei nº 8.666/93.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em duas (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes e por duas testemunhas.

....., ... de..... de 20.....

_____
Representante legal da CONTRATANTE

_____
Representante legal da CONTRATADA

TESTEMUNHAS:
1-
2-

Documento assinado eletronicamente por **Antonio Aparecido Rosalem**, **Analista de Tecnologia da Informação**, em 15/10/2021, às 17:39, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Erick Lazaro Melo**, **Secretário(a) Geral**, em 18/10/2021, às 10:26, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015 .

A autenticidade deste documento pode ser conferida no site https://sei.ufscar.br/autenticacao, informando o código verificador **0513419** e o código CRC **B414178B**.