**MINISTÉRIO DA EDUCAÇÃO**
**UNIVERSIDADE FEDERAL DO CARIRI**
**PRÓ-REITORIA DE ADMINISTRAÇÃO**
**COORDENADORIA DE LICITAÇÕES**

# INFORMAÇÕES PRELIMINARES DO PREGÃO ELETRÔNICO

| | | | | | |
|---|---|---|---|---|---|
| Pregão Eletrônico: | 38/2020 | | | | |
| UASG: | 158719 | | | | |
| Processo: | 23507.2141/2020-56 | | | | |
| Data de abertura: | 13 / 11 /2020 às 09:00 horas no sítio www.gov.br/compras/pt-br/ | | | | |
| Objeto: | Registro de preço para contratação de empresa especializada para fornecimento de licenças para expansão do sistema de gerenciamento de rede e de solução de proteção de dados (Firewall). | | | | |
| Esclarecimentos/ Impugnações: | Até 03 dias úteis antes da abertura da licitação no e-mail Impugna.proad@ufca.edu.br | | | | |
| Valor Total Estimado | Registro de Preços? | Item(ns) e/ou Lote(s) exclusivo(s) para ME/EPP | Item(ns) e/ou Lote(s) para ampla concorrência | Lances | Exige amostra? |
| R$ 1.364.717,10 | SIM | NÃO | Itens 1, 2 e 3 | Por valor unitário | NÃO |

| **PROPOSTA ESCRITA** |
|---|
| **Observar o(s) item(ns) 10 e Anexo II (Modelo de Proposta) do edital.**<br>Deve o licitante enviar, no sistema Comprasnet, arquivo contendo a sua proposta escrita, quando finalizar o cadastramento da sua proposta no sistema. O prazo para envio ENCERRA-SE no momento da abertura da licitação, antes da fase de lances. |
| **Composição da proposta escrita** *(é obrigação do licitante verificar se o Edital exige outros requisitos além dos listados abaixo):*<br>- CNPJ, Razão Social, Endereço e Telefone;<br>- Número do Edital da Licitação;<br>- Número do Item do Edital, Descrição Completa, Marca/Modelo ofertado;<br>- Quantidade, Valor unitário e Valor total em Reais, Valor total por extenso;<br>- Prazo de Entrega (ou de execução, no caso de serviços), Prazo de Garantia, Prazo de Vigência da Proposta (Validade);<br>- Declarações contidas no Modelo do Anexo II: Composição do Preço; Que está De Acordo com o Edital; e Que atende as especificações dos itens;<br>- Dados Bancários, Data da Proposta e Assinatura (Caso seja assinada por procuração, devem ser enviados, juntamente com a proposta, Procuração e documentos do procurador) |

| **HABILITAÇÃO** |
|---|
| **Observar o(s) item(ns) 11 do edital** |
| **Requisitos básicos de habilitação** *(é obrigação do licitante verificar se o Edital exige outros documentos além dos listados abaixo):*<br>- SICAF atualizado ou Documentos equivalentes (**) |

- Regularidade da empresa licitante e do sócio majoritário perante TCU

(https://certidoes apf.apps.tcu.gov.br/),CNJ(www.cnj.jus.br/improbidade_adm/consultar_requerido.php) e CGU (www.portaldatransparencia.gov.br/ceis)

- Regularidade Fiscal Federal, Estadual e Municipal (**)

- Regularidade com o FGTS

- Regularidade trabalhista

- Atestado(s) de Capacidade Técnica (**);

- Certidão Falimentar (**).

(**)*Caso os documentos não constem no SICAF, ou estejam vencidos, devem ser atualizados no SICAF ou enviados pelo Comprasnet,* ***antes da abertura da licitação.*** *O envio pelo sistema Comprasnet se dá no campo "Documentos de habilitação"* ***no momento do cadastramento da Proposta.*** *O prazo para envio ENCERRA-SE no momento da abertura da licitação, antes da fase de lances.*

**OBSERVAÇÃO 1:** Recomenda-se especial ATENÇÃO ao atestado de capacidade técnica, ato constitutivo devidamente registrado, balanço comercial (quando o edital exigir), certidão de regularidade com o fisco estadual e certidão de regularidade com o fisco municipal. Certifiquem-se de que estejam válidos e acessíveis ao pregoeiro.

**OBSERVAÇÃO 2:** Após a abertura da licitação não será permitido enviar DOCUMENTOS DE HABILITAÇÃO AUSENTES. Poderá haver convocação somente para envio de documentos que COMPLEMENTEM informações contidas nos documentos enviados anteriormente da abertura ou cadastrados no Comprasnet.

**Recomendamos verificar o Tutorial do Comprasnet para Fornecedor no Link abaixo:**

https://demonstra.serpro.gov.br/tutoriais/comprasnet_pregao_eletronico_20191202-16-28-20/html/demo_7.html

**O Edital e outros anexos estão disponíveis para download no Comprasnet também no endereço:** https://www.ufca.edu.br/instituicao/administrativo/estrutura-organizacional/pro-reitorias/proad/licitacoes/pregao-eletronico/

**MINISTÉRIO DA EDUCAÇÃO**

**UNIVERSIDADE FEDERAL DO CARIRI**

**Pró-Reitoria de Administração**

# EDITAL PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇO Nº 38/2020

Torna-se público, para conhecimento dos interessados, que a Universidade Federal do Cariri (UASG: 158719), por meio da Coordenadoria de Licitações, sediada no Centro Multiuso – "Vapt Vupt", Rua Interventor Francisco Erivano Cruz, nº 120, 3º andar, Centro, Juazeiro do Norte-CE, CEP: 63010-015, realizará licitação para REGISTRO DE PREÇOS, na modalidade PREGÃO, na forma ELETRÔNICA, **do tipo menor preço**, **para execução indireta, em regime de empreitada por preço unitário** nos termos da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 7.892, de 23 de janeiro de 2013, da Instrução Normativa SEGES/MPDG nº 03, de 26 de abril de 2018, da Lei Complementar n° 123, de 14 de dezembro de 2006, do Decreto n° 8.538, de 06 de outubro de 2015, e do Decreto nº 10.024, de 20 de setembro de 2019, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993, no que couber, bem como as exigências estabelecidas neste Edital.

Data da sessão: 13/11/2020

Horário: 09:00 horas (horário de Brasília-DF)

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

Pregoeiro (a): Luciano Gomes Silva

## DO OBJETO

**1.** O objeto da presente licitação é o registro de preço para contratação de empresa especializada para fornecimento de licenças para expansão do sistema de gerenciamento de rede e de solução de proteção de dados (Firewall), conforme condições, quantidades e exigências estabelecidas neste instrumento convocatório, acrescido de seus anexos.

**1.1.** A licitação será dividida em itens conforme tabela constante do Anexo I (Termo de referência), facultando-se ao licitante a participação em quantos itens for de seu interesse.

**1.2.** O critério de julgamento adotado será o de menor preço para cada item, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

## 2 DAS ESPECIFICAÇÕES DO OBJETO E MUDANÇA DE DATA NA SESSÃO DE ABERTURA

**2.1.** Em caso de discordância existente entre as especificações deste objeto descritas no site www.gov.br/compras/pt-br/ e as especificações constantes deste Edital, prevalecerão as últimas.

**2.1.1.** Em caso de discordância existente entre as especificações/valores deste objeto descritos no site mencionado e as especificações/valores constantes deste Edital, prevalecerão os últimos.

**2.1.2.** Em caso de discordância existente entre a nomenclatura da unidade de medida apresentada no site mencionado e aquela constante deste Edital, prevalecerá a última.

**2.2.** Não havendo expediente na UFCA 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 e endereço eletrônico, salvo comunicação do Pregoeiro em sentido contrário.

**3 DA ADESÃO À ATA E DOS ÓRGÃOS ENVOLVIDOS (GERENCIADOR E PARTICIPANTES)**

**3.1.** O órgão gerenciador será a Universidade Federal do Cariri (UASG: 158719).

**3.2.** Não houve manifestação de interesse aceita para esta Intenção de Registro de Preços.

**3.3.** As regras referentes aos órgãos gerenciador e participantes (se existirem) são as que constam da minuta de Ata de Registro de Preços.

**3.4. Não será admitida a adesão de órgão não participante** à ata de registro de preços decorrente desta licitação.

**4 DO CREDENCIAMENTO**

**4.1.** 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.

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

**4.3.** 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.

**4.4.** 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 se tornem desatualizados.

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

**4.5.** Caberá ao licitante interessado em participar do pregão:

**4.5.1.** acompanhar as operações no sistema eletrônico durante o processo licitatório e responsabilizar-se pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pelo sistema ou de sua desconexão;

**4.5.2.** comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a inviabilidade do uso da senha, para imediato bloqueio de acesso;

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

indevido das credenciais de acesso, ainda que por terceiros.

**5 DA PARTICIPAÇÃO NO PREGÃO**

**5.1.** 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 inciso II do art. 21 da Instrução Normativa SEGES/MPDG nº 03/2018.

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

**5.1.2.** Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 34 da Lei nº 11.488, de 2007, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

**5.1.3. Não há item(ns) e/ou lote(s)** destinado(s) à participação exclusiva de microempresas e empresas de pequeno porte.

**5.2.** Não poderão participar desta licitação interessados:

**5.2.1.** proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

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

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

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

**5.2.5.** que estejam sob falência, em recuperação judicial ou extrajudicial (exceto quando houver plano de recuperação devidamente aprovado e homologado), concurso de credores, concordata ou insolvência, em processo de dissolução ou liquidação; (TCU, AC. 8271/2011 2º Câmara; Parecer nº 04/2015/CPLC/DEPCONSUIPGF/AGU; Nota técnica AGU/PGF/PF-UFCA nº 035/2017).

**5.2.6.** entidades empresariais que estejam reunidas em consórcio;

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

**5.2.8.** Instituições sem fins lucrativos (parágrafo único do art. 12 da Instrução Normativa/SEGES nº 05/2017).

**5.2.8.1** É admissível a participação de organizações sociais, qualificadas na forma dos arts. 5º a 7º da Lei 9.637/1998, desde que o objeto desta licitação se coadune com os objetivos estatutários específicos da entidade (Acórdão nº 2.847/2019- TCU-Plenário), mediante apresentação do Contrato de Gestão e dos respectivos atos constitutivos.

**5.2.9.** Será permitida a participação de cooperativas, desde que apresentem modelo de gestão operacional adequado ao objeto desta licitação, com compartilhamento ou rodízio das atividades de coordenação e supervisão da execução dos serviços, e desde que os serviços contratados sejam executados obrigatoriamente pelos cooperados, vedando-se qualquer intermediação ou subcontratação.

**5.2.9.1.** Em sendo permitida a participação de cooperativas, serão estendidas a elas os benefícios previstos para as microempresas e empresas de pequeno porte quando elas

atenderem ao disposto no art. 34 da Lei nº 11.488, de 15 de junho de 2007.

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

**5.3.1.** 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.

**5.3.1.1.** no(s) item(ns) e/ou lote(s) exclusivo(s) para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;

**5.3.1.2.** no(s) item(ns) e/ou lote(s) 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.

**5.3.2.** que está ciente e concorda com as condições contidas no Edital e seus anexos,

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

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

**5.3.5.** 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;

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

**5.3.7.** 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;

**5.3.8.** no caso de serviços, que eles 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.

**5.4.** 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.

**5.4.1.** 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);

**5.5.** 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.

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

**6 DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO**

**6.1.** Após a divulgação do edital no sítio eletrônico, **OS LICITANTES ENCAMINHARÃO OS DOCUMENTOS DE HABILITAÇÃO JUNTAMENTE COM A PROPOSTA** (contendo descrição do objeto e seu preço), exclusivamente por meio do sistema**,** até a data e o horário estabelecidos para abertura da sessão pública.

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

**6.1.2.** A apresentação da proposta e dos documentos de habilitação implicará na plena aceitação, por parte da proponente, das condições estabelecidas neste Edital e seus anexos.

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

**6.2. O prazo para o envio** conjunto da proposta e dos documentos de habilitação **encerrar-se-á com a abertura da sessão pública.**

**6.3.** Os licitantes **poderão retirar ou substituir** a proposta e os documentos de habilitação anteriormente inseridos no sistema, **até a abertura da sessão pública.**

**6.4.** 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.**

**6.4.1.** 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.

**6.5.** O Cadastro Nacional da Pessoa Jurídica – CNPJ, indicado nos documentos da proposta de preço e da habilitação deverão ser do mesmo estabelecimento.

**6.6.** 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.

**6.7.** 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.

**7 DO PREENCHIMENTO DA PROPOSTA**

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

**7.1.1.** Preço correspondente ao valor unitário dos itens, sendo considerada vencedora a proposta que oferecer o MENOR VALOR POR ITEM;

**7.1.2.** Preços correspondentes ao valor UNITÁRIO de CADA ITEM, sendo que estes preços unitários NÃO PODERÃO SER SUPERIORES aos valores estimativos da contratação, para cada item, conforme valores do Anexo I – Termo de Referência;

**7.1.2.1.** Havendo contradição entre o preço em algarismos e sua transcrição, prevalecerá o valor por extenso;

**7.1.2.2.** Os preços devem conter até duas casas decimais após a vírgula.

**7.1.3.** Quantitativo por item, observada a quantidade mínima fixada em tabela do Anexo I;

**7.1.4.** Marca e fabricante – quando for o caso;

**7.1.5.** Prazo referente à garantia – dos serviços e/ou dos bens;

**7.1.5.1.** Este prazo corresponderá a 1 (um) ano quando o Anexo I deste edital (Termo de referência) não estabelecer outro.

**7.1.6** Prazo referente à validade da proposta – observado o item 7.5.

**7.1.7.** Descrição do objeto, contendo as informações similares à especificação do Termo de Referência;

**7.1.7.1.** As licitantes deverão observar a orientação estabelecida pelo Ministério do Planejamento, Orçamento e Gestão, no sentido de se incluir o detalhamento do objeto ofertado no campo "Descrição Detalhada do Objeto".

**7.1.7.2.** A ausência de informação importante do objeto no citado campo não acarretará a desclassificação da proposta da licitante, podendo tal falha ser sanada mediante realização de diligência destinada a esclarecer ou complementar as informações.

**7.2.** Todas as especificações do objeto contidas na proposta vinculam a contratada.

**7.3.** Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens e/ou na prestação dos serviços.

**7.3.1.** 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.

**7.3.1.1.** 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/MP n.5/2017.

**7.3.2.** 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:

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

**7.3.2.2.** 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.

**7.3.3.** 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.

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

**7.3.4.** 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.

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

**7.5.** O prazo de validade da proposta não será inferior a 90 (noventa) dias, a contar da data de sua apresentação.

**7.6.** Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas (Acórdão nº 1455/2018 -TCU - Plenário);

**7.6.1.** 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.

**8 DA ABERTURA DA SESSÃO PÚBLICA E ENVIO DE LANCES**

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

**8.2.** O pregoeiro verificará as propostas apresentadas e desclassificará aquelas que não estejam em conformidade com os requisitos estabelecidos no edital.

**8.2.1.** Consideram-se em conformidade com os requisitos estabelecidos neste Edital, as propostas que: não forem omissas, não contenham vícios insanáveis/ ilegalidades ou não apresentem as especificações técnicas exigidas no Termo de Referência.

**8.2.2.** Também será desclassificada a proposta que identifique o licitante.

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

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

**8.3.** O sistema ordenará automaticamente as propostas classificadas pelo pregoeiro, sendo que somente estas participarão da fase de lances.

**8.4.** O sistema disponibilizará campo próprio para troca de mensagens entre o pregoeiro e os licitantes.

**8.5.** 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.

**8.5.1. O lance deverá ser ofertado pelo valor unitário do(s) item(ns).**

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

**8.7.** O licitante somente poderá oferecer lance valor inferior ou percentual de desconto superior ao último lance por ele ofertado e registrado pelo sistema.

**8.7.1.** O intervalo de tempo entre os lances enviados pelo mesmo licitante não poderá ser inferior a vinte (20) segundos e o intervalo entre lances não poderá ser inferior a três (3) segundos.

**8.7.2.** Deve ser observado o intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

**8.8.** Não serão aceitos dois ou mais lances iguais e prevalecerá aquele que for recebido e registrado primeiro.

**8.9.** Durante a sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

**8.9.1.** Caso o licitante não apresente lance, concorrerá com o valor ou percentual de sua proposta.

**8.10.** O critério de julgamento será MENOR VALOR PARA OS ITENS.

**8.11.** Será adotado o modo de disputa "**aberto",** em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

**8.12.** A etapa de envio de lances na sessão pública durará **dez minutos**;

**8.12.1.** Só serão admitidos os seguintes **intervalos mínimos** entre os lances:

| ITEM LICITADO | INTERVALO MÍNIMO (R$) |
|---|---|
| 01 | 240,00 |
| 02 | 185,00 |
| 03 | 40,00 |

**8.12.2.** Não havendo lances ofertados nos dois últimos minutos, a sessão pública será encerrada automaticamente.

**8.13. Havendo lance ofertado nos últimos dois minutos,** a etapa de lances será automaticamente **prorrogada;**

**8.14.** A prorrogação automática, citada no item anterior, será de **dois minutos** e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

**8.15.** Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

**8.16. Encerrada a sessão pública sem prorrogação automática pelo sistema, o pregoeiro poderá, assessorado pela equipe de apoio, admitir o reinício da etapa de envio de lances**, mediante

justificativa, em prol da consecução do melhor preço.

**8.17.** Em caso de falha no sistema, os lances em desacordo com os subitens anteriores deverão ser desconsiderados pelo pregoeiro, devendo a ocorrência ser comunicada imediatamente à Secretaria de Gestão do Ministério do Planejamento, Desenvolvimento e Gestão;

**8.17.1.** Na hipótese do subitem anterior, a ocorrência será registrada em campo próprio do sistema.

**8.18.** 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.

**8.18.1.** Nessa hipótese os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

**8.18.2.** Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente decorridas VINTE E QUATRO HORAS APÓS A COMUNICAÇÃO DO FATO AOS PARTICIPANTES, no sítio eletrônico utilizado para divulgação.

**8.19.** A ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação, de maneira que 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.

**8.20. Após a etapa de envio de lances, haverá a aplicação dos critérios de desempate previstos nos art. 44 e art. 45 da Lei Complementar nº 123, de 14 de dezembro de 2006:**

**8.20.1.** Em relação ao(s) item(ns) e/ou lote(s) não exclusivo(s) a 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.

**8.20.2.** 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.

**8.20.3.** 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.

**8.20.4.** 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.

**8.20.5.** 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.

**8.21**. Não havendo licitante que atenda à primeira hipótese de desempate (aquele previsto nos

arts. 44 e 45 da LC 123/2006), serão aplicados os critérios de desempate do § 2º do art. 3º da Lei nº 8.666, de 1993.

**8.21.1.** Estes critérios também serão aplicados no caso de não existir envio de lances após o início da fase competitiva.

**8.22.** Na hipótese de persistir o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

**8.23.** 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 previstas no edital.

**8.23.1.**Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.

**8.23.2.** A negociação será realizada por meio do sistema e poderá ser acompanhada pelos demais licitantes.

**8.23.3. O pregoeiro solicitará ao licitante melhor classificado que, no prazo de 03 (três)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.

**8.23.4.** O licitante deverá anexar a proposta de preço adequada ao último lance no sistema do site https://www.gov.br/compras/pt-br/, obedecendo ao prazo acima.

**8.23.5.** É indevida a majoração de preço unitário de item definido na etapa de lances, quer para os itens adjudicados individualmente, quer para os adjudicados em grupos (AC 8060/2020 – 2ª Câmara - TCU).

**8.23.6.** Sem prejuízo da obrigatoriedade de envio por meio do sistema do site https://www.gov.br/compras/pt-br/, o pregoeiro poderá solicitar o envio desta para o e-mail: propostas.proad@ufca.edu.br.

**8.23.7.** Os originais ou cópias autenticadas, caso sejam solicitados, deverão ser encaminhados à Coordenadoria de Licitações da UFCA, localizada localizado no Centro Multiuso – "Vapt Vupt", Rua Interventor Francisco Erivano Cruz, nº 120, 3º andar, Centro, Juazeiro do Norte-CE, CEP: 63010-015.

**8.23.8.** A licitante poderá solicitar prorrogação do prazo de 03 (três) horas, desde que este não tenha se esgotado e através do próprio sistema do site https://www.gov.br/compras/pt-br/ ou pelo e-mail propostas.proad@ufca.edu.br.

**8.23.9.** A prorrogação dependerá de decisão do pregoeiro, pois não constitui direito do licitante e sempre será concedida no interesse da Administração.

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

**9 DA ACEITABILIDADE DA PROPOSTA VENCEDORA**

**9.1.** Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação do 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.

**9.2.** O licitante qualificado como produtor rural pessoa física deverá incluir, na sua proposta, os percentuais das contribuições previstas no art. 176 da Instrução Normativa RFB n. 971, de 2009, em razão do disposto no art. 184, inciso V, sob pena de desclassificação.

**9.3.** Será **desclassificada** a proposta ou o lance vencedor que:

**9.3.1.** contenha vício insanável ou ilegalidade;

**9.3.2.** Não apresente as especificações técnicas exigidas pelo edital ou seus anexos;

**9.3.3.** Apresentar preços finais (unitários e/ou totais) superiores ao valor máximo estabelecido neste Edital;

**9.3.3.1.** Consideram-se preços máximos aqueles estabelecidos no Anexo I (Termo de Referência);

**9.3.4.**Apresentar preços que sejam manifestamente inexequíveis.

**9.3.4.1.** Considera-se inexequível a proposta que 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.

**9.3.4.2.** 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.

**9.3.4.3.** Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, não sendo possível a sua imediata desclassificação por inexequibilidade, será obrigatória a realização de diligências para o exame da proposta.

**9.3.4.4.** 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;

**9.4.** SERÃO DESCLASSIFICADAS as propostas que NÃO VIEREM A COMPROVAR SUA EXEQUIBILIDADE, em especial em relação ao preço e a produtividade apresentada.

**9.5. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências**, com vistas ao saneamento, 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.

**9.6.** O pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível aos licitantes, e lhes atribuirá validade e eficácia para fins de habilitação e classificação, observado o disposto na Lei nº 9.784, de 29 de janeiro de 1999.

**9.7.** O Pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal da UFCA ou, ainda de pessoas físicas ou jurídicas estranhas ao órgão, para orientar sua decisão.

**9.8.** O Pregoeiro poderá convocar o licitante para enviar documento complementar, em formato digital, por meio de funcionalidade disponível no sistema, estabelecendo no “chat” prazo razoável para tanto, sob pena de não aceitação da proposta.

**9.8.1.** Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, a exemplo de catálogos, folhetos ou propostas, ou planilhas de custo retificadas (em caso de contratação de serviços), encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

**9.8.2.** Sem prejuízo da obrigatoriedade de envio por meio do sistema do site https://www.gov.br/compras/pt-br/, o pregoeiro poderá solicitar o envio para o e-mail: propostas.proad@ufca.edu.br.

**9.8.3.** Os originais ou cópias autenticadas, **caso sejam solicitados**, deverão ser encaminhados para o endereço da Coordenadoria de Licitações da UFCA, localizado no Centro Multiuso – "Vapt Vupt", Rua Interventor Francisco Erivano Cruz, nº 120, 3º andar, Centro, Juazeiro do Norte-CE, CEP: 63010-015.

**9.8.4.** O prazo estabelecido pelo Pregoeiro NUNCA SERÁ INFERIOR A 2 (DUAS) HORAS.

**9.8.5.** A licitante poderá solicitar prorrogação do prazo, desde que este não tenha se esgotado e através do próprio sistema do site https://www.gov.br/compras/pt-br/ ou pelo e-mail propostas.proad@ufca.edu.br.

**9.8.6.** A prorrogação dependerá de decisão do pregoeiro, pois não constitui direito do licitante e sempre será concedida no interesse da Administração.

**9.9**. Tratando-se de pregão por **SRP, quando a proposta** do licitante vencedor **não atender ao quantitativo total** estimado para a contratação, poderá ser convocada a quantidade de licitantes necessária para alcançar o total estimado, respeitada a ordem de classificação, observado o preço da proposta vencedora, precedida de posterior habilitação.

**9.10.** 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.

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

**9.12.** Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

**10 DA HABILITAÇÃO**

**10.1.** 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, 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;

**10.2.** 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/)

**10.3.** 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.

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

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

**10.3.3.** O licitante será convocado para manifestação previamente à sua desclassificação.

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

**10.3.5.** 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.

**10.4.** Não ocorrendo inabilitação, o Pregoeiro consultará o Sistema de Cadastro Unificado de Fornecedores – SICAF, em relação à habilitação jurídica; à regularidade fiscal e trabalhista; e à qualificação econômica financeira conforme disposto no inciso III do art. 21 da Instrução Normativa SEGES/MPDG nº 03/2018. O SICAF também poderá ser utilizado para consulta no tocante à qualificação técnica conforme art. 6º, inciso V e art. 14 da mencionada instrução.

**10.4.1.** 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.

**10.4.2.** 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).

**10.5.** A verificação pelo órgão ou entidade promotora do certame nos sítios eletrônicos oficiais de órgãos e entidades emissores de certidões **constitui meio legal de prova,** para fins de habilitação.

**10.5.1.** Também poderão ser consultados os sítios oficiais emissores de certidões, especialmente quando o licitante esteja com alguma documentação vencida junto ao SICAF.

**10.6.** Não serão aceitos documentos com indicação de CNPJ diferentes, salvo aqueles legalmente permitidos, observado o item 6.5 deste edital.

**10.6.1.** 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.

**10.6.2.** 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.

**10.7. 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 **03 (três) horas**, sob pena de inabilitação.

**10.7.1**. A licitante poderá solicitar prorrogação do prazo de 03 (três) horas, desde que este não tenha se esgotado, através do próprio sistema do site https://www.gov.br/compras/pt-br/ ou pelo e-mail propostas.proad@ufca.edu.br.

**10.7.1.1.** A prorrogação dependerá de decisão do pregoeiro, pois não constitui direito do licitante e sempre será concedida no interesse da Administração.

**10.8. 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.**

**10.8.1**. **Caso o pregoeiro solicite**, os documentos serão remetidos em original, por qualquer processo de cópia reprográfica, autenticada por tabelião de notas, ou por servidor da Administração, desde que conferidos com o original, ou publicação em órgão da imprensa oficial, para o endereço da Coordenadoria de Licitações da UFCA, localizada no Centro Multiuso – "Vapt Vupt", Rua Interventor Francisco Erivano Cruz, nº 120, 3º andar, Centro, Juazeiro do Norte-CE, CEP: 63010-015.

**10.9.** 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.

**10.10.** Ressalvado o disposto no item 6.6, **os licitantes que não estiverem cadastrados no Sistema de Cadastro Unificado de Fornecedores – SICAF** além do nível de credenciamento exigido pela Instrução Normativa SLTI/MPOG nº 03, de 2018, deverão apresentar a seguinte documentação relativa à Habilitação Jurídica, à Regularidade Fiscal e trabalhista e a Qualificação Econômico-Financeira:

**10.11. HABILITAÇÃO JURÍDICA**

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

**10.11.2.** 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;

**10.11.3.** 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;

**10.11.4.** 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;

**10.11.5.** 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;

**10.11.6.** No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;

**10.11.7.** No caso de agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pela Secretaria Especial de Agricultura Familiar e do Desenvolvimento Agrário, nos termos do art. 4º, §2º do Decreto n. 7.775, de 2012.

**10.11.8.** No caso de produtor rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB n. 971, de 2009 (arts. 17 a 19 e 165).

**10.11.9.** No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

**10.11.10.**Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

**10.12. REGULARIDADE FISCAL E TRABALHISTA**

**10.12.1.** Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, se for o caso;

**10.12.2.** 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.

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

**10.12.4.**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 5.452, de 1º de maio de 1943;

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

**10.12.6.** Prova de regularidade com a Fazenda Estadual do domicílio ou sede do licitante;

**10.12.7.** Prova de regularidade com a Fazenda Municipal do domicílio ou sede do licitante;

**10.12.8.** Caso o fornecedor seja considerado isento dos tributos estaduais e/ou municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Estadual ou Municipal do domicílio ou sede do fornecedor, ou outra equivalente, na forma da lei;

**10.12.9. O licitante enquadrado como microempreendedor individual** que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal, na medida em que essas informações constem no Certificado de Condição de Microempreendedor Individual – CCMEI.

**10.12.10.** Caso o licitante detentor do menor preço seja microempresa, empresa de pequeno porte, ou sociedade cooperativa enquadrada no artigo 34 da Lei nº 11.488, de 2007,deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

**10.13. DA QUALIFICAÇÃO ECONÔMICO-FINANCEIRA**

**10.13.1.** A título de **QUALIFICAÇÃO ECONÔMICO-FINANCEIRA**, deverão apresentar o(s) seguinte(s) documento(s):

**10.13.2.** certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante, dentro do prazo de validade previsto na própria certidão ou, na omissão desta, expedida a menos de 180 (cento e oitenta) dias contados da data da sua apresentação;

**10.13.2.1. Caso a certidão seja positiva de recuperação,** cabe ao licitante apresentar o plano de recuperação aprovado e homologado judicialmente, na forma do art. 58 da lei 11.101, de 2005 (TCU, AC. 8271/2011 2º Câmara; Parecer nº 04/2015/CPLC/DEPCONSUIPGF/AGU; Nota técnica AGU/PGF/PF-UFCA nº 035/2017).

**10.13.2.2.** Se a empresa postulante à recuperação não obteve o acolhimento judicial de seu plano, não há demonstração da sua viabilidade econômica, não devendo ser habilitada no certame licitatório (TCU, AC. 8271/2011 2º Câmara; Parecer nº 04/2015/CPLC/DEPCONSUIPGF/AGU; Nota técnica AGU/PGF/PF-UFCA nº 035/2017).

**10.13.2.3.** É aplicável à empresa em recuperação extrajudicial, com plano de recuperação homologado judicialmente, a possibilidade de participar desta licitação, nos mesmos moldes da empresa em recuperação judicial. (TCU, AC. 8271/2011 2º Câmara; Parecer nº 04/2015/CPLC/DEPCONSUIPGF/AGU, Nota técnica AGU/PGF/PF-UFCA nº 035/2017).

**10.13.2.4.** A empresa em recuperação (extrajudicial ou judicial) com plano de recuperação acolhido, como qualquer licitante, deve demonstrar os demais requisitos para a habilitação econômico-financeira. (TCU, AC. 8271/2011 2º Câmara; Parecer nº 04/2015/CPLC/DEPCONSUIPGF/AGU, Nota técnica AGU/PGF/PF-UFCA nº 035/2017).

**10.13.3.** 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.

**10.13.3.1.** 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.

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

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

**10.13.4.** A comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas,**com os valores extraídos de seu balanço patrimonial ou apurados mediante consulta "on line", no caso de empresas inscritas no SICAF:**

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

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

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

**10.13.5.** As empresas, cadastradas ou não no SICAF, 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 estimado da contratação ou do item pertinente.

**10.13.6. O licitante enquadrado como microempreendedor individual** que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

**10.14. DA QUALIFICAÇÃO TÉCNICA**

**10.14.1.** As empresas cadastradas ou não no SICAF deverão comprovar, ainda, a **QUALIFICAÇÃO TÉCNICA**, por meio de:

**10.14.2.** Comprovação de aptidão para o fornecimento de bens ou prestação de serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, por meio da apresentação de um ou mais atestados fornecidos por pessoas jurídicas de direito público ou privado;

**10.14.2.1.** Os atestados de capacidade técnico-operacional deverão referir-se a serviços prestados/bens fornecidos no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

**10.14.2.2.** Poderá ser admitida, para fins de comprovação de quantitativo mínimo, a apresentação de diferentes atestados de serviços executados de forma concomitante, pois essa situação se equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação.

**10.14.2.3.** Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior.

**10.15.** Em relação às licitantes cooperativas será, ainda, exigida a seguinte documentação

complementar:

**10.15.1.** A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764 de 1971

**10.15.2.** A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

**10.15.3.** A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

**10.15.4.** O registro previsto no art. 107 da Lei nº 5.764, de 1971;

**10.15.5.** A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato;

**10.15.6.** Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

**10.15.7.** A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764/71 ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

**10.16.** 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.

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

**10.16.2.** Caso a proposta mais vantajosa seja ofertada por licitante qualificada como microempresa ou empresa de pequeno porte, 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.

**10.16.3.** 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.

**10.17.** 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.

**10.18.** Na hipótese de **não haver licitante classificado NA ETAPA DE LANCE FECHADO que atenda**

**às exigências para HABILITAÇÃO,** o pregoeiro poderá, assessorado pela equipe de apoio, admitir o reinício da etapa de envio de lances, mediante justificativa.

**10.19.** O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, caso lhe seja solicitado, apresentando cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram fornecidos os bens e/ou prestados os serviços, dentre outros documentos.

**10.20.** 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.

**10.20.1.** Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação.

**10.21.** Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

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

**11 DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA**

**11.1.** A proposta escrita deverá ser encaminhada nos seguintes moldes:

**11.1.1.** 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;

**11.1.2.** Conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento;

**11.1.3.** Conter as especificações do objeto, tais como marca, modelo, tipo, fabricante e procedência, se for o caso, ressalvando-se que a contratada estará vinculada a estes termos;

**11.1.4.** Conter o **prazo de validade de no mínimo 90 (noventa dias)**, consoante este edital, bem como o prazo correspondente à garantia do produto.

**11.1.5.** Ser datada conforme o dia em que for apresentada (anexada ao sistema do site https://www.gov.br/compras/pt-br/).

**11.1.6.** Ser assinada pelo representante legal da empresa, contendo, para fins de esclarecimento, o nome completo de quem assina, RG e CPF.

**11.2.** É vedado o uso do termo "conforme o edital" ou semelhantes visando substituir informação que deve constar expressamente na proposta

**11.3.** A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e no caso de eventual aplicação de sanção à Contratada.

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

**11.4.** Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso

**11.4.1.** Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros;

**11.4.2.** Havendo contradição entre o preço em algarismos e sua transcrição, prevalecerá o valor por extenso;

**11.4.3.** Os preços devem conter até duas casas decimais após a vírgula.

**11.5.** 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.

**11.6.** 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.

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

**12 DOS RECURSOS**

**12.1.** Declarado o vencedor e decorrida a fase de regularização fiscal da licitante qualificada como microempresa ou empresa de pequeno porte, se for o caso, será concedido **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.**

**12.2.** 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.

**12.2.1.** Nesse momento o Pregoeiro não analisará o mérito recursal (os motivos de quem recorre), mas apenas verificará as condições de admissibilidade do recurso (as condições de prazo e forma em que foi interposto).

**12.2.2.** A ausência de manifestação imediata e motivada do licitante, quanto à intenção de recorrer, importará na decadência desse direito, e o pregoeiro estará autorizado a adjudicar o objeto ao licitante declarado vencedor.

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

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

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

**13 DA REABERTURA DA SESSÃO PÚBLICA**

**13.1.** A sessão pública poderá ser reaberta:

**13.1.1.** 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.

**13.1.2.** Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar a Ata de Registro de Preços ou não comprovar a regularização fiscal, 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.

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

**13.2.1.** A convocação se dará por meio do sistema eletrônico ("chat"), e-mail, ou, ainda, fac-símile, de acordo com a fase do procedimento licitatório.

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

**14 DA ADJUDICAÇÃO E HOMOLOGAÇÃO**

**14.1.** Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto e homologará o procedimento licitatório.

**14.2.** Na ausência de recurso, caberá ao pregoeiro adjudicar o objeto e encaminhar o processo devidamente instruído à autoridade superior e propor a homologação.

**15 DA GARANTIA CONTRATUAL DOS BENS (ITENS 1 E 2 DO ANEXO I)**

**15.1.** A garantia contratual será exigida para o(s) item(ns) cuja(s) descrição(ões) expressamente a exija(m), em caráter complementar à garantia legal.

**16 DA GARANTIA DE EXECUÇÃO PARA O SERVIÇO DESIGNADO NO ITEM 3 (ANEXO I)**

**16.1.** Não haverá exigência de garantia de execução para a presente contratação.

**17 DA ATA DE REGISTRO DE PREÇOS**

**17.1**. Homologado o resultado da licitação, o adjudicatário terá o prazo de 10 (dez) dias, contados a partir da data de sua convocação, para assinar a ata de registro de preços, cujo prazo de validade encontra-se nela fixado, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

**17.1.1.** O adjudicatário será convocado a assinar enquanto for válida a proposta, dentro do prazo acima estabelecido pela Administração.

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

**17.2.** Alternativamente à(s) convocação(ões) para comparecer(em) perante o órgão ou entidade para a assinatura da Ata de Registro de Preços, a Administração poderá encaminhá-la para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinada no prazo fixado acima.

**17.3.**O prazo estabelecido para assinatura da Ata de Registro de Preços poderá ser prorrogado uma única vez, por igual período, quando solicitado pelo(s) licitante(s) vencedor(es), durante o seu transcurso, e desde que devidamente aceito.

**17.4.** É facultado à administração, quando o convocado não assinar a ata de registro de preços no prazo e condições estabelecidos, convocar os licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro classificado.

**17.5.** Será incluído na ata, sob a forma de anexo, o registro dos licitantes que aceitarem cotar os bens com preços iguais aos do licitante vencedor na sequência da classificação do certame, excluído o percentual referente à margem de preferência, quando o objeto não atender aos requisitos previstos no art. 3º da Lei nº 8.666, de 1993.

**17.6.** Serão formalizadas tantas Atas de Registro de Preços quanto necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor e dos licitantes que aceitarem cotar preços iguais aos deste, observada a ordem da última proposta apresentada durante a fase competitiva, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

**17.7.** Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar a ata de registro de preços, outro licitante poderá ser convocado, 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 a ata, sem prejuízo de eventual sanção.

**18 DA FORMAÇÃO DO CADASTRO DE RESERVA**

**18.1.** Após o encerramento da etapa competitiva, os licitantes poderão reduzir seus preços ao valor da proposta do licitante mais bem classificado.

**18.1.1.** A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante melhor classificado.

**18.2.** Havendo um ou mais licitantes que aceitem cotar suas propostas em valor igual ao do licitante vencedor, estes serão classificados segundo a ordem da última proposta individual apresentada durante a fase competitiva.

**18.3.** Esta ordem de classificação dos licitantes registrados deverá ser respeitada nas contratações e somente será utilizada caso o melhor colocado no certame não assine a ata ou tenha seu registro cancelado nas hipóteses previstas nos artigos 20 e 21 do Decreto n° 7.892/2013.

**19 DA VIGÊNCIA, DA ALTERAÇÃO E DO CANCELAMENTO DA ATA**

**19.1. A Ata de Registro de Preços terá vigência de 12 (doze) meses,** improrrogáveis, a contar da data de sua publicação.

**19.2.** A alteração da Ata de Registro de Preços e o cancelamento do registro do fornecedor obedecerão à disciplina do Decreto n° 7.892/13, e suas atualizações, conforme previsto na Minuta da Ata de Registro de Preços anexa ao Edital.

**19.3.** É vedado efetuar acréscimos nos quantitativos fixados pela ata de registro de preços, inclusive o acréscimo de que trata o § 1º do art. 65 da Lei nº 8.666/93.

**20 DO REAJUSTAMENTO EM SENTIDO GERAL**

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

**21 DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE**

**21.1.** Dentro da validade da Ata de Registro de Preços, o fornecedor registrado poderá ser convocado para assinar Termo de Contrato ou aceitar/retirar instrumento equivalente (Nota de Empenho/Carta Contrato/Autorização).

**21.1.1.** O adjudicatário terá o prazo de 10 (dez) dias, 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.

**21.1.2.** 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.

**21.2.** 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.

**21.3.** O prazo previsto originalmente poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

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

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

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

**21.4.3** 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.

**21.5.** 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.

**21.5.1** 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.

**21.5.2** 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.

**21.6.** Se o adjudicatário, no ato da assinatura do Termo de Contrato, não comprovar que mantém as mesmas condições de habilitação, ou quando, injustificadamente, recusar-se à assinatura, poderá ser convocado outro licitante, desde que respeitada a ordem de classificação, para, após a verificação da aceitabilidade da proposta, negociação e comprovados os requisitos de habilitação, celebrar a contratação, sem prejuízo das sanções previstas neste Edital e das demais cominações legais.

**21.7.** O prazo de vigência do termo de contrato será de 12 (doze) meses, prorrogável de acordo com o disposto na minuta do contrato anexada a este edital.

**22 DA ENTREGA E DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO**

**22.1.** Os critérios de recebimento e aceitação do objeto e de fiscalização estão previstos no Anexo I (Termo de Referência).

**23 DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA**

**23.1.** As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência (Anexo I deste edital).

**23.2.** É obrigação da contratada o fornecimento do(s) objeto(s) contratado(s) de acordo com os

critérios de sustentabilidade ambiental contidos na Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI/MPOG).

**23.3.** No tocante ao fornecimento dos bens – itens 1 e 2 do Anexo I, a contratada deve fazê-lo de forma parcelada conforme o Anexo I.

**24 DO PAGAMENTO – PARA O ITEM 3 DO ANEXO I**

**24.1.** O pagamento será efetuado pela Contratante no prazo de 30 (trinta) dias, contados do recebimento da Nota Fiscal/Fatura.

**24.2.** É admitida a cessão de crédito decorrente da contratação de que trata este Instrumento Convocatório, nos termos do previsto na minuta contratual anexa a este Edital.

**24.3.** A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do serviço, conforme estabelecido no Termo de Referência.

**24.4.** Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

**24.5.** Havendo instrumento de fiscalização e medição da qualidade definido no Anexo I (Termo de referência), o pagamento estará condicionado ao atendimento das metas nele estabelecidas. A contratada, portanto, será comunicada para que emita a Nota Fiscal ou Fatura com o valor exato dimensionado pela fiscalização com base no Instrumento de Medição.

**24.6.** Caberá retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a contratada:

**24.6.1.** não produziu os resultados acordados;

**24.6.2.** deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida descrita no item 7 - MODELO DE GESTÃO DO CONTRATO (Anexo I);

**24.6.3.** deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada descritas no item 7 - MODELO DE GESTÃO DO CONTRATO (Anexo I).

**24.7.** Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

**24.8.** Considera-se ocorrido o recebimento da Nota Fiscal ou Fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

**24.8.1.** O pagamento somente será autorizado depois de efetuado o “atesto” pelo servidor competente, devidamente acompanhada das comprovações mencionadas no Anexo XI da IN SEGES/MPDG n. 5/2017.

**24.9**. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

**24.10.** Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a

manutenção das condições de habilitação exigidas no edital.

**24.11.** Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

**24.12.** Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

**24.13.** Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

**24.14.** Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

**24.15.** Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, nos termos do item 6 do Anexo XI da IN SEGES/MPDG n. 5/2017, quando couber:

**24.15.1.** A Contratada regularmente optante pelo Simples Nacional, exclusivamente para as atividades de prestação de serviços previstas no §5º-C, do artigo 18, da LC 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime, observando-se as exceções nele previstas. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

**24.16.** Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

| | | |
|---|---|---|
| I = (TX) | I = $\frac{(6/100)}{365}$ | I = 0,00016438<br>TX = Percentual da taxa anual = 6% |

**25 DO PAGAMENTO – PARA OS ITENS 1 e 2 DO ANEXO I**

**25.1. O pagamento será realizado no prazo máximo de até 30 (trinta) dias,** contados a partir da data final do período de adimplemento a que se referir, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

**25.2.** É admitida a cessão de crédito decorrente da contratação de que trata este Instrumento Convocatório, nos termos do previsto na minuta contratual anexa a este Edital.

**25.3.** Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados **no prazo de até 5 (cinco) dias úteis**, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

**25.4. O pagamento somente será autorizado depois de efetuado o "atesto"** pelo servidor competente na nota fiscal apresentada.

**25.5.** Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

**25.6.** Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

**25.7.** Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

**25.8.** Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

**25.9.** Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

**25.10.** Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

**25.11.** Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

**25.12.** Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

**25.12.1.** A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

**25.13.** Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

| | | |
|---|---|---|
| I = (TX) | I = (6/100)<br>365 | I = 0,00016438<br>TX = Percentual da taxa anual = 6% |

**26 DAS SANÇÕES ADMINISTRATIVAS**

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

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

**26.1.2.** não assinar a ata de registro de preços, quando cabível;

**26.1.3.** apresentar documentação falsa;

**26.1.4.** deixar de entregar os documentos exigidos no certame;

**26.1.5.** ensejar o retardamento da execução do objeto;

**26.1.6.** não mantiver a proposta;

**26.1.7.** cometer fraude fiscal;

**26.1.8.** Comportar-se de modo inidôneo:

**26.1.8.1.** 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;

**26.1.9.** Aquele que cometer quaisquer das infrações acima e/ou falhar na execução do contrato, garantido o direito à ampla defesa, ficará impedido de licitar e de contratar com a União, e será descredenciado no SICAF, pelo prazo de até cinco anos, sem prejuízo das sem prejuízo da responsabilidade civil e criminal.

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

**26.2.** O licitante/contratado que cometer qualquer das infrações anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções extraídas do Termo de Referência (Anexo I):

**26.2.1.** Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para a Administração;

**26.2.2. Multa de**:

**26.2.2.1.** 0,1% (um décimo por cento) por dia sobre o valor adjudicado em caso de atraso na execução do objeto, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

**26.2.2.2.** 5% (cinco por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem anterior ou de inexecução parcial da obrigação assumida;

**26.2.2.3.** 10% (dez por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

**26.2.2.4.** 0,02% a 0,32% por dia sobre o valor total do contrato, conforme detalhamento constante das tabelas abaixo;

**26.3.** A multa deverá ser depositada na conta da contratante pelo contratado, mediante guia de recolhimento a ser fornecida pela autoridade aplicadora da multa;

**26.3.1.** As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si;

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

**26.3.3.** As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

**26.3.4.** Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

**26.4.** 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;

**26.5.** Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

**26.5.1.** A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa;

**26.6.** 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;

**26.6.1.** A mera participação de pessoa jurídica autodeclarada como microempresa ou empresa de pequeno porte visando os benefícios concedidos pela LC 123/2006 que tenha participação societária em outra pessoa jurídica, é fato que contraria o art. 3º, § 4º, inciso VII, dessa lei, ensejando a declaração de inidoneidade do fraudador(AC. 2891/2019 – TCU – Plenário).

**26.7.** Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas a seguir:

| Grau | Correspondência |
|---|---|
| 1 | 0,02% ao dia sobre o valor total do |

| | |
|---|---|
| | contrato |
| 2 | 0,04% ao dia sobre o valor total do contrato |
| 3 | 0,08% ao dia sobre o valor total do contrato |
| 4 | 0,16% ao dia sobre o valor total do contrato |
| 5 | 0,32% ao dia sobre o valor total do contrato |

Tabela Grau de Infrações

| Item | Correspondência | Grau |
|---|---|---|
| 1 | Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais, por ocorrência | 5 |
| 2 | Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento | 4 |
| 3 | Manter funcionário sem qualificação para executar os serviços contratados, por empregado e por dia. | 3 |
| 4 | Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia. | 2 |
| 5 | Deixar de cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência. | 2 |
| 6 | Deixar de substituir empregado alocado que não atenda às necessidades do serviço, por funcionário e por dia. | 2 |
| 7 | Deixar de indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato. | 1 |

Tabela Infrações

**26.8.** Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

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

b) tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

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

**26.9.** Se, durante o processo de aplicação de penalidade, 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.

**26.10.** 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.

**26.11.** 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.

**26.12.** 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.

**26.13.** 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.

**26.14.** 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.

**26.15.** A aplicação das sanções previstas neste Edital não exclui a possibilidade de aplicações de outras, previstas em Lei, inclusive responsabilização do fornecedor por eventuais perdas e danos causados à Administração.

**26.16.** As penalidades serão obrigatoriamente registradas no SICAF.

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

**27 DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO**

**27.1. Qualquer pessoa poderá impugnar** os termos do edital do pregão, por meio eletrônico, na forma prevista no edital**, até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública.**

**27.2.** A impugnação poderá ser realizada por forma eletrônica, pelo e-mail impugna.proad@ufca.edu.br dentro do prazo mencionado.

**27.3.** Acolhida a impugnação contra o edital, será definida e publicada nova data para realização do certame.

**27.4. 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, através do e-mail: impugna.proad@ufca.edu.br.

**27.5.** 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.

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

**27.7.** A impugnação não possui efeito suspensivo e caberá ao pregoeiro, auxiliado pelos responsáveis pela elaboração do edital e dos anexos, decidir sobre a impugnação no prazo de dois dias úteis, contado da data de recebimento da impugnação.

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

**27.8.** As respostas às impugnações e os esclarecimentos prestados pelo Pregoeiro serão entranhados nos autos do processo licitatório e estarão disponíveis para consulta por qualquer interessado.

**27.9.** As respostas aos pedidos de esclarecimentos vincularão os participantes e a administração.

**27.10**. **Modificações no edital** (incluindo as oriundas de impugnação acolhida) **serão divulgadas pelo mesmo instrumento de publicação utilizado para divulgação do texto original e o prazo** inicialmente estabelecido **será reaberto, EXCETO SE**, inquestionavelmente, a alteração não afetar a formulação das propostas, resguardado o tratamento isonômico aos licitantes.

**28. DAS DISPOSIÇÕES FINAIS**

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

**28.1.1.** A autoridade competente para homologar o procedimento licitatório poderá revogá-lo somente em razão do interesse público, por motivo de fato superveniente devidamente comprovado, pertinente e suficiente para justificar a revogação, e deverá anulá-lo por ilegalidade, de ofício ou por provocação de qualquer pessoa, por meio de ato escrito e fundamentado.

**28.1.2.** Os licitantes não terão direito à indenização em decorrência da anulação do procedimento licitatório, ressalvado o direito do contratado de boa-fé ao ressarcimento dos encargos que tiver suportado no cumprimento do contrato.

**28.2.** 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.

**28.3.** 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.

**28.4.** 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.

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

**28.6.** Em caso de divergência entre disposições deste Instrumento convocatório e de seus anexos (ou demais peças que compõem o processo) prevalecerão aquelas constantes deste Edital.

**28.7.** O Edital está disponibilizado, na íntegra, no endereço eletrônico https://www.gov.br/compras/pt-br/ e também poderão ser lidos e/ou obtidos na Coordenadoria de Licitações, localizada no Centro Multiuso – "Vapt Vupt", Rua Interventor Francisco Erivano Cruz, nº 120, 3º andar, Centro, Juazeiro do Norte-CE, CEP: 63010-015, em dias úteis, no horário das 08h:00 às 12h:00min e das 13h:00min às 17h:00min, mesmo endereço e período nos quais os autos do processo administrativo permanecerão com vista franqueada aos interessados.

**28.8.** Este edital está em conformidade com o modelo do sítio da Advocacia-Geral da União - http://www.agu.gov.br/ da Comissão Permanente de Atualização de Editais da Consultoria-Geral da União.

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

ANEXO I – Termo de Referência;

ANEXO II – Modelo de Proposta;

ANEXO III – Minuta de Ata de Registro de Preços;

ANEXO IV – Minuta do Termo de Contrato.

Juazeiro do Norte-CE, 29 de outubro de 2020

_____

Silvério de Paiva Freitas Júnior

Pró-Reitor de Administração

**MINISTÉRIO DA EDUCAÇÃO**
**UNIVERSIDADE FEDERAL DO CARIRI**
**Pró-Reitoria de Administração**
**ANEXO I – TERMO DE REFERÊNCIA**

# TERMO DE REFERÊNCIA

**PROCESSO ADMINISTRATIVO Nº 23507.002141/2020-56**

## SOLUÇÕES DE GERENCIAMENTO E SEGURANÇA DE REDES

**JUAZEIRO DO NORTE-CE, SETEMBRO DE 2020**

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

## HISTÓRICO DE REVISÕES

| Data | Versão | Descrição | Autor |
|---|---|---|---|
| 23/07/2020 | 1.0 | Finalização da primeira versão do documento | Equipe de Planejamento da Contratação |
| 06/08/2020 | 2.0 | Revisão do documento | Equipe de Planejamento da Contratação |
| 04/09/2020 | 2.1 | Revisão do documento | Equipe de Planejamento da Contratação |
| 18/09/2020 | 2.3 | Modicação do documento | Equipe de Planejamento da Contratação |

**TERMO DE REFERÊNCIA**

Referência: Arts. 12 a 24 IN SGD-ME Nº 1/2019

## 1. OBJETO DA CONTRATAÇÃO

1.1. Registro de preço para contratação de empresa especializada para fornecimento de licenças para expansão do sistema de gerenciamento de rede e de solução de proteção de dados (Firewall), conforme especificações constantes neste Termo de Referência.

## 2. 2 – DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. Bens e serviços que compõem a solução

| Item | Descrição do Bem ou Serviço | CATMAT /CATSER | Quantidade | Métrica ou Unidade |
|---|---|---|---|---|
| 1 | SOLUÇÃO DE PROTEÇÃO DE DADOS FIREWALL TIPO 01 \| LICENÇA CONTRA AMEAÇAS CONHECIDAS \| LICENÇA PARA BLOQUEIO DE URL E CATEGORIAS DE SITES MALICIOSOS \| 60 MESES DE SUPORTE E GARANTIA \| SERVIÇO DE INSTALAÇÃO PROFISSIONAL | 150100 | 02 | UN |
| 2 | SOLUÇÃO DE PROTEÇÃO DE DADOS FIREWALL TIPO 02 \| LICENÇA CONTRA AMEAÇAS CONHECIDAS \| LICENÇA PARA BLOQUEIO DE URL E CATEGORIAS DE SITES MALICIOSOS \| 60 MESES DE SUPORTE E GARANTIA \| SERVIÇO DE INSTALAÇÃO PROFISSIONAL | 150100 | 04 | UN |
| 3 | LICENÇA PARA EXPANSÃO DE SISTEMA DE GERENCIAMENTO DE REDE. MARCA: HPE, MODELO: INTELLIGENT MANAGEMENT CENTER (IMC) ENTERPRISE EDITION (JG748AAE). A LICENÇA DEVE SER PERPÉTUA E CADA PACOTE DEVERÁ ADICIONAR O SUPORTE A GERÊNCIA DE 50 DISPOSITIVOS, SOMANDO-SE ÀS LICENÇAS JÁ EXISTENTES. | 27464 | 04 | UN |

2.2. A existência de preços registrados não obriga a Administração a firmar contratações que deles poderão advir, facultando-se a realização de licitação específica para a contratação pretendida, sendo assegurada ao beneficiário do Registro a preferência de fornecimento em igualdade de condições;

2.3. As quantidades previstas neste Termo de Referência são estimativas máximas para o período de validade deste Registro de Preços, e a Universidade Federal do Cariri se reserva o direito de adquirir, em cada item, o quantitativo que julgar necessário, podendo ser parcial, integral ou abster-se de adquirir algum item especificado;

2.4. Deve-se ser considerado pelos licitantes interessados sobre a possibilidade da UFCA emitir Notas de Empenho com quantitativos que podem variar de zero até o máximo previsto para cada item.

## 3. JUSTIFICATIVA PARA A CONTRATAÇÃO

**3.1. Contextualização e Justificativa da Contratação:**

3.1.1. Para os ITENS 01 e 02:

a) Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, seja em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, dados pessoais ou informações importantes. Os criminosos virtuais podem ter diversos objetivos e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados importantes criptografados (como reféns), até que a instituição pague um valor como resgate pela liberação destas informações ou até mesmo fazendo uso indevido dos dados para vantagens próprias.

b) A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição, faz crescer a preocupação de todos sobre a proteção dos dados e da privacidade dos seus cidadãos. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrará em vigor a partir de agosto de 2020, descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, exige que as instituições invistam mais em recursos tecnológicos para aprimorar sua segurança da informação. Um simples vazamento de informações pessoais de qualquer cidadão pode acarretar sanções administrativas que vão desde uma advertência, com indicação de prazo para adoção de medidas corretivas, até multa e publicitação da infração após devidamente apurada, o que não é favorável para a imagem e "saúde" de qualquer instituição.

c) Um simples acesso à internet pelos membros desta instituição pode sujeitá-los a riscos de trazerem para a rede local softwares mal-intencionados (malwares) que podem causar interrupção do funcionamento da rede, dos computadores e, consequentemente, a interrupção de serviços administrativos e operacionais do dia-a-dia da instituição. Uma solução de firewall de próxima geração funciona como um filtro eletrônico que examina todo o tráfego da rede sinalizando quais operações de transmissão e recebimento de dados têm a possibilidade de serem executadas ou não. Além disso, o firewall evita que os usuários acessem conteúdos ilícitos, protegendo contra todas as ameaças originárias deste tipo de conteúdo, garantindo a integridade e a segurança dos dados e informações pessoais ou corporativas.

d) O firewall de próxima geração, além de impedir que hackers ou softwares mal-intencionados obtenham acesso indevido à rede através da Internet, também impede que um computador propague um software mal-intencionado para outros computadores da mesma rede. Uma das principais motivações para a execução deste projeto são as ameaças emergentes e, muitas vezes, direcionadas à ambientes públicos, onde o atacante pode, inclusive estar dentro do ambiente, necessitando ser detectado e remediado imediatamente.

e) Atualmente a UFCA possui 01 equipamento (appliance) do tipo firewall no Campus Juazeiro do Norte que opera nas redes dos campi e do datacenter. Este equipamento é de modelo Palo Alto Networks PA-3020, nº de série 001801027906 e patrimônio 0000001057. O mesmo se encontra sem garantia desde 22 de fevereiro de 2019 e foi descontinuado conforme informação do fabricante em:

f) https://www.paloaltonetworks.com/services/support/end-of-life-announcements/end- of-sale.

g) O que deixa uma este equipamento com um fim de vida anunciado no quesito atualizações do sistema operacional, para correção de bugs e novas funcionalidades, e proteções contra ameaças, colocando em risco a rede da universidade contra novas ameaças e suporte de garantia limitado, sendo necessária a atualização de equipamento, mantendo assim a rede completamente protegida. Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais da UFCA.

h) Visando a proteção da rede de dados dos Campi da UFCA, é necessária a aquisição de novas soluções de segurança de redes (Firewall), com características de Next Generation Firewall (NGFW). É pretendido a aquisição de 02 appliances para o Campus Juazeiro do Norte, os mesmos formarão um sistema de alta disponibilidade (HA:High-Availability), resistente a falhas de hardware, software e energia, cujo objetivo é manter os serviços disponíveis o máximo de tempo possível. Foi especificado um objeto mais robusto para atender esse campus, pois concentra a maior parte do volume de dados da instituição

i) Para os Campi: Barbalha, Brejo Santo, Crato e Reitoria é pretendido a aquisição de 01 appliance de menor capacidade para cada campus, porém que atenda de forma eficiente as demandas de segurança habituais geradas pelas redes de dados de cada localidade.

3.1.2. Para o ITEM 03:

a) A Divisão de Redes e Telefonia realizou, recentemente, a aquisição de novos switches gerenciáveis visando melhorar a performance da rede de dados, expandir e atender a demanda gerada com a construção e entrega de novos prédios. Como as atividades de configurações, identificação de problemas de acesso e gerência destes switches é uma atividade rotineira, utiliza-se um sistema centralizado para realizar essas funções, tornando ágil, padronizado e mais eficiente o tempo para identificação e resolução de problemas. Todavia, o sistema de gerenciamento atual, IMC (Intelligent Management Center), do fabricante HPE, está com sua capacidade total utilizada, o que faz com que os novos switches sejam acessados individualmente para configuração e manutenção, demandando um tempo muito maior despendido pela equipe técnica e possibilitando a perda da padronização de configurações da rede, assim como dificuldade para realização de backups das configurações dos novos switches.

**3.2. Das justificativas para adoção do Sistema de Registro de Preços:**

3.2.1. Segundo o art. 3º do Decreto Federal 7.892/2013: “O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:

> I - Quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;

> II - Quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;
>
> III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; ou
>
> IV - Quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração" (grifado).

3.2.2. Dessa forma, a licitação para registro de preços será realizada nos termos da Lei nº 8.666, de 1993, de acordo com o Decreto Federal nº 7.892/2013.

3.2.3. Em consonância com o inciso II do Art. 3 do Decreto nº 7.892/2013, "II -Quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa", a justificativa da SRP se justifica pautado na intenção de uma implementação gradativa das soluções.

3.2.4. **Da Natureza dos Bens e/ou Serviços**:

a) Quanto ao tipo, em conformidade com o art. 1° da Lei n° 10.520/2002 e com o Decreto n° 10.024/2019, o OBJETO pretendido enquadra-se como "COMUM" por apresentar, independentemente de sua complexidade, "padrões de desempenho e qualidade que possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado.

## 3.3. Alinhamento aos Instrumentos de Planejamento Institucionais:

| ALINHAMENTO AOS PLANOS ESTRATÉGICOS | |
|---|---|
| ID | Objetivos Estratégicos do Planejamento Estratégico Institucional a Universidade Federal do Cariri – PEI/UFCA 2025 |
| OB15 | Redimensionar e ampliar a infraestrutura física e tecnológica, com foco na sustentabilidade. |

| ALINHAMENTO AO PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DO CARIRI PDTI-UFCA 2019-2022 | | | |
|---|---|---|---|
| ID | Ação do PDTI | ID | Meta do PDTI associada |
| A025 | Renovar os equipamentos de TI obsoletos | OB07 | Manter os serviços de TI disponíveis |
| | | OB08 | Garantir a atualização dos equipamentos de TI |

| ALINHAMENTO AO PLANO DE COMPRAS DA UFCA - 2020 | |
|---|---|
| Item | Descrição |
| TIC1 | Storage, backup, switch tor, firewall e software para gestão do datacenter |

## 3.4. Estimativa da demanda:

3.4.1. Devido a necessidade da universidade em renovar a solução de firewall de próxima geração existente e ampliar a abrangência de proteção baseada na mesma solução, as quantidades abaixo foram estimadas no estudo técnico para compor o projeto em sua totalidade.

3.4.2. Atualmente o firewall existente, além de desatualizado, está com carga de processamento acima do esperado e recomendado pelas melhores práticas do fabricante, chegando a altos picos de uso de CPU em vários momentos. Considerando a ampliação da rede

de dados e o consumo de processamento mostrado acima, foi dimensionada uma nova arquitetura de rede de dados para melhor aproveitamento da solução existente e atendimento das novas demandas, onde o equipamento existente terá carga de processamento reduzida e o(s) novo(s) equipamento(s) assumirá(ão) o tráfego de rede. Esta realocação do firewall atual, fará com que o investimento feito anteriormente continue efetivo.

3.4.3. Ainda na linha de gerenciamento unificado, a universidade possui um sistema gerenciamento centralizado para os switches, e se faz necessário a inclusão de licenciamento para os switches adquiridos no ano de 2019, com estas licenças pode-se configurar todos os switches a partir de um ponto único e acompanhar a saúde sistêmica deles, unificadamente.

3.4.4. A tabela a seguir contém o quantitativo total, obtido no Estudo Técnico Preliminar:

| Item | Descrição | Qtd |
|---|---|---|
| 1 | SOLUÇÃO DE PROTEÇÃO DE DADOS FIREWALL TIPO 01 \| LICENÇA CONTRA AMEAÇAS CONHECIDAS \| LICENÇA PARA BLOQUEIO DE URL E CATEGORIAS DE SITES MALICIOSOS \| 60 MESES DE SUPORTE E GARANTIA \| SERVIÇO DE INSTALAÇÃO PROFISSIONAL | 02 |
| 2 | SOLUÇÃO DE PROTEÇÃO DE DADOS FIREWALL TIPO 02 \| LICENÇA CONTRA AMEAÇAS CONHECIDAS \| LICENÇA PARA BLOQUEIO DE URL E CATEGORIAS DE SITES MALICIOSOS \| 60 MESES DE SUPORTE E GARANTIA \| SERVIÇO DE INSTALAÇÃO PROFISSIONAL | 04 |
| 3 | LICENÇA PARA EXPANSÃO DE SISTEMA DE GERENCIAMENTO DE REDE. MARCA: HPE, MODELO: INTELLIGENT MANAGEMENT CENTER (IMC) ENTERPRISE EDITION (JG748AAE). A LICENÇA DEVE SER PERPÉTUA E CADA PACOTE DEVERÁ ADICIONAR O SUPORTE A GERÊNCIA DE 50 DISPOSITIVOS, SOMANDO-SE ÀS LICENÇAS JÁ EXISTENTES. | 04 |

**3.5. Parcelamento da Solução de TIC:**

3.5.1. Depois de análise realizada pela equipe de planejamento da contratação foi constatado que a solução dividida em lotes não seria a ideal para a contratação dos objetos deste Termo de Referência, pois limitaria a livre concorrência de fornecedores na fase de contratação. Na escolha da divisão por itens foi levado em consideração a não dependência dos objetos a serem contratados, ou seja, os 03 (três) itens não necessariamente, devem compor uma solução unificada.

**3.6. Resultados e Benefícios a Serem Alcançados:**

3.6.1. Para os ITENS 01 e 02:

a) Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

b) Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;

c) Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;

d) Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet;

e) Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio de aplicações como programas de compartilhamento de dados

(P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;

f) Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);

g) Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

h) Minimizar as ameaças virtuais ao ambiente computacional da UFCA, com capacidade de identificar ameaças complexas e avançadas de forma automática;

i) Garantir a segurança da informação trafegada na rede de dados e proteção dos dados armazenados nas estações de trabalho da UFCA;

j) Melhoria do processo de resposta a incidentes, com a capacidade de análise e rastreabilidade a partir de uma gerência centralizada, assim, minimizando os custos de operação e administração das rotinas de segurança e auditoria;

k) Capacidade de oferecer proteção e análise aos segmentos e maior throughput da rede;

l) Monitoração segura e não intrusiva dos acessos realizados aos recursos na rede;

m) Maior poder e autonomia da área de segurança no tocante ao gerenciamento dos acessos aos sistemas e aplicações;

n) Aumento do sigilo das informações tratadas em aplicações em rede com a redução de riscos de ataques e maior rastreabilidade quanto às tentativas de invasão.

3.6.2. Para o ITEM 03:

a) Continuidade e expansão do licenciamento do Sistema atual de Gerenciamento de Redes, administrado pela DTI/Divisão de Redes e Telefonia;

b) Continuidade e expansão da segurança, eficiência, confiabilidade e celeridade à execução das atividades;

c) Continuidade da visibilidade do tráfego de rede, visualização de topologia de rede, com a capacidade de monitorar e gerenciar dispositivos;

d) Gerência das VLANs globalmente ou por dispositivo e criação de VLANs padronizadas uma a uma ou em lote;

e) Continuidade da Análise de Tráfego de Rede através de módulo NTA - Network Traffic Analyzer.

## 4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. As especificações técnicas dos itens estão descritas no **ANEXO III - ESPECIFICAÇÕES TÉCNICAS** deste Termo de Referência.

**4.2. Requisitos de Negócio:**

4.2.1. Para os itens 01 e 02:

a) Contratação de empresa especializada para o fornecimento de solução de firewall (proteção de dados);

b) Solução para manter visibilidade de todo o tráfego que se passa na infraestrutura de rede de dados da UFCA, permitindo que a DTI seja proativa na detecção de problemas;

c) Garantir um satisfatório nível de segurança no ambiente de TI da UFCA, protegendo contra qualquer tipo de tentativa de invasão ou ataque;

d) Suporte técnico e repasse de conhecimento (hands on) de toda a solução a fim de atender às necessidades da UFCA;

4.2.2. Para o ITEM 03:

a) Contratação de empresa para fornecimento de licença para sistema de gerenciamento de redes, essas licenças deverão ser totalmente integrados em todas as suas funcionalidades ao software em produção na UFCA, modelo "HPE IMC Enterprise Edition (JG748AAE)", para aproveitamento de sistema legado;

b) Não serão aceitos licenças que recusem qualquer acesso e/ou não suporte a um recurso disponibilizado pelo "Sistema de Gerenciamento de Rede" em produção na UFCA;

**4.3. Requisitos de Capacitação:**

4.3.1. Para os ITENS 01 e 02:

a) Deverá ser realizada capacitação do corpo técnico indicado pela CONTRATANTE através de treinamento (do tipo hand's on) oferecido pela CONTRATADA, para a administração e gerenciamento do ambiente;

b) A capacitação deve fornecer instruções para criação, manutenção e administração do ambiente.

c) A capacitação é considerada como um importante requisito de manutenção já que, após o fim do contrato, é importante que a equipe tenha domínio total para manter a solução em pleno funcionamento;

d) Em função da equipe já estar familiarizada com produtos de segurança e rede já instalados, deverá ser ministrado um treinamento do tipo hand's on com duração de, pelo menos, 8 (oito) horas por técnico responsável da CONTRATADA. Este treinamento deverá contemplar orientações de tarefas e funcionalidades de administração diárias.

4.3.2. Para o ITEM 03:

a) Não se aplica.

**4.4. Requisitos Legais:**

4.4.1. Para TODOS OS ITENS:

a) Lei nº 8.666, de 21 de julho de 1993, que institui normas para licitações e contratos da Administração Pública;

b) Lei nº 10.520, de 17 de julho de 2002, que institui modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns;

c) Lei nº 8.248, de 23 de outubro de 1991, que dispõe sobre a capacitação e competitividade do setor de informática e automação;

d) Decreto nº 3.555, de 08 de agosto de 2000, que aprova o regulamento para modalidade de licitação denominado pregão, para aquisição de bens e serviços comuns;

e) Decreto nº 10.024, de 20 de setembro de 2019, que regulamenta o pregão, na forma eletrônica, para bens e serviços comuns;

4.4.2. O presente processo de contratação deve estar aderente à Constituição da República Federativa do Brasil de 1988, Decreto-Lei nº 200/1967, Decreto 10.024/2019 (Pregão Eletrônico), Decreto 7.892/2013 (Registro de Preços), IN. 01/2019 SGD/ME (Contratação de Soluções de TIC) e legislação específica aplicada.

**4.5. Requisitos de Manutenção:**

4.5.1. Para os ITENS 01 e 02:

a) A garantia e suporte técnico da Solução deverão ser prestadas conforme especificado dentro de cada item descrito neste Termo de Referência, pelo período contratado. Os técnicos envolvidos deverão estar treinados no processo de instalação e configuração do ambiente. Dentre as vantagens de possuir um contrato de manutenção ativo, destacam-se:

4.5.1.a.1. Hardware: possibilidade de troca de equipamento ou peça no caso de falha, possibilidade de atualização de firmware para melhoria de operação ou utilização de novos recursos do equipamento, suporte da CONTRATADA na resolução de problemas graves;

4.5.1.a.2. Software: possibilidade de atualização das versões de software durante o período de garantia. As atualizações são úteis para resolução de problemas (bugs), correções de segurança e implantação de novos recursos/funcionalidades da solução.

b) Mecanismo de continuidade: Solução continuará funcionando, mesmo sem contrato de suporte;

c) O suporte técnico deverá estar disponível, no mínimo, em horário comercial, 05 (cinco) dias por semana; Disponibilidade para abertura de chamado: 24x7x365 (web, e-mail ou telefone gratuito 0800) com disponibilidade para início de atendimento definidos no item 7.3 deste Termo de Referência.

d) O suporte técnico inicial deverá ser prestado em horário comercial, de forma remota ou presencial;

e) Apoio a dúvidas de configurações, funcionamento, atualizações de versões;

f) Análises e soluções de alertas e problemas apresentados pela solução;

g) Caso haja necessidade de intervenção local, esta poderá ser executada, sempre com acompanhamento pela equipe técnica da UFCA. O atendimento

deverá ser realizado por técnicos da CONTRATADA, em língua portuguesa ou oferecer um tradutor;

h) Acesso web à base de conhecimento oficial; Abertura ilimitada de chamados de suporte.

**4.6. Para o ITEM 03:**

4.6.1. Não se aplica.

**4.7. Requisitos Temporais:**

4.7.1. Para TODOS OS ITENS:

a) O prazo para a entrega, instalação e configuração da solução será de até 60 (sessenta) dias consecutivos, contados a partir do primeiro dia útil após a emissão da Ordem de Serviço.

**4.8. Requisitos de Segurança:**

4.8.1. Para os ITENS 01 e 02

a) A CONTRATADA deverá fornecer aos funcionários os equipamentos de segurança que se fizerem necessários, para a execução dos serviços de instalação da Solução;

b) A CONTRATANTE deverá liberar o acesso dos funcionários da CONTRATADA e servidores técnicos ao Data Center e aos sistemas necessários;

c) Todo e qualquer tipo de acesso on-site ou remoto necessário ao suporte da solução deverá ser previamente autorizado pela CONTRATANTE e respeitar as normas vigentes da UFCA, mantendo o sigilo e a confidencialidade de qualquer informação que venha a obter conhecimento;

4.8.2. Para o ITEM 03:

a) Não se aplica.

**4.9. Requisitos Sociais, Ambientais e Culturais:**

4.9.1. Para os ITENS 01 e 02:

a) Utilizar equipamentos, quando aplicável, homologados pela Anatel e/ou ABNT, no que diz respeito a normas ambientais;

b) Respeitar as Normas Brasileiras - NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos, incluindo práticas de logística reversa, conforme o caso;

c) Dar preferência ao uso de bens constituídos por material reciclado, atóxico, biodegradável, conforme ABNT NBR - 15448-1 e 15448-2;

d) Acondicionar os bens preferencialmente em embalagem individual adequada, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;

e) Que os bens não contenham substâncias perigosas em concentração acima das recomendadas pelas normas técnicas;

f) Todos documentos ou artefatos gerados pela contratada, salvo manifestação explícita pela UFCA deverão ser entregues em formato digital;

g) A documentação dos produtos que integram a presente solução deverá estar, preferencialmente, na língua portuguesa do Brasil;

h) O presente processo deve estar aderente à Lei 12.305/ 2010 que Institui a Política Nacional de Resíduos Sólidos.

4.9.2. Para o ITEM 03:

a) Não se aplica.

**4.10. Requisitos de Arquitetura Tecnológica:**

4.10.1. Para os ITENS 01 e 02:

a) Disponibilidade de espaço físico nos racks da sala de redes para instalação de hardwares disponíveis.

4.10.2. Para o ITEM 03:

a) Permitir acesso, acesso a VM onde o software de gerenciamento de redes "Intelligent Management Center-IMC" está instalado para inclusão da licença adquirida, por técnico indicado pela CONTRATADA;

**4.11. Requisitos de Projeto e de Implementação:**

4.11.1. Não é necessário projeto de implementação para essa contratação.

**4.12. Requisitos de Implantação:**

4.12.1. Para os ITENS 01 e 02:

a) Disponibilidade de espaço físico nos racks onde os firewalls serão alocados;

b) Alimentação elétrica para os equipamentos;

c) Ficarão por conta da CONTRATADA as possíveis despesas de transporte e hospedagem necessárias à execução dos objetos.

4.12.2. Para o ITEM 03:

a) Não se aplica.

**4.13. Requisitos de Garantia:**

4.13.1. Para todos os itens (1, 2 e 3):

a) Os serviços de garantia deverão ser prestados pela CONTRATADA;

b) O tempo de garantia esperado está descrito no ANEXO III - ESPECIFICAÇÕES TÉCNICAS.

**4.14. Requisitos de Experiência Profissional e Formação da Equipe:**

4.14.1. Para os ITENS 01 e 02:

a) Devido a especificidade da solução de proteção de dados e o nível de criticidade relacionado à segurança da informação na UFCA, é exigido que o profissional da CONTRATADA que realizará a implantação possua certificação específica emitida pelo FABRICANTE da solução;

b) A comprovação da certificação será exigida no início da execução da implantação da solução;

c) A CONTRATADA deverá comprovar que já realizou implantação semelhante anteriormente, através de Atestado de Capacidade Técnica, emida por empresa cliente da CONTRATADA;

**4.15. Requisitos de Metodologia de Trabalho:**

4.15.1. Para os ITENS 01 e 02:

a) A CONTRATADA deve prestar o suporte técnico (hardware e software) desta contratação durante todo o período de vigência da garantia;

b) A CONTRATADA deve fornecer número telefônico para contato e registro de ocorrências do funcionamento do serviço contratado, com funcionamento 24 horas por dia e 7 dias por semana;

c) A CONTRATADA deve prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATANTE em até 72 horas corridas, por intermédio do preposto designado para acompanhamento do contrato, a contar de sua solicitação;

4.15.2. Para o ITEM 03:

a) A CONTRATADA deve prestar o suporte técnico desta contratação durante todo o período de vigência da garantia;

b) A CONTRATADA deve fornecer número telefônico para contato e registro de ocorrências do funcionamento do serviço contratado.

**4.16. Requisitos de Segurança da Informação:**

4.16.1. Para os ITENS 01 e 02:

4.17.1.a.1.1. Realizem o tratamento de dados pessoais (Lei 13709/2018) e informações classificadas, conforme legislação vigente;

4.17.1.a.1.2. Prevejam a realização de auditoria de SIC (Segurança da Informação e Comunicação) de conformidade dos requisitos de segurança da informação previstos pela contratação;

4.17.1.a.1.3. Assegurem a gestão e tratamento de incidentes de forma sistematizadas:

4.17.1.a.1.3.1. A empresa fornecedora da Solução é integralmente responsável pela manutenção de sigilo sobre quaisquer dados e informações fornecidos pela CONTRATANTE ou contidos em quaisquer documentos e em quaisquer mídias de que venham a ter conhecimento durante a etapa de repasse, de execução dos trabalhos e de encerramento dos serviços, não podendo, se não formalmente autorizado pela CONTRATANTE, sob qualquer pretexto e forma, divulgá-los, reproduzi-los ou utilizá-los a qualquer tempo;

4.17.1.a.1.3.2. A empresa deverá possuir nas suas instalações, onde atividades serão executadas de modo remoto, padrões de segurança da informação e de tecnologia da informação para evitar a perda ou o vazamento, ataques externos e tentativas de invasão, como firewall e sistemas antivírus;

4.17.1.a.1.3.3. Cada profissional a serviço da empresa CONTRATADA, envolvido na execução do objeto, deverá assinar o Termo de Sigilo e Confidencialidade (Anexo I), bem como declaração de estar ciente de que a estrutura computacional da CONTRATANTE não poderá ser utilizada para fins diversos daqueles do objeto relacionado à prestação do serviço;

4.17.1.a.1.3.4. O correio eletrônico e a navegação em sítios da internet a partir do ambiente de rede da CONTRATANTE poderão, a exclusivo critério da CONTRATANTE, ser objeto de controle e auditoria;

b) A CONTRATADA deverá configurar de maneira apropriada os elementos de rede para habilitar o log dos eventos da rede da CONTRATANTE, tais como conexões externas e registros de utilização de serviços (arquivos transferidos via FTP, acessos a páginas web e tentativas de login não autorizado);

c) Os logs devem estar com o horário sincronizado via NTP e possuir o quanto possível de detalhes, sem, no entanto, gerar dados em excesso. A Contratada deverá configurar os elementos da rede para enviar os logs para um Servidor de Logs dedicado, disponibilizado pela UFCA;

d) A CONTRATADA deverá aplicar e manter atualizados os patches de segurança nos equipamentos que compõem a Solução;

e) Os ativos de rede deverão suportar autenticação 802.1x, listas de controle de acesso (ACLs) e proteção por usuário e senha de todas as ferramentas de gerenciamento, tais como: web, SSH e console.

4.16.2. Para todos os itens (1, 2 e 3):

a) A CONTRATADA deve assegurar a continuidade do negócio implementado pela solução, evitando vazamentos de dados da CONTRATANTE;

b) A CONTRATADA deverá fornecer e manter atualizados os patches de segurança que compõem a Solução;

c) Apresentar um cronograma para implantação e configuração da Solução adquirida, o qual deverá sofrer aval do Gestor do Contrato;

## 5. RESPONSABILIDADES

5.1. Esta seção se aplica a todos os itens (1,2 e 3) do Termo de Referência

**5.2. Deveres e responsabilidades da CONTRATANTE:**

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

5.2.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.2.3. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

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

5.2.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.2.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.2.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável;

5.2.8. Prever que 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, pertençam à Administração.

**5.3. Deveres e responsabilidades da CONTRATADA:**

5.3.1. Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato;

5.3.2. Após a assinatura do contrato, a CONTRATADA deverá apresentar a relação do pessoal técnico, adequado e disponível para a execução do objeto, bem como a formação de cada um dos membros da equipe;

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

5.3.4. 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;

5.3.5. 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, sempre que considerar a medida necessária;

5.3.6. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

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

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

5.3.9. 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, os modelos de dados e as bases de dados à Administração.

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

5.4.1. O órgão gerenciador será a UFCA;

5.4.2. São deveres e responsabilidades do órgão gerenciador da ata de registro de preços:

5.4.2.1. Compilar as demandas envolvidas, os quantitativos mínimos por requisição e os máximos, os locais de entrega e prazos, entre outras informações fornecidas pelos órgãos participantes, para sistematizar e harmonizar as disposições do Edital e Termo de Referência, e dispor os itens do objeto licitatório da forma mais adequada para a obtenção da melhor proposta para a Administração Pública;

5.4.2.2. Confirmar junto aos órgãos participantes a sua concordância com o objeto a ser licitado, inclusive quanto aos quantitativos e termo de referência;

5.4.2.3. Realizar o pregão, efetuar o registro do licitante vencedor, efetivar a homologação da licitação e firmar a correspondente Ata de Registro de Preços;

5.4.2.4. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

5.4.2.5. Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

5.4.2.5.1. as formas de comunicação entre os envolvidos, a exemplo de ofício,

telefone, e-mail, ou sistema informatizado, quando disponível; e

5.4.2.5.2. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;

5.4.2.6. Avaliar e decidir, garantida a realização da Homologação do Bem, acerca da eventual substituição da solução registrada em função de fatores supervenientes e imperativos;

5.4.2.7. Cumprir outras obrigações que se apliquem ao objeto da contratação.

## 6. MODELO DE EXECUÇÃO DO CONTRATO

### 6.1. Rotinas de Execução:

6.1.1. Para TODOS OS ITENS:

a) Esclarecimentos sobre a forma de comunicação a ser adotada entre o Órgão e a CONTRATADA;

b) Esclarecimentos acerca dos níveis de serviço previstos no contrato, bem como sobre o período de adaptação e ajustes da CONTRATADA ao contrato;

c) Esclarecimentos relacionados ao funcionamento do Órgão, tais como: horário de trabalho, forma de trabalho com a equipe da CONTRATADA, regimento interno do Órgão, forma de acesso dos colaboradores da CONTRATADA às dependências da CONTRATANTE e demais informações pertinentes;

d) Pagamentos só serão realizados à medida em que serviços ou bens solicitados pela UFCA sejam corretamente prestados, conforme os procedimentos de recebimento e ateste da fiscalização;

e) A execução dos serviços demandados para a licitante vencedora deverá obedecer aos prazos estabelecidos pela CONTRATANTE;

6.1.2. Apenas para os ITENS 01 e 02:

a) Imediatamente após a assinatura do contrato, o Gestor do Contrato na UFCA convocará os responsáveis das CONTRATADAS para a reunião de abertura do contrato, a qual poderá ser realizada presencialmente ou por meio de videoconferência, na qual serão tratados os seguintes assuntos:

b) Formalização da ordem de serviço ou de fornecimento de bens para a execução, após a análise e aprovação do plano de trabalho pela equipe técnica da CONTRATANTE;

c) A CONTRATADA deverá realizar o repasse de conhecimento (hands on) de toda a solução a fim de atender às necessidades da CONTRATANTE;

d) Todos os materiais que fazem parte do objeto da licitação deverão ser fornecidos pela licitante vencedora;

e) Somente a instalação de bens e/ou a prestação de serviços efetivamente demandados serão pagos, os quais serão verificados e atestados pela equipe de fiscalização que validará os quantitativos e autorizará a emissão do documento fiscal equivalente;

f) A entrega dos equipamentos deverá ser realizada na Av. Tenente Raimundo Rocha, N° 1639, Bairro: Cidade Universitária, CEP: 63.048-080,

Cidade: Juazeiro do Norte-CE. Nos horários entre 08:00 às 11:30 e 13:30 às 16:30;

g) Ficarão por conta da CONTRATADA as possíveis despesas de transporte e hospedagem necessárias à execução dos objetos;

**6.2. Mecanismos formais de comunicação:**

6.2.1. Para TODOS OS ITENS:

a) A UFCA comunicar-se-á com a empresa por intermédio do seu preposto a ser indicado em 5 (cinco) dias após a assinatura do contrato;

b) Serão utilizados os seguintes mecanismos formais de comunicação: Ordem de Serviço ou de Fornecimento de Bens, Ofícios, Atas de reunião devidamente reduzidos a termo e assinados eletronicamente;

c) Para comunicação eletrônica disponibiliza-se o endereço citi.dti@ufca.edu.br e dti@ufca.edu.br.

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

6.3.1. Para TODOS OS ITENS:

a) 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;

b) O Termo de Sigilo e Confidencialidade, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade e o Termo de Ciência encontram-se, respectivamente, nos ANEXOS I e II e devem ser assinados por cada profissional a serviço da CONTRATADA envolvidos na execução desse objeto.

## 7. MODELO DE GESTÃO DO CONTRATO

**7.1. Critérios de Aceitação e Qualidade:**

7.1.1. Para TODOS OS ITENS:

a) Os equipamentos, softwares e serviços serão recebidos **Provisoriamente**: no prazo de 5 (cinco) dias úteis, por servidor designado da Diretoria de Tecnologia da Informação, para efeito de verificação da conformidade com as especificações e condições da contratação;

b) Os equipamentos, softwares e serviços serão recebidos **Definitivamente**: após a verificação da conformidade do objeto entregue com as especificações e condições da contratação e consequente aceitação, no prazo de 10 (dez) dias úteis, contados da data do recebimento provisório, com a certificação da nota fiscal por servidor designado da Diretoria de Tecnologia da Informação, pelo gestor do contrato ou pela comissão de recebimento designada;

c) O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente nas especificações técnicas deste Termo de Referência;

d) A CONTRATADA deverá informar a UFCA a disponibilidade dos produtos, por meio do endereço eletrônico informado no item 6.2.1.c, para que sejam tomadas todas as providências necessárias ao início da execução dos testes de aceitação;

e) Os bens/serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da CONTRATADA, sem prejuízo da aplicação de penalidades;

f) O aceite dos bens/serviços deverá ser efetuado por servidores designados para o acompanhamento e fiscalização do contrato;

g) Antes de proceder o aceite definitivo dos bens/serviço, além de observar o atendimento a todas as cláusulas deste Termo de Referência, deve-se proceder com a aprovação dos procedimentos de teste e inspeção definidos no item 7.2 e atendimento aos níveis mínimos de serviços exigidos no item 7.3.

7.1.2. Apenas para os ITENS 01 e 02:

a) Somente serão aceitos equipamentos novos e sem uso, não serão aceitos equipamentos remanufaturados, NFR (Not For Resale) ou de demonstração;

b) Os equipamentos deverão ser entregues nas caixas lacradas pela CONTRATADA, não sendo aceitos equipamentos com caixas violadas;

c) Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital;

**7.2. Procedimentos de Teste e Inspeção:**

7.2.1. Para TODOS OS ITENS:

a) Será realizado acesso ao site do fabricante para, por meio do número de série dos equipamentos e/ou software, a verificação do tipo e validade do serviço de garantia e suporte;

b) Será realizado abertura de chamado teste por intermédio dos canais de atendimento;

7.2.2. Apenas para o ITEM 03:

a) Em referência ao software de gerenciamento de redes, serão realizados testes de inclusão e exclusão de novos ativos de redes após a implantação das novas licenças contratadas.

**7.3. Níveis Mínimos de Serviço Exigidos:**

7.3.1. Apenas para os ITENS 01 e 02:

a) Deverá ser disponibilizado suporte técnico para todos os equipamentos ofertados, assegurando prazos de atendimentos compatíveis com a instalação, ou seja, 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana (à exceção dos chamados de Severidade 4);

b) O atendimento aos chamados deverá obedecer à seguinte classificação quanto ao nível de severidade:

| Severidade | Descrição | Tipo de Atendimento | Tempo de Atendimento | Tempo de solução ou de contorno |
|---|---|---|---|---|
| 1. Crítica | Chamados referentes a emergências ou problema crítico, caracterizados pela existência de ambiente paralisado. | On-site. | No máximo 4 (quatro) horas após a abertura do chamado. | No máximo, três dias úteis após o início do atendimento do chamado |
| 2. Alta | Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho. | On-site. | No máximo 4 (quatro) horas após a abertura do chamado. | No máximo, quatro dias úteis após o início do atendimento do chamado |
| 3. Média | Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente, incluindo os casos em que haja necessidade de substituição de componentes) que possuam redundância | Remoto, com exceção das situações em que seja necessária intervenção física | No máximo 8 (oito) horas após a abertura do chamado | No máximo, cinco dias úteis após o início do atendimento do chamado |
| 4. Baixa | Chamados com o objetivo de sanar dúvidas quanto ao uso ou à implementação do produto | Remoto | No máximo 48 (quarenta e oito) horas após a abertura do chamado. | No máximo, sete dias úteis após a abertura do chamado. |

Tabela 1 – Níveis de Severidade

c) Os chamados de Severidade 1 serão atendidos inicialmente de forma remota com atendimento iniciado em no máximo 4 (quatro) horas após a abertura do chamado e contarão com esforço concentrado da CONTRATADA com vistas a aplicar solução ou medida de contorno até o terceiro dia útil após o início do atendimento do chamado; O atendimento de Severidade 1 não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias não úteis;

d) Os chamados de Severidade 2 serão atendidos inicialmente de forma remota com atendimento iniciado em no máximo 4 (quatro) horas após a abertura do chamado e contarão com esforço concentrado da CONTRATADA com vistas a aplicar solução ou medida de contorno em até quatro dias úteis após o início do atendimento do chamado. O atendimento de Severidade 2 não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias não úteis;

e) Os chamados de Severidade 3 serão atendidos em no máximo 8 (oito) horas após a sua abertura e contarão com esforço concentrado da CONTRATADA com vistas a aplicar solução ou medida de contorno em até cinco dias úteis após o início do atendimento do chamado. Caso o problema não possa ser resolvido remotamente, a CONTRATADA deverá colocar à disposição da CONTRATANTE, um especialista devidamente habilitado e credenciado que trabalhará o tempo que for necessário para a solução do problema, sendo que

o ônus financeiro de tal providência será da CONTRATADA;

f) Tratamento dos chamados de Severidade 4: os chamados de Severidade 4 serão atendidos em no máximo 48 (quarenta e oito) horas após a sua abertura e deverão ser concluídos em até sete dias úteis após a abertura do chamado. Os chamados classificados com Severidade 4 serão atendidos das 08h00 às 18h00, de segunda-feira a sexta-feira, horário de Brasília, exceto feriados;

g) Caso necessário, para as severidades 1, 2 e 3, um técnico da CONTRATADA deverá comparecer ao local onde o equipamento está instalado a fim de aplicar a solução de contorno, como por exemplo: troca de peças, diagnóstico do equipamento, instalação de novos módulos, etc.

**h) Escalação de Severidade:**

7.3.1.h.1. Por necessidade de serviço ou criticidade do problema, o UFCA poderá solicitar a escalação de chamado para níveis superiores de severidade. Os prazos dos chamados escalados passam a contar novamente do início;

7.3.1.h.2. Os prazos para atendimento e para solução ou medida de contorno terão suas contagens de prazo reiniciadas na nova severidade a partir da escalação;

7.3.1.h.3. No caso de não cumprimento dos prazos na nova severidade as penalidades decorrentes serão aplicadas conforme Severidade da escalação, considerando o prazo total desde a abertura do chamado original.

**7.4. Manutenções:**

7.4.1. Apenas para os ITENS 01 e 02:

a) A CONTRATADA deverá prover, sempre que necessário, todas as correções e/ou atualizações dos hardwares instalados, tais como: nível de firmware e microcódigos, que permitam melhorar as funcionalidades dos equipamentos, bem como mantê-los compatíveis com os demais componentes de hardware e software dos Centros de Dados do UFCA, sem ônus adicional para o UFCA;

b) A CONTRATADA deverá dar conhecimento a CONTRATANTE, através de e-mail, da existência de alterações nas configurações dos equipamentos (firmwares e microcódigos). A CONTRATANTE avaliará o impacto dessas alterações e agendará a realização da manutenção do equipamento, tanto do hardware quanto do firmware instalados, sendo de responsabilidade da CONTRATADA prover todas as correções e/ou atualizações necessárias;

c) No caso de manutenções em que haja risco de indisponibilidade total ou parcial dos equipamentos, a CONTRATANTE deverá ser previamente notificada para que se proceda à aprovação e o agendamento da manutenção em horário conveniente a CONTRATANTE;

d) Caso a CONTRATANTE identifique a necessidade de manutenção em algum equipamento, a CONTRATADA será informada para que proceda o seu agendamento;

e) Correrá por conta exclusiva da CONTRATADA, a responsabilidade pelo deslocamento do seu técnico ao local da instalação do equipamento, bem como pela retirada e entrega do equipamento e peças de reposição, além de todas as despesas de transporte, frete e seguro correspondente;

f) Para os equipamentos ofertados, a CONTRATADA deverá prestar, durante o período de garantia, suporte técnico, tanto do hardware quanto do firmware e softwares instalados, observando os níveis de serviço especificados neste Contrato;

g) Em qualquer hipótese (e ainda que não seja o fabricante dos equipamentos) a CONTRATADA deverá possuir acesso para suporte técnico de 2º e 3º níveis, bem como aos firmwares e microcódigos dos equipamentos, de forma a prestar os serviços de manutenção e assistência técnica, sem ônus adicional para a UFCA;

h) Para todos os efeitos da contratação em espécie, vigoram os seguintes conceitos:

7.4.1.h.1. Suporte Técnico Primeiro Nível: equipe treinada para atender diretamente os usuários em demandas referentes a diagnóstico e tratamento de problemas, configuração e administração do ambiente e esclarecimento de dúvidas em geral;

7.4.1.h.2. Suporte Técnico Segundo Nível: equipe multidisciplinar treinada, devidamente capacitada e com grande experiência em ambientes críticos e complexos, que exigem alta disponibilidade;

7.4.1.h.3. Suporte Técnico Terceiro Nível: escalonamento ao fabricante, devido à necessidade de retaguarda nas tecnologias de hardware suportadas;

7.4.1.h.4. Todas as peças de reposição deverão ser novas, sem uso.

**7.5. METODOLOGIA E ADEQUAÇÃO DA SOLUÇÃO DE TIC ÀS ESPECIFICAÇÕES FUNCIONAIS E TECNOLÓGICAS:**

7.5.1. Apenas para os ITENS 01 e 02:

a) A CONTRATANTE, por intermédio da empresa CONTRATADA para prestação dos serviços de análise e operação de suporte de infraestrutura e de atendimento aos usuários de soluções e recursos de Tecnologia da Informação e Comunicação, produzirá um script de acionamento da CONTRATADA, bem como a forma de registro desses chamados a serem definidos pela fiscalização contratual;

b) Por isso, a CONTRATADA deverá disponibilizar os canais de atendimento para o hardware e software, abaixo:

c) Canais de atendimento através de telefone gratuito 0800, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

d) Chamado técnico através de site na Internet, 24 (vinte e quatro) horas por dia, 7(sete) dias por semana e/ou canal telefônico gratuito 0800;

e) Registrado o chamado, caso este viole os níveis de serviço, a equipe de fiscalização, conforme descrito no script, será acionada para contactar o preposto do contrato para resolução do problema e verificar o cumprimento dos níveis de serviço aqui descritos.

f) Eventualmente, a equipe de fiscalização poderá solicitar da CONTRATADA a entrega de relatório constando os acionamentos técnicos abertos, em andamento e encerrados no período com no mínimo as seguintes informações: número de acionamento, descrição da ocorrência, severidade, nome do responsável da UFCA pela abertura do chamado, data e hora de abertura do chamado, data e hora do início do atendimento, data e hora do início de atendimento local, se for o caso, data e hora de encerramento ou contorno e descrição da resolução adotada;

g) A CONTRATANTE irá disponibilizar os recursos humanos necessários às atividades de gestão e fiscalização do contrato, inclusive quanto à qualificação técnica e disponibilidade de tempo para aplicação das listas de verificação e roteiros de testes:

| Função | Qtd | Atribuições |
|---|---|---|
| Gestor de Contrato | 01 | Servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente. |
| Fiscal Requisitante | 01 | Servidor representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista técnico-funcional da Solução de Tecnologia da Informação. |
| Fiscal Técnico | 01 | Servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato. |
| Fiscal Administrativo | 01 | Servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos. |

Tabela 2 – Funções da equipe de fiscalização do contrato

**7.6. FIXAÇÃO DOS VALORES PARA SANÇÕES CABÍVEIS:**

7.6.1. Para os ITENS 01 e 02:

a) Penalidades pelo descumprimento dos níveis de serviço:

7.6.1.a.1. O não atendimento dentro do prazo estabelecido para o chamado ou a interrupção do atendimento de um chamado por parte da CONTRATADA, que não tenha sido previamente autorizada pela CONTRATANTE ensejará aplicação de multa à CONTRATADA, conforme o nível de severidade do mesmo:

7.6.1.a.2. Severidade 1 – 0,5% (cinco décimos por cento) do valor constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso

7.6.1.a.3. Severidade 2 – 0,4% (quatro décimos por cento) do valor constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso;

7.6.1.a.4. Severidade 3 – 0,2% (dois décimos por cento) do valor constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso;

7.6.1.a.5. Severidade 4 – 0,1% (um décimo por cento) do valor constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.

7.6.2. Para o ITEM 3:

a) Não se aplica.

**7.7. Procedimentos e Sanções Administrativas:**

7.7.1. Para TODOS OS ITENS:

a) Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a CONTRATADA que:

7.7.1.a.1. Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

7.7.1.a.2. Ensejar o retardamento da execução do objeto;

7.7.1.a.3. Falhar ou fraudar na execução do contrato;

7.7.1.a.4. Comportar-se de modo inidôneo; e

7.7.1.a.5. Cometer fraude fiscal.

b) Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

7.7.1.b.1. **Advertência por escrito**, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para a Administração;

7.7.1.b.2. **Multa de**:

7.7.1.b.2.1. 0,1% (um décimo por cento) por dia sobre o valor adjudicado em caso de atraso na execução do objeto, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

7.7.1.b.2.2. 5% (cinco por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem anterior ou de inexecução parcial da obrigação assumida;

7.7.1.b.2.3. 10% (dez por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

7.7.1.b.2.4. 0,02% a 0,32% por dia sobre o valor total do contrato, conforme detalhamento constante das tabelas abaixo;

7.7.1.b.2.5. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

7.7.1.b.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;

7.7.1.b.4. Sanção de impedimento de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

7.7.1.b.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;

7.7.1.b.6. Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas 3 e 4.

| Grau | Correspondência |
|---|---|
| 1 | 0,02% ao dia sobre o valor total do contrato |
| 2 | 0,04% ao dia sobre o valor total do contrato |
| 3 | 0,08% ao dia sobre o valor total do contrato |

| | |
|---|---|
| 4 | 0,16% ao dia sobre o valor total do contrato |
| 5 | 0,32% ao dia sobre o valor total do contrato |

Tabela 3 - Grau de Infrações

| Item | Correspondência | Grau |
|---|---|---|
| 1 | Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais, por ocorrência | 5 |
| 2 | Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento | 4 |
| 3 | Manter funcionário sem qualificação para executar os serviços contratados, por empregado e por dia. | 3 |
| 4 | Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia. | 2 |
| 5 | Deixar de cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência. | 2 |
| 6 | Deixar de substituir empregado alocado que não atenda às necessidades do serviço, por funcionário e por dia. | 2 |
| 7 | Deixar de indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato. | 1 |

Tabela 4 – Infrações

7.7.2. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

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

b) tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

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

7.7.3. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999;

7.7.4. As multas devidas e/ou prejuízos causados à CONTRATANTE serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente;

7.7.5. Caso a CONTRATANTE determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente;

7.7.6. 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.

7.7.7. 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.

7.7.8. 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.

7.7.9. 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.

7.7.9. 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.

7.7.10. As penalidades serão obrigatoriamente registradas no SICAF.

**7.8. DO PAGAMENTO (Para TODOS OS ITENS):**

7.8.1. O pagamento será efetuado pela CONTRATANTE no prazo de 30 dias, contados do recebimento da Nota Fiscal/Fatura, por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

7.8.1.1. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

7.8.1.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que a CONTRATANTE atestar a execução do objeto do contrato.

7.8.2. A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do serviço, conforme previsto neste Termo de Referência

7.8.3. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

7.8.3.1. Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

7.8.4. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

7.8.5. O setor competente para proceder o pagamento deve verificar se a Nota Fiscal/Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

7.8.5.1. o prazo de validade;

7.8.5.2. a data da emissão;

7.8.5.3. os dados do contrato e da CONTRATANTE;

7.8.5.4. o período de prestação dos serviços;

7.8.5.5. o valor a pagar; e

7.8.5.6. eventual destaque do valor de retenções tributárias cabíveis.

7.8.6. Nos termos do item 1, do Anexo VIII-A da Instrução Normativa SEGES/MP nº 05, de 2017, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:

7.8.6.1. não produziu os resultados acordados;

7.8.6.2. deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida descrita no item 7 - MODELO DE GESTÃO DO CONTRATO;

7.8.6.3. deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior descritas no item 7 - MO- DELO DE GESTÃO DO CONTRATO;

7.8.7. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.8.8. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

7.8.9. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.

7.8.10. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar 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.

7.8.11. Não havendo regularização ou sendo a defesa considerada improcedente, a CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.8.12. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.

7.8.13. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

7.8.13.1. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da CONTRATANTE.

7.8.14. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1991, nos termos do item 6 do Anexo XI da IN SEGES/MP n. 5/2017, quando couber.

7.8.15. É vedado o pagamento, a qualquer título, por serviços prestados ou fornecimento de bens, à empresa privada que tenha em seu quadro societário servidor público da ativa da CONTRATANTE, com fundamento na Lei de Diretrizes Orçamentárias vigente.

7.8.16. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela CONTRATANTE, entre a data do vencimento e o efetivo adimplemento da parcela é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira diário= 0,00016438, assim apurado:

| | | |
|---|---|---|
| I = (TX) | I = (6/100)/365 | I = 0,00016438<br>TX = Percentual da taxa anual = 6% |

## 8. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1. Para os itens 01 e 02: foram encontradas 02 propostas no painel de preços, a 3ª proposta foi cotada com fornecedor, pois não foi encontrada contratação em nenhum órgão federal, no último ano, com as configurações idênticas ou próximas das especificações técnicas dos objetos a serem contratados neste processo.

8.2. Para o ITEM 03: não foram encontradas contratações do software Intelligent Management Center (IMC) na versão Enterprise Edition no Painel de Preços, com isso a coleta foi realizada com fornecedores;

| ITEM | DESCRIÇÃO | QTD | UNIDADE | VALOR UNITÁRIO | VALOR TOTAL |
|---|---|---|---|---|---|
| 1 | SOLUÇÃO DE PROTEÇÃO DE DADOS FIREWALL TIPO 01 \| LICENÇA CONTRA AMEAÇAS CONHECIDAS \| LICENÇA PARA BLOQUEIO DE URL E CATEGORIAS DE SITES MALICIOSOS \| 60 MESES DE SUPORTE E GARANTIA \| SERVIÇO DE INSTALAÇÃO PROFISSIONAL | 2 | UN | R$ 233.374,95 | R$ 466.749,90 |
| 2 | SOLUÇÃO DE PROTEÇÃO DE DADOS FIREWALL TIPO 02 \| LICENÇA CONTRA AMEAÇAS CONHECIDAS \| LICENÇA PARA BLOQUEIO DE URL E CATEGORIAS DE | 4 | UN | R$ 184.167,67 | R$ 736.670,68 |

| | | | | | |
|---|---|---|---|---|---|
| | SITES MALICIOSOS \| 60 MESES DE SUPORTE E GARANTIA \| SERVIÇO DE INSTALAÇÃO PROFISSIONAL | | | | |
| 3 | LICENÇA PARA EXPANSÃO DE SISTEMA DE GERENCIAMENTO DE REDE. MARCA: HPE, MODELO: INTELLIGENT MANAGEMENT CENTER (IMC) ENTERPRISE EDITION (JG748AAE). A LICENÇA DEVE SER PERPÉTUA E CADA PACOTE DEVERÁ ADICIONAR O SUPORTE A GERÊNCIA DE 50 DISPOSITIVOS, SOMANDO-SE ÀS LICENÇAS JÁ EXISTENTES. | 4 | UN | R$ 40.324,13 | R$ 161.296,52 |
| | | | | **VALOR TOTAL:** | **R$ 1.364.717,10** |

8.3. O valor total estimado da contratação é **R$ 1.364.717,10** (um milhão, trezentos e sessenta e quatro mil, setecentos e dezessete reais e dez centavos).

8.4. Estão incluídas nos preços unitários todas as despesas do fornecedor até a entrega definitiva do objeto no local e prazos avençados, tais como: frete, encargos trabalhistas e previdenciários e todos os tributos incidentes;

8.5. Todos os valores constantes da proposta da licitante vencedora deverão contemplar todas as despesas com peças, materiais, ferramentas e mão-de-obra, inclusive salários, fretes, seguros, taxas, tributos, contribuições e qualquer outra incidência fiscal, parafiscal e trabalhista decorrente da execução do objeto do Contrato;

8.6. Ficarão por conta da Contratada as possíveis despesas de transporte e hospedagem de seus funcionários, necessárias à consecução do objeto.

## 9. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

9.1. Conforme o parágrafo 2º do Artigo 7º do Decreto 7892/2013: § 2º Na licitação para registro de preços não é necessário indicar a dotação orçamentária, que somente será exigida para a formalização do contrato ou outro instrumento hábil.

## 10. DA VIGÊNCIA DO CONTRATO

10.1. Para todos os itens:

10.1.1. O(s) CONTRATO(S) decorrente(s) da ATA REGISTRO DE PREÇOS (ARP) terão vigência de 12 (DOZE) MESES e deverão ser assinados no prazo de validade da ARP.

10.1.2. O encerramento da vigência contratual não interrompe a obrigação de prestação da GARANTIA TÉCNICA, devendo a CONTRATADA honrá-la durante todo o período estipulado.

## 11. DO REAJUSTE DE PREÇOS

11.1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas;

11.1.1. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade;

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

11.3. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer;

11.4. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo;

11.5. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor;

11.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

11.7. O reajuste será realizado por apostilamento.

## 12. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

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

12.1.1. Regime: Menor preço por item;

12.1.2. Modalidade: Pregão Eletrônico, separado por itens;

12.1.3. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a Administração CONTRATANTE, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta;

12.1.4. As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no edital;

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

## 13. DA GARANTIA DE EXECUÇÃO

13.1. Não haverá exigência de garantia contratual da execução, pelas razões abaixo justificadas:

13.1.1. Conforme se depreende do disposto no art. 56 da Lei n° 8.666/1993, a exigência de garantia de execução contratual é discricionária, pelo que cabe ao administrador avaliar se representará um benefício para a Administração;

13.2. Desta forma, a garantia será dispensada, a fim de atender ao princípio da economicidade, tendo em vista que a sua exigência resultaria em onerosidade à contratação, e em virtude da natureza simples do serviço.

## 14. DA SUBCONTRATAÇÃO

14.1. Não será admitida a subcontratação do objeto licitatório.

## 15. DA ALTERAÇÃO SUBJETIVA

15.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na contratação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

## 16. GARANTIA E SUPORTE TÉCNICO

16.1. O suporte e garantia dos bens adquiridos (hardware/software) nesse processo de contratação deverá, obrigatoriamente, vigorar por 60 (sessenta) meses, contados a partir da data da sua assinatura.

## 17. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

17.1. A Equipe de Planejamento da Contratação foi instituída pelo Documento de Oficialização da Demanda, de 17 de abril de 2020.

17.2. Conforme o §6º do art. 12 da IN SGD/ME nº 01, 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<br>Marcos Iury Fernandes Maia da Silva<br>Técnico de Tecnologia da Informação<br>Matrícula SIAPE: 1040185 | Integrante Técnico<br>Francisco Henrique Balbino de Godoy<br>Técnico de Tecnologia da Informação<br>Matrícula SIAPE: 1184038 | Integrante Administrativo Cícero Wagner Farias Souza Assistente em Administração Matrícula SIAPE: 1853772 |

Juazeiro do Norte-CE, 18 de setembro de 2020

| Diretor - Diretoria de Tecnologia da Informação |
|---|
| Herbert Novais Onofre<br>Diretor de TI<br>Universidade Federal do Cariri<br>Matrícula SIAPE: 1571618 |

Juazeiro do Norte-CE, 18 de setembro de 2020

Aprovo,

| Pró-Reitor – Pró-Reitoria de Administração |
|---|
| Silvério de Paiva Freitas Júnior Pró-Reitor de Administração<br>Universidade Federal do Cariri<br>Matrícula SIAPE: 1772643 |

Juazeiro do Norte-CE, 18 de setembro de 2020

**ANEXO I - TERMO DE SIGILO E CONFIDENCIALIDADE**

**Razão Social:**

**CNPJ:**

**Endereço da Sede:**

**Por este termo nomeado Contratada**

Pelo presente TERMO DE SIGILO E CONFIDENCIALIDADE, a Contratada assume o compromisso de manter confidencialidade e sigilo sobre todas as informações confidenciais a que tenha acesso durante todo o período em que tenha atuado ou venha a atuar como prestadora de serviço para a Universidade Federal de CARIRI (UFCA), em razão do contrato Nº XX/20XX.

**Cláusula primeira – Do Termo e das Obrigações**

A Contratada assume as seguintes obrigações:

1. Não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro;

2. Tomar todas as medidas necessárias à proteção das informações confidenciais recebidas, inclusive com relação a todos os seus empregados diretamente envolvidos na contratação, bem como para evitar e prevenir revelação a terceiros, exceto se comprovadamente solicitadas em razão de ordem judicial que imponha tal revelação.

3. Não divulgar, publicar ou noticiar qualquer informação que tenha tido acesso em decorrência da execução do contrato nº XX/20XX, responsabilizando-se por todas as pessoas que vierem a ter acesso a tais informações, por seu intermédio;

4. Destruir quaisquer documentos por ela produzidos que contenham informações confidenciais da Contratante, quando não mais for necessária a manutenção dessas informações confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades legais e contratuais;

5. Ressarcir a ocorrência de qualquer dano e/ou prejuízo oriundo de uma eventual quebra de sigilo das informações confidenciais.

**Subcláusula Primeira** - a Contratada fica, desde já, proibida de produzir cópias, transferir arquivos digitalizados ou registrar por escrito as informações confidenciais a que tenha acesso, exceto aquelas estritamente necessárias para a prestação do serviço, sendo responsável pela sua guarda e sigilo.

Neste Termo, a expressão “Informação Confidencial” fica assim definida:

**Informação confidencial:** toda informação escrita, verbal ou apresentada de modo

tangível ou intangível, e revelada ou obtida devido às atividades desempenhadas por sua função como prestador de serviço;

A confidencialidade é obrigatória, mesmo após o término das atividades da Contratada como prestadora de serviço e, somente deixa de ser obrigatória, se comprovado que as informações confidenciais foram solicitadas em razão de ordem judicial que imponha tal revelação.

**Cláusula segunda - Da Validade**

Este termo tornar-se-á válido a partir da data de sua efetiva assinatura pela Contratada.

**Cláusula terceira – Das Penalidades**

Caso a Contratada, comprovadamente, descumpra quaisquer das obrigações previstas no presente termo, a UFCA desencadeará processo administrativo, assegurado o contraditório e a ampla defesa, além de ação indenizatória junto à autoridade competente, que aplicará as devidas sanções de cunho civil, criminal ou outra penalidade na forma da Lei.

**Cláusula quarta – Do Foro**

Por força do artigo 109, inciso I, da Constituição Federal, o foro competente para dirimir quaisquer controvérsias resultantes da execução deste Instrumento é o da Justiça Federal, Subseção Judiciária de Juazeiro do Norte, caso não sejam resolvidos administrativamente.

**Cláusula quinta**

A Contratada compromete-se a obter o fiel cumprimento das cláusulas deste termo pelos seus empregados.

Por estar de acordo com o exposto, a Contratada firma o presente termo.

Juazeiro do Norte,_____de_____de 2020.

_____

Representante Legal da Contratada

**ANEXO II - TERMO DE CIÊNCIA**

| | | | |
|---|---|---|---|
| **Contrato N°:** | | | |
| **Objeto:** | | | |
| **Contratante:** | | | |
| **Contratada:** | | **CNPJ:** | |
| **Preposto da Contratada:** | | **CPF:** | |

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do **Termo de Compromisso de Sigilo e Confidencialidade** referente ao contrato nº XX/20XX e se comprometem a manter o absoluto sigilo com relação a toda e qualquer informação confidencial a que tiverem acesso em decorrência das atividades desenvolvidas em cumprimento da referida Ata.

Neste Termo, a expressão "Informação Confidencial" fica assim definida:

**Informação confidencial**: toda informação escrita, verbal ou apresentada de modo tangível ou intangível, e revelada ou obtida devido às atividades desempenhadas por sua função como prestador de serviço.

A Contratada se compromete a:

a) tomar todas as medidas necessárias à proteção das informações confidenciais recebidas, inclusive com relação a todos os seus empregados diretamente envolvidos na contratação, bem como para evitar e prevenir revelação a terceiros, exceto se comprovadamente solicitadas em razão de ordem judicial que imponha talrevelação.

b) não divulgar, publicar ou noticiar qualquer informação que tenha tido acesso em decorrência da execução do contrato nº XX/20XX, responsabilizando-se por todas as pessoas que vierem a ter acesso a tais informações, por seu intermédio;

c) não produzir cópias, transferir arquivos digitalizados ou registrar por escrito as informações confidenciais a que tenha acesso, exceto aquelas estritamente necessárias para a prestação do serviço, sendo responsável pela sua guarda esigilo;

d) destruir quaisquer documentos por ela produzidos que contenham informações confidenciais da **Contratante**, quando não mais for necessária a manutenção dessas informações confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades legais e contratuais.

Caso a **Contratada**, comprovadamente, descumpra quaisquer das obrigações previstas no presente termo, a UFCA desencadeará processo administrativo, assegurado o contraditório e a ampla defesa, além de ação indenizatória junto à autoridade competente, que aplicará as devidas sanções de cunho civil, criminal ou outra penalidade na forma da Lei.

Juazeiro do Norte,_____de_____de 20XX.

**Ciência**

_____

Representante Legal da Contratada

| **Funcionários:** | |
|---|---|
| _____<br><Nome><br>CPF: <CPF> | _____<br><Nome><br>CPF: <CPF> |
| _____<br><Nome><br>CPF: <CPF> | _____<br><Nome><br>CPF: <CPF> |
| _____<br><Nome><br>CPF: <CPF> | _____<br><Nome><br>CPF: <CPF> |

## ANEXO III - ESPECIFICAÇÕES TÉCNICAS

## ITEM 1 - SOLUÇÃO DE PROTEÇÃO DE DADOS TIPO 01:

**1. DESCRIÇÃO:**

1.1. Aquisição de solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", Filtro de URL, bem como controle de transmissão de dados e acesso a internet compondo uma plataforma (hardware e software integrados do tipo appliance) de segurança integrada e robusta;

**2. CAPACIDADE E QUANTIDADES:**

2.1. A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento:

2.1.1. Throughput de, no mínimo, 1.6 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

2.1.2. Throughput de, no mínimo, 750 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

2.1.3. Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos às sanções previstas em lei;

2.1.4. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante;

2.1.5. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4;

2.1.6. Suporte a, no mínimo, 190.000 conexões simultâneas;

2.1.7. Suporte a, no mínimo, 9.500 novas conexões por segundo;

2.1.8. Fonte 120/240 AC ou DC, redundante;

2.1.9. Disco Solid State Drive (SSD), no mínimo, 240 GB;

2.1.10. No mínimo, 04 (quatro) interfaces de rede 10/100/1000 base-TX;

2.1.11. No mínimo, 04 (quatro) interfaces de rede 1 Gbps SFP;

2.1.12. No mínimo, 02 (duas) interfaces de rede 10 Gbps SFP+;

2.1.13. 01 (uma) interface de rede 1 Gbps dedicada para gerenciamento;

2.1.14. 01 (uma) interface do tipo console ou similar;

2.1.15. Suporte a, no mínimo, 30 (trinta) zonas de segurança;

2.1.16. Estar licenciada para ou suportar sem o uso de licença, no mínimo, 500 (quinhentos) clientes de VPN SSL simultâneos;

2.1.17. Estar licenciada para ou suportar sem o uso de licença no mínimo, 200 (duzentos) túneis de VPN IPSEC simultâneos;

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

2.3. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.

**3. CARACTERÍSTICAS GERAIS:**

3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração;

3.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

3.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

3.4. O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos

equipamentos servidores e sistema operacional de uso genérico;

3.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

3.6. O software deverá ser fornecido em sua versão mais atualizada;

3.7. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

3.7.1. Suporte a 4094 VLAN Tags 802.1q;

3.7.2. Agregação de links 802.3ad e LACP;

3.7.3. Policy based routing ou policy based forwarding;

3.7.4. Roteamento multicast (PIM-SM);

3.7.5. DHCP Relay;

3.7.6. DHCP Server;

3.7.7. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;

3.8. O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;

3.9. Deve suportar os seguintes tipos de NAT:

3.9.1. Nat dinâmico: Many-to-1 e Many-to-Many;

3.9.2. Nat estático: 1-to-1 e Many-to-Many;

3.9.3. Nat estático bidirecional 1-to-1;

3.9.4. Tradução de porta (PAT);

3.9.5. NAT de origem e destino;

3.9.6. Suportar NAT de Origem e NAT de Destino simultaneamente;

3.10. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;

3.11. Deve implementar balanceamento de link através do método round-robin;

3.12. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links;

3.13. Deve suportar o balanceamento de, no mínimo, quarto links;

3.14. Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;

3.15. Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;

3.16. Enviar log para sistemas de monitoração externos, simultaneamente;

3.17. Deve haver a opção de enviar logs para os sistemas de monitoração externos;

3.18. Proteção contra anti-spoofing;

3.19. Deve permitir bloquear sessões que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;

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

3.21. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;

3.22. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

3.23. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

3.24. Suportar a OSPF graceful restart;

3.25. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;

3.26. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação;

3.27. O dispositivo de proteção deve ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3):

3.27.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

3.27.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e

controle do tráfego em nível de aplicação;

3.27.3. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

3.27.4. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

3.28. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

3.28.1. Em modo transparente;

3.28.2. Em layer 3;

3.29. A configuração em alta disponibilidade deve sincronizar:

3.29.1. Sessões;

3.29.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

3.29.3. Certificados de-criptografados;

3.29.4. Associações de Segurança das VPNs;

3.29.5. Tabelas FIB;

3.29.6. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

3.30. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

## 4. CONTROLE POR POLÍTICA DE FIREWALL:

4.1. Deverá suportar controles por zona de segurança;

4.2. Controles de políticas por porta e protocolo;

4.3. Controle de políticas por aplicações: grupos estáticos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

4.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

4.5. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs;

4.6. Controle de políticas por código de País (exemplo: BR, USA, UK, RUS);

4.7. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);

4.8. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

4.9. Deve de-criptografar sites e aplicações que utilizam certificados ECC e/ou Elliptical Curve Digital Signature Algorithm (ECDSA);

4.10. Controle de inspeção e de-criptografia de SSH por política;

4.11. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

4.12. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;

4.13. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

4.14. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;

4.15. Suporte a objetos e regras IPV6;

4.16. Suporte a objetos e regras multicast;

4.17. Deve suportar, no mínimo, dois tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;

4.18. Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

## 5. CONTROLE DE APLICAÇÕES:

5.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

5.1.1. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

5.1.2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos,

compartilhamento de arquivos, e-mail;

5.1.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, LDAP, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;

5.1.4. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;

5.1.5. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

5.1.6. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443;

5.1.7. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

5.1.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

5.1.9. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para algunsusuários;

5.1.10. Deve permitir habilitar aplicações SAAS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal, tais como: aplicativos google, gmail, etc;

5.1.11. Identificar o uso de táticas evasivas via comunicações criptografadas;

5.1.12. Atualizar a base de assinaturas de aplicações automaticamente;

5.1.13. Reconhecer aplicações em IPv6;

5.1.14. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

5.1.15. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

5.1.16. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

5.1.17. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

5.1.18. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

5.1.19. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

5.1.20. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

5.1.21. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;

5.1.22. Deve possibilitar a diferenciação de tráfegos de Instant Messaging, possuindo granularidade de controle/políticas para os mesmos;

5.1.23. Deve possibilitar a diferenciação e controle de partes das aplicações;

5.1.24. Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;

5.1.25. Deve ser possível a criação de grupos de aplicações baseados em características:

5.1.25.1. Tecnologia utilizada na aplicação (Client-Server, Browser Based, Network Protocol, etc);

5.1.25.2. Nível de risco da aplicação;

5.1.25.3. Aplicações que usem técnicas evasivas, utilizadas por malwares, como

transferência de arquivos e/ou uso excessivo de banda, etc.

**6. IDENTIFICAÇÃO DE USUÁRIOS:**

6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

6.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

6.3. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

6.4. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários;

6.5. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

6.6. Suporte a autenticação Kerberos;

6.7. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;

6.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

6.9. Deve identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

6.10. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for;

6.11. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

6.12. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

**7. QOS:**

7.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

7.2. Suportar a criação de políticas de QoS por:

7.2.1. Endereço de origem e endereço de destino;

7.2.2. Por usuário e grupo do LDAP/AD;

7.2.3. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

7.2.4. Por porta;

7.3. O QoS deve possibilitar a definição de classes por:

7.3.1. Banda Garantida;

7.3.2. Banda Máxima;

7.3.3. Fila de Prioridade.

7.4. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

7.5. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

7.6. Deve implementar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);

7.7. Disponibilizar estatísticas RealTime para classes de QoS;

7.8. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

**8. FILTRO DE DADOS:**

8.1. Permite a criação de filtros para arquivos e dados pré-definidos;

8.2. Os arquivos devem ser identificados por extensão e assinaturas;
8.3. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);
8.4. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
8.5. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
8.6. Permitir listar o número de aplicações suportadas para controle de dados;
8.7. Permitir listar o número de tipos de arquivos suportados para controle de dados.

**9. GEOLOCALIZAÇÃO:**

9.1. Suportar a criação de políticas por Geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
9.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
9.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

**10. VPN:**

10.1. Suportar VPN Site-to-Site e Client-To-Site;
10.2. Suportar IPSec VPN;
10.3. Suportar SSL VPN;
10.4. A VPN IPSEc deve suportar:
10.4.1. DES e 3DES;
10.4.2. Autenticação MD5 e SHA-1;
10.4.3. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
10.4.4. Algoritmo Internet Key Exchange (IKEv1 e v2);
10.4.5. AES 128, 192 e 256 (Advanced Encryption Standard);
10.4.6. Autenticação via certificado IKE PKI;

10.5. Deve possuir interoperabilidade com os seguintes fabricantes:
10.5.1. Cisco;
10.5.2. Checkpoint;
10.5.3. Juniper;
10.5.4. Palo Alto Networks;
10.5.5. Fortinet;
10.5.6. Sonic Wall;

10.6. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo dethroubleshooting;

10.7. A VPN SSL deve suportar:
10.7.1. O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
10.7.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
10.7.3. Atribuição de endereço IP nos clientes remotos de VPN SSL;
10.7.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
10.7.5. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
10.7.6. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
10.7.7. Atribuição de DNS nos clientes remotos de VPN;
10.7.8. Deve suportar a criação de políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
10.7.9. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;
10.7.10. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
10.7.11. Deve permitir a distribuição de certificado para o usuário de remoto através do

portal de VPN de forma automatizada;

10.7.12. Suporta leitura e verificação de CRL (certificate revocation list);

10.7.13. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

10.7.14. O agente de VPN a ser instalado nos equipamentos desktop e laptops, deve ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory;

10.7.15. O agente poderá comunicar-se com o portal para determinar as políticas de segurança do usuário;

10.7.16. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

10.7.16.1. Antes do usuário autenticar na estação;

10.7.16.2. Sob demanda do usuário;

10.7.17. Deve manter uma conexão segura com o portal durante a sessão;

10.7.18. O agente, se necessário, do serviço de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista, 7, 8 e Mac OSx;

## 11. CONSOLE DE GERÊNCIA E MONITORAÇÃO:

11.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

11.2. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;

11.3. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;

11.4. O gerenciamento deve permitir/possuir:

11.4.1. Criação e administração de políticas de firewall e controle de aplicação;

11.4.2. Monitoração de logs;

11.4.3. Ferramentas de investigação de logs;

11.4.4. Debugging;

11.4.5. Captura de pacotes.

11.4.6. Acesso concorrente de administradores;

11.5. Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI;

11.6. Deve possuir mecanismos de busca na solução, onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;

11.7. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

11.8. Deve permitir usar palavras chaves para facilitar identificação de regras;

11.9. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

11.10. Autenticação integrada ao Microsoft Active Directory e servidor Radius;

11.11. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

11.12. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

11.13. Criação de regras que fiquem ativas em horário definido;

11.14. Criação de regras com data de expiração;

11.15. Backup das configurações e rollback de configuração para a última configuração salva;

11.16. Suportar Rollback de Sistema Operacional para a última versão local;

11.17. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

11.18. Deve possibilitar a integração com outras soluções de SIEM de mercado (*third-party SIEM vendors*);

11.19. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

11.20. Deve permitir a criação de *dashboards* customizados para visibilidades do tráfego de aplicativos, usuários e tráfego bloqueado;

11.21. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

11.22. Dever permitir a visualização dos logs de tráfego (IP de origem, destino, usuário e porta), aplicação e filtro de arquivos em uma única tela;
11.23. Deve possuir relatórios de utilização dos recursos por aplicações;
11.24. Prover uma visualização sumarizada de todas as aplicações e ameaças que passaram pela solução;
11.25. Deve possuir mecanismo "*Drill-Down*" para navegação nos relatórios em RealTime;
11.26. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
11.27. Deve ser possível exportar os logs em CSV;
11.28. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada;
11.29. Deverá ser possível rotação do log;
11.30. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;
11.31. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;
11.32. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
    11.32.1. Situação do dispositivo e do:
        11.32.1.1. Principais aplicações;
        11.32.1.2. Administradores autenticados na gerência da plataforma de segurança;
        11.32.1.3. Número de sessões simultâneas;
        11.32.1.4. Status das interfaces;
        11.32.1.5. Uso de CPU;

11.33. Geração de relatórios: no mínimo, os seguintes relatórios devem ser gerados:
    11.33.1. Resumo de aplicações utilizadas;
    11.33.2. Principais aplicações por utilização de largura de banda de entrada e saída;
    11.33.3. Principais aplicações por taxa de transferência de bytes;
    11.33.4. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas de rede vinculadas a este tráfego;
    11.33.5. Deve permitir a criação de relatórios personalizados;

11.34. Gerar alertas automáticos via:
    11.34.1. Email;
    11.34.2. SNMP;
    11.34.3. Syslog;

11.35. A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP;
11.36. Conforme 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), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote).

## 12. LICENÇA CONTRA AMEAÇAS CONHECIDAS PARA SOLUÇÃO DE PROTEÇÃO DE DADOS:

Este item deve prover licenciamento para proteção contra ameaças conhecidas compatível com SOLUÇÃO DE PROTEÇÃO DE DADOS TIPO 01 desta especificação técnica, conforme requisitos abaixo:

12.1. Esta licença deve ser fornecida com validade mínima de 60 (sessenta) meses;
12.2. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante;
12.3. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
12.4. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber

atualizações ou que não haja contrato de garantia de software com o fabricante;

12.5. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

12.6. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e Antispyware: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

12.7. Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2;

12.8. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

12.9. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

12.10. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

12.11. Deve permitir o bloqueio de vulnerabilidades;

12.12. Deve permitir o bloqueio de exploits conhecidos;

12.13. Deve incluir proteção contra ataques de negação de serviços;

12.14. Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelados pelo protocolo GRE;

12.15. Deverá possuir os seguintes mecanismos de inspeção de IPS:

12.15.1. Análise de padrões de estado de conexões;

12.15.2. Análise de decodificação de protocolo;

12.15.3. Análise para detecção de anomalias de protocolo;

12.15.4. Análise heurística;

12.15.5. IP Defragmentation;

12.15.6. Remontagem de pacotes de TCP;

12.15.7. Bloqueio de pacotes malformados.

12.16. Ser imune e capaz de impedir ataques básicos como: *Synflood*, *ICMPflood*, *UDPfloof*, etc;

12.17. Detectar e bloquear a origem de *portscans* com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

12.18. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

12.19. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

12.20. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

12.21. Possuir assinaturas para bloqueio de ataques de buffer overflow;

12.22. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

12.23. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti- spyware, permitindo a criação de exceções com granularidade nas configurações;

12.24. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

12.24.1. É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;

12.25. Suportar bloqueio de arquivos por tipo;

12.26. Identificar e bloquear comunicação com botnets;

12.27. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

12.28. Deve suportar referência cruzada com CVE;

12.29. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

12.29.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

12.30. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e *Antispyware*;

12.31. Deve permitir que na captura de pacotes por assinaturas de IPS e *Antispyware* seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;

12.32. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

12.33. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

12.34. Os eventos devem identificar o país de onde partiu a ameaça;
12.35. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
12.36. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos;
12.37. Rastreamento de vírus em pdf;
12.38. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);
12.39. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
12.40. Conforme 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), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote);

**13. LICENÇA PARA BLOQUEIO DE URL E CATEGORIAS DE SITES MALICIOSOS PARA SOLUÇÃO DE PROTEÇÃO DE DADOS:**

Este item deve prover licenciamento para filtro e bloqueio de sites/categorias de conteúdos e URLs maliciosas compatível com a SOLUÇÃO DE PROTEÇÃO DE DADOS TIPO 01 desta especificação técnica, conforme requisitos abaixo:

13.1. Esta licença deve ser fornecida com validade mínima de 60 (sessenta) meses;
13.2. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
13.3. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;
13.4. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, *E-directory* e base de dados local;
13.5. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
13.6. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
13.7. Deve bloquear o acesso a sites de busca (Exemplo: Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir pagina de bloqueio fornecendo instruções ao usuário de como habilitar a função;
13.8. Suporte base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
13.9. Possuir, pelo menos, 60 categorias de URLs;
13.10. Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;
13.11. Deve possuir categoria específica para classificar domínios recém registrados (com menos de 30 dias);
13.12. A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;
13.13. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;
13.14. Suportar a criação categorias de URLs customizadas;
13.15. Suportar a exclusão de URLs do bloqueio, por categoria;
13.16. Permite a customização de página de bloqueio;
13.17. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;
13.18. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;
13.19. Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);
13.20. Suporta a inclusão nos logs do produto de informações das atividades dos usuários;
13.21. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;
13.22. Conforme 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), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote).

**14. LICENÇA DE SUPORTE E GARANTIA PARA SOLUÇÃO DE PROTEÇÃO DE DADOS:**

Este item deve prover licença de SLA para suporte técnico e garantia compatível com a SOLUÇÃO DE PROTEÇÃO DE DADOS TIPO 01 desta especificação técnica, conforme requisitos abaixo:

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

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

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

14.4. 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);

14.5. 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, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana);

14.6. O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo:

14.6.1. Crítico: significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 2 (duas) hora para resolução total ou encontro de solução temporária de contorno. Neste caso o chamado deverá ser aberto via telefone (0800);

14.6.2. Alta: impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária decontorno;

14.6.3. Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

14.6.4. Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta.

14.7. Conforme 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), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote);

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

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

**15. SERVIÇO DE INSTALAÇÃO PROFISSIONAL:**

15.1. A CONTRATADA deverá fornecer pacote de 40 (quarenta) horas de prestação de serviços de instalação e configuração da solução podendo ser utilizadas para os seguintes procedimentos e especificações:

15.1.1. Reunião de alinhamento para criação do escopo do projeto previamente a instalação;

15.1.2. 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);

15.1.3. Analise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados;

15.1.4. Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

15.1.5. Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;

15.1.6. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

15.1.7. Configuração do sistema de firewall, VPN, IPS, Filtro URL, Antivírus e Anti-malware de acordo com as exigências levantadas;

15.1.8. Toda 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 firewalls a fim de garantir a melhor eficiência da solução durante o período de vigência das licenças;

15.1.9. Repasse de informação das configurações realizadas no formato hands-on de 8 (oito) horas após validação da migração;

15.1.10. Deve haver geração de relatório com as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;

15.2. Os serviços de instalação e configuração deverá ser realizado por técnico certificado oficialmente pelo fabricante da solução ofertada ou pelo próprio fabricante;

15.3. Este pacote deverá ser utilizado exclusivamente para as soluções ofertadas neste termo de especificação técnica.

## ITEM 2 - SOLUÇÃO DE PROTEÇÃO DE DADOS TIPO 02:

**1. DESCRIÇÃO:**

1.1. Aquisição de solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", Filtro de URL, bem como controle de transmissão de dados e acesso a internet compondo uma plataforma (hardware e software integrados do tipo appliance) de segurança integrada e robusta;

**2. CAPACIDADE E QUANTIDADES:**

2.1. A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento:

2.1.1. Throughput de, no mínimo, 1,6 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

2.1.2. Throughput de, no mínimo, 750 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor seráaceito;

2.1.3. Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos às sanções previstas em lei;

2.1.4. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante;

2.1.5. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4;

2.1.6. Suporte a, no mínimo, 190.000 conexões simultâneas;

2.1.7. Suporte a, no mínimo, 9.500 novas conexões por segundo;
2.1.8. Fonte 120/240 AC ou DC, redundante ou fonte externa redundante;
2.1.9. Disco Solid State Drive (SSD), no mínimo, 240 GB;
2.1.10. No mínimo, 04 (quatro) interfaces de rede 10/100/1000 base-TX;
2.1.11. No mínimo,04 (quatro) interfaces de rede 1 Gbps SFP;
2.1.12. 01 (uma) interface de rede 1 Gbps dedicada para gerenciamento;
2.1.13. 01 (uma) interface do tipo console ou similar;
2.1.14. Suporte a, no mínimo, 20 (vinte) zonas de segurança;
2.1.15. Estar licenciada para ou suportar sem o uso de licença, 500 (quinhentos) clientes de VPN SSL simultâneos;
2.1.16. Estar licenciada para ou suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC simultâneos;

2.2. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;
2.3. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.

**3. CARACTERÍSTICAS GERAIS:**

3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
3.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
3.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
3.4. O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
3.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
3.6. O software deverá ser fornecido em sua versão mais atualizada;
3.7. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
3.7.1. Suporte a 4094 VLAN Tags 802.1q;
3.7.2. Agregação de links 802.3ad e LACP;
3.7.3. Policy based routing ou policy based forwarding;
3.7.4. Roteamento multicast (PIM-SM);
3.7.5. DHCP Relay;
3.7.6. DHCP Server;
3.7.7. Jumbo Frames;
3.7.8. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
3.8. O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;
3.9. Deve suportar os seguintes tipos de NAT:
3.9.1. Nat dinâmico: Many-to-1 e Many-to-Many;
3.9.2. Nat estático: 1-to-1 e Many-to-Many;
3.9.3. Nat estático bidirecional 1-to-1;
3.9.4. Tradução de porta (PAT);
3.9.5. NAT de origem e destino;
3.9.6. Suportar NAT de Origem e NAT de Destino simultaneamente;

3.10. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;
3.11. Deve implementar balanceamento de link através do método round-robin;
3.12. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links;
3.13. Deve suportar o balanceamento de, no mínimo, quarto links;
3.14. Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;
3.15. Deve implementar balanceamento de link através de políticas por aplicação e porta de

destino;

3.16. Enviar log para sistemas de monitoração externos, simultaneamente;
3.17. Deve haver a opção de enviar logs para os sistemas de monitoração externos;
3.18. Proteção contra anti-spoofing;
3.19. Deve permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;
3.20. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;
3.21. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
3.22. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
3.23. Suportar a OSPF graceful restart;
3.24. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
3.25. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação;
3.26. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);
    3.26.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados darede;
    3.26.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
    3.26.3. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
    3.26.4. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
3.27. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
    3.27.1. Em modo transparente;
    3.27.2. Em layer 3;
3.28. A configuração em alta disponibilidade deve sincronizar:
    3.28.1. Sessões;
    3.28.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
    3.28.3. Certificados de-criptografados;
    3.28.4. Associações de Segurança das VPNs;
    3.28.5. Tabelas FIB;
    3.28.6. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha delink;
3.29. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com ofabricante.

**4. CONTROLE POR POLÍTICA DE FIREWALL:**

4.1. Deverá suportar controles por zona de segurança;
4.2. Controles de políticas por porta e protocolo;
4.3. Controle de políticas por aplicações: grupos estáticos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
4.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
4.5. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs
4.6. Controle de políticas por código de País (exemplo: BR, USA, UK, RUS);
4.7. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);
4.8. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
4.9. Deve de-criptografar sites e aplicações que utilizam certificados ECC e/ou Elliptical Curve Digital Signature Algorithm (ECDSA);
4.10. Controle de inspeção e de-criptografia de SSH por política;
4.11. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o

protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

4.12. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;

4.13. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

4.14. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;

4.15. Suporte a objetos e regras IPV6;

4.16. Suporte a objetos e regras multicast;

4.17. Deve suportar, no mínimo, três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;

4.18. Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

**5. CONTROLE DE APLICAÇÕES:**

5.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

5.1.1. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

5.1.2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

5.1.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, LDAP, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;

5.1.4. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;

5.1.5. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

5.1.6. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443;

5.1.7. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

5.1.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

5.1.9. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para algunsusuários;

5.1.10. Deve permitir habilitar aplicações SAAS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal, tais como: aplicativos google, gmail, etc;

5.1.11. Identificar o uso de táticas evasivas via comunicações criptografadas;

5.1.12. Atualizar a base de assinaturas de aplicações automaticamente;

5.1.13. Reconhecer aplicações em IPv6;

5.1.14. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

5.1.15. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o

usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

5.1.16. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

5.1.17. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

5.1.18. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

5.1.19. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

5.1.20. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

5.1.21. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;

5.1.22. Deve possibilitar a diferenciação de tráfegos de Instant Messaging, possuindo granularidade de controle/políticas para os mesmos;

5.1.23. Deve possibilitar a diferenciação e controle de partes das aplicações;

5.1.24. Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;

5.1.25. Deve ser possível a criação de grupos de aplicações baseados em características:

5.1.25.1. Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc);

5.1.25.2. Nível de risco da aplicação;

5.1.25.3. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

**6. IDENTIFICAÇÃO DE USUÁRIOS:**

6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

6.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

6.3. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

6.4. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários:

6.5. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

6.6. Suporte a autenticação Kerberos;

6.7. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;

6.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestesserviços;

6.9. Deve identificar usuários através de leitura do campo *x-fowarded-for*, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

6.10. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo *x-fowarded-for*;

6.11. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

6.12. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

**7. QOS:**

7.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a

solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

7.2. Suportar a criação de políticas de QoS por:
- 7.2.1. Endereço de origem;
- 7.2.2. Endereço de destino;
- 7.2.3. Por usuário e grupo do LDAP/AD;
- 7.2.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
- 7.2.5. Por porta;

7.3. O QoS deve possibilitar a definição de classes por:
- 7.3.1. Banda Garantida;
- 7.3.2. Banda Máxima;
- 7.3.3. Fila de Prioridade.

7.4. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

7.5. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

7.6. Deve implementar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);

7.7. Disponibilizar estatísticas RealTime para classes de QoS;

7.8. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

**8. FILTRO DE DADOS:**

8.1. Permite a criação de filtros para arquivos e dados pré-definidos;

8.2. Os arquivos devem ser identificados por extensão e assinaturas;

8.3. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);

8.4. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

8.5. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

8.6. Permitir listar o número de aplicações suportadas para controle de dados;

8.7. Permitir listar o número de tipos de arquivos suportados para controle de dados;

**9. GEOLOCALIZAÇÃO:**

9.1. Suportar a criação de políticas por Geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

9.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

9.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

**10. VPN:**

10.1. Suportar VPN Site-to-Site e Client-To-Site;

10.2. Suportar IPSec VPN;

10.3. Suportar SSL VPN;

10.4. A VPN IPSEc deve suportar:
- 10.4.1. DES e 3DES;
- 10.4.2. Autenticação MD5 e SHA-1;
- 10.4.3. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
- 10.4.4. Algoritmo Internet Key Exchange (IKEv1 e v2);
- 10.4.5. AES 128, 192 e 256 (Advanced Encryption Standard);
- 10.4.6. Autenticação via certificado IKE PKI;

10.5. Deve possuir interoperabilidade com os seguintes fabricantes:
- 10.5.1. Cisco;
- 10.5.2. Checkpoint;
- 10.5.3. Juniper;
- 10.5.4. Palo Alto Networks;
- 10.5.5. Fortinet;
- 10.5.6. Sonic Wall;

10.6. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir

da interface gráfica da solução, facilitando o processo dethroubleshooting;

10.7. A VPN SSL deve suportar:

10.7.1. O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

10.7.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

10.7.3. Atribuição de endereço IP nos clientes remotos de VPN SSL;

10.7.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;

10.7.5. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;

10.7.6. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

10.7.7. Atribuição de DNS nos clientes remotos de VPN;

10.7.8. Deve suportar a criação de políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

10.7.9. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;

10.7.10. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

10.7.11. Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;

10.7.12. Suporta leitura e verificação de CRL (certificate revocation list);

10.7.13. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

10.7.14. O agente de VPN a ser instalado nos equipamentos desktop e laptops, deve ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory;

10.7.15. O agente poderá comunicar-se com o portal para determinar as políticas de segurança do usuário;

10.7.16. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

10.7.16.1. Antes do usuário autenticar na estação;

10.7.16.2. Sob demanda do usuário;

10.7.17. Deve manter uma conexão segura com o portal durante a sessão;

10.7.18. O agente, se necessário, do serviço de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista, 7, 8 e Mac OSx;

**11. CONSOLE DE GERÊNCIA E MONITORAÇÃO:**

11.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

11.2. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;

11.3. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;

11.4. O gerenciamento deve permitir/possuir:

11.4.1. Criação e administração de políticas de firewall e controle de aplicação;

11.4.2. Monitoração de logs;

11.4.3. Ferramentas de investigação de logs;

11.4.4. Debugging;

11.4.5. Captura de pacotes;

11.4.6. Acesso concorrente de administradores;

11.5. Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI;

11.6. Deve possuir mecanismos busca na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;
11.7. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
11.8. Deve permitir usar palavras chaves para facilitar identificação de regras;
11.9. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
11.10. Autenticação integrada ao Microsoft Active Directory e servidor Radius;
11.11. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
11.12. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;
11.13. Criação de regras que fiquem ativas em horário definido;
11.14. Criação de regras com data de expiração;
11.15. Backup das configurações e rollback de configuração para a última configuração salva;
11.16. Suportar Rollback de Sistema Operacional para a última versão local;
11.17. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
11.18. Deve possibilitar a integração com outras soluções de SIEM de mercado (*third-party SIEM vendors*);
11.19. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
11.20. Deve permitir a criação de *Dashboards* customizados para visibilidades do tráfego de aplicativos, usuários e tráfego bloqueado;
11.21. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
11.22. Deve permitir a visualização dos logs de tráfego (IP de origem, destino, usuário e porta), aplicação e filtro de arquivos em uma única tela;
11.23. Deve possuir relatórios de utilização dos recursos por aplicações;
11.24. Prover uma visualização sumarizada de todas as aplicações e ameaças que passaram pela solução;
11.25. Deve possuir mecanismo "*Drill-Down*" para navegação nos relatórios em RealTime;
11.26. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
11.27. Deve ser possível exportar os logs em CSV;
11.28. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada;
11.29. Deverá ser possível rotação do log;
11.30. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;
11.31. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;
11.32. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
    11.32.1. Situação do dispositivo e do:
        11.32.1.1. Principais aplicações;
        11.32.1.2. Administradores autenticados na gerência da plataforma de segurança;
        11.32.1.3. Número de sessões simultâneas;
        11.32.1.4. Status das interfaces;
        11.32.1.5. Uso de CPU;
11.33. Geração de relatórios: no mínimo os seguintes relatórios devem ser gerados:
    11.33.1. Resumo de aplicações utilizadas;
    11.33.2. Principais aplicações por utilização de largura de banda de entrada e saída;
    11.33.3. Principais aplicações por taxa de transferência de bytes;
    11.33.4. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas de rede vinculadas a este tráfego;
    11.33.5. Deve permitir a criação de relatórios personalizados;
11.34. Gerar alertas automáticos via:
    11.34.1. Email;
    11.34.2. SNMP;
    11.34.3. Syslog;

11.35. A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP;

11.36. Conforme 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), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote);

**12. LICENÇA CONTRA AMEAÇAS CONHECIDAS PARA SOLUÇÃO DE PROTEÇÃO DE DADOS** Este item deve prover licenciamento para proteção contra ameaças conhecidas compatível com SOLUÇÃO DE PROTEÇÃO DE DADOS TIPO 02 desta especificação técnica, conforme requisitos abaixo:

12.1. Esta licença deve ser fornecida com validade mínima de 60 (sessenta) meses;

12.2. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante;

12.3. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

12.4. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

12.5. Deve sincronizar as assinaturas de IPS, Antivírus, *Antispyware* quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

12.6. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e *Antispyware*: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

12.7. Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2;

12.8. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

12.9. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

12.10. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

12.11. Deve permitir o bloqueio de vulnerabilidades;

12.12. Deve permitir o bloqueio de exploits conhecidos;

12.13. Deve incluir proteção contra ataques de negação de serviços;

12.14. Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelados pelo protocolo GRE;

12.15. Deverá possuir os seguintes mecanismos de inspeção de IPS:

12.15.1. Análise de padrões de estado de conexões;

12.15.2. Análise de decodificação de protocolo;

12.15.3. Análise para detecção de anomalias de protocolo;

12.15.4. Análise heurística;

12.15.5. IP Defragmentation;

12.15.6. Remontagem de pacotes de TCP;

12.15.7. Bloqueio de pacotes malformados.

12.16. Ser imune e capaz de impedir ataques básicos como: *Synflood*, *ICMPflood*, *UDPfloof*, etc;

12.17. Detectar e bloquear a origem de *portscans* com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

12.18. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

12.19. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para

detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

12.20. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

12.21. Possuir assinaturas para bloqueio de ataques de buffer overflow;

12.22. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

12.23. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

12.24. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

12.24.1. É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;

12.25. Suportar bloqueio de arquivos por tipo;

12.26. Identificar e bloquear comunicação com botnets;

12.27. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

12.28. Deve suportar referência cruzada com CVE;

12.29. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

12.29.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

12.30. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e *Antispyware*;

12.31. Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;

12.32. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

12.33. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

12.34. Os eventos devem identificar o país de onde partiu a ameaça;

12.35. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

12.36. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos;

12.37. Rastreamento de vírus em pdf;

12.38. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);

12.39. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

12.40. 40. Conforme 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), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo(lote).

## 13. LICENÇA PARA BLOQUEIO DE URL E CATEGORIAS DE SITES MALICIOSOS PARA SOLUÇÃO DE PROTEÇÃO DE DADOS

Este item deve prover licenciamento para filtro e bloqueio de sites/categorias de conteúdos e URLs maliciosas compatível com a SOLUÇÃO DE PROTEÇÃO DE DADOS TIPO 02 desta especificação técnica, conforme requisitos abaixo:

13.1. Esta licença deve ser fornecida com validade mínima de 60 (sessenta) meses;

13.2. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

13.3. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;

13.4. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, *E-directory* e base de dados local;

13.5. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
13.6. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
13.7. Deve bloquear o acesso a sites de busca (Exemplo: Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir pagina de bloqueio fornecendo instruções ao usuário de como habilitar a função;
13.8. Suporte base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
13.9. Possui pelo menos 60 categorias de URLs;
13.10. Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;
13.11. Deve possuir categoria específica para classificar domínios recém registrados (com menos de 30 dias);
13.12. A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;
13.13. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;
13.14. Suportar a criação categorias de URLs customizadas;
13.15. Suportar a exclusão de URLs do bloqueio, por categoria;
13.16. Permitir a customização de página de bloqueio;
13.17. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;
13.18. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;
13.19. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);
13.20. Suportar a inclusão nos logs do produto de informações das atividades dos usuários;
13.21. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: *UserAgent*, *Referer*, e *X-Forwarded For*;
13.22. Conforme 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), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote).

## 14. LICENÇA DE SUPORTE E GARANTIA PARA SOLUÇÃO DE PROTEÇÃO DE DADOS

Este item deve prover licença de SLA para suporte técnico e garantia compatível com a SOLUÇÃO DE PROTEÇÃO DE DADOS TIPO 02 desta especificação técnica, conforme requisitos abaixo:

14.1. Deve possuir garantia do fabricante ou autorizada no Brasil com validade mínima de 60 (sessenta) meses;
14.2. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção debugs;
14.3. Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução;
14.4. 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);
14.5. 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, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana);
14.6. O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo:
14.6.1. Crítico: significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 2 (duas) hora para resolução total ou encontro de solução temporária de contorno. Neste caso o chamado deverá ser aberto via telefone (0800);
14.6.2. Alta: impacto moderado no sistema, travamento, ou parada de ambiente parcial.

Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

14.6.3. Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

14.6.4. Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta.

14.7. Conforme 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), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote);

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

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

**15. SERVIÇO DE INSTALAÇÃO PROFISSIONAL**

15.1. A CONTRATADA deverá fornecer pacote de 40 (quarenta) horas de prestação de serviços de instalação e configuração da solução podendo ser utilizadas para os seguintes procedimentos e especificações:

15.1.1. Reunião de alinhamento para criação do escopo do projeto previamente a instalação;

15.1.2. 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);

15.1.3. Analise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados;

15.1.4. Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

15.1.5. Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;

15.1.6. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

15.1.7. Configuração do sistema de firewall, VPN, IPS, Filtro URL, Antivírus e Anti-malware de acordo com as exigências levantadas;

15.1.8. Toda 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 firewalls a fim de garantir a melhor eficiência da solução durante o período de vigência das licenças;

15.1.9. Repasse de informação das configurações realizadas no formato hands-on de 8 (oito) horas após validação da migração;

15.1.10. Deve haver geração de relatório com as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;

15.2. Os serviços de instalação e configuração deverá ser realizado por técnico certificado oficialmente pelo fabricante da solução ofertada ou pelo próprio fabricante;

15.3. Este pacote deverá ser utilizado exclusivamente para as soluções ofertadas neste termo de especificação técnica.

**ITEM 3 - LICENÇA PARA SISTEMA DE GERENCIAMENTO DE REDES - HPE/IMC:**

3.1. Pacote de licença adicional para software de gerenciamento existente na Universidade Federal do Cariri - UFCA;

3.2. Cada pacote deverá adicionar o suporte a gerência de 50 dispositivos, somando-se às licenças já existentes;

3.3. Marca: HP, modelo: Intelligent Management Center (IMC) Enterprise Edition(JG748AAE);

3.4. Deve possuir suporte do fabricante pelo período de 60 meses, incluindo: atualização de versão, correção de

bugs e suporte remoto ao produto;

3.5. Estar totalmente integrado em todas as suas funcionalidades com o sistema de gerenciamento em produção na ANS de modelo “HPE IMC Enterprise Edition (JG748AAE)”, para aproveitamento do sistema legado;

3.6. Não serão aceitos licenças que recusem qualquer acesso e/ou não suporte a um recurso disponibilizado pelo “Sistema de Gerenciamento de Rede” em produção na ANS;

3.7. Deverá prover a expansão do licenciamento do software de gerenciamento modelo "HPE IMC Enterprise Edition (JG748AAE)";

3.8. Deverá possibilitar Análise de Tráfego de Rede através de módulo NTA – Network TrafficAnalyzer;

3.9. Inclui módulos NTA e WSM e eAPIlicense - Suporte a dispositivos expansíveis -Modular

# ANEXO IV – MODELO DE ORDEM DE SERVIÇO OU DE FORNECIMENTO DE BENS

| IDENTIFICAÇÃO | | | | | |
|---|---|---|---|---|---|
| OS/OFB | | Requisitante | | Data de Emissão | |
| Nome do Projeto | | | | Emergencial | Sim ( ) Não ( ) |
| Contratada | | | | Contrato | |

| 1 – ESPECIFICAÇÃO DOS PRODUTOS / SERVIÇOS E VOLUMES | | | | |
|---|---|---|---|---|
| ID | PRODUTOS / SERVIÇOS | MÉTRICA | QUANT. | PREÇO (R$) |
| | | | | |
| | | | | |
| TOTAL | | | | R$ |

| 2 – INSTRUÇÕES COMPLEMENTARES |
|---|
| |

| 3 – CRONOGRAMA | | | |
|---|---|---|---|
| ID | TAREFA | INÍCIO | FIM |
| 01 | | | |
| 02 | | | |
| 03 | | | |

| 4 – DOCUMENTOS ENTREGUES |
|---|
| |

| 5 – DATAS E PRAZOS |
|---|

| Data Prevista para Início dos Produtos / Serviços | Data Prevista para Entrega dos Produtos / Serviços | Prazo Total do Contrato (com a Garantia) |
|---|---|---|
| | | |

| 6 – CRITÉRIOS DE AVALIAÇÃO DOS SERVIÇOS | |
|---|---|
| | |
| | |

| 7 – RECURSOS FINANCEIROS | |
|---|---|
| Os recursos financeiros necessários ao pagamento desta Ordem de serviço serão originários da classificação funcional programática abaixo especificada: | |
| Unidade Orçamentária: | |
| Função Programática: | |
| Projeto de Atividade: | |
| Elemento de Despesa: | |
| Fonte de Recurso: | |
| Saldo Orçamentário: | |

| CIÊNCIA | |
|---|---|
| CONTRATANTE | |
| Fiscal Requisitante | Gestor do Contrato |
| _____<br>Nome<br>Matrícula: | _____<br>Nome<br>Matrícula: |
| CONTRATADA | |
| Preposto | |
| _____<br>Nome<br>Cargo | |
| Juazeiro do Norte-CE,_____de _____de 20_____. | |

**MINISTÉRIO DA EDUCAÇÃO**
**UNIVERSIDADE FEDERAL DO CARIRI**
**Pró-Reitoria de Administração**
**ANEXO II DO EDITAL**
**SISTEMA DE REGISTRO DE PREÇOS – SRP**
**PREGÃO ELETRÔNICO Nº 38/2020**
**Modelo de Proposta**

**DADOS DO PROPONENTE**
RAZÃO SOCIAL:
CNPJ/CPF:
ENDEREÇO COMPLETO:
TELEFONE:
E-mail (se houver):
Banco:
Tipo de Conta:
Número da conta:
Agência:

| ITEM | DESCRIÇÃO | UNIDADE | QUANT | VALOR UNITÁRIO MÁXIMO ACEITÁVEL (R$) | VALOR TOTAL (R$) |
|---|---|---|---|---|---|
| | (Material/serviço)<br>Obs.: Descrição de cada Item em conformidade com o Termo de Referência – Anexo I do edital; marca; garantia. | | | | |

**Valor Total do item em algarismos:**
**Valor Total do item por extenso:**
**Prazo de validade** (não inferior a 90 (noventa) dias corridos, a contar da data de sua apresentação):
**Prazo de garantia dos itens e/ou serviços:**
**Composição dos preços:** Nos preços propostos acima estão incluídos todas as despesas, frete, tributos e demais encargos de qualquer natureza incidentes sobre o objeto deste Pregão.
Esta empresa DECLARA estar ciente de que a apresentação da presente proposta implica na plena aceitação das condições estabelecidas no Edital e seus Anexos.
Esta empresa DECLARA que as aquisições constantes da presente proposta ATENDEM ÀS ESPECIFICAÇÕES e todas as exigências constantes no edital e seus anexos.

**(Local e data)**

**(Assinatura do Representante Legal, com NOME COMPLETO e CPF, ambos legíveis)**

**MINISTÉRIO DA EDUCAÇÃO**
**UNIVERSIDADE FEDERAL DO CARIRI**
**Pró-Reitoria de Administração**
**ANEXO III DO EDITAL**
**SISTEMA DE REGISTRO DE PREÇOS – SRP**
**PREGÃO ELETRÔNICO Nº 38/2020**
**Ata de Registro de Preços nº ___**
**Minuta**

ATA DE REGISTRO DE PREÇOS N.º .....
PREGÃO ELETRÔNICO N.º 38/2020

**A UNIVERSIDADE FEDERAL DO CARIRI – UFCA**, com sede na Av. Tenente Raimundo Rocha, nº 1639, Bairro Cidade Universitária, na cidade de Juazeiro do Norte/CE, inscrita no CNPJ sob o nº 18.621.825/0001-99, neste ato representada pelo seu Pró-Reitor de Administração, o Sr. SILVÉRIO DE PAIVA FREITAS JÚNIOR, nomeado pela Portaria nº 1.362, de 11/11/2016, publicada no Diário Oficial da União de 16/11/2016, no exercício das competências que lhe foram subdelegadas pela Portaria nº 062 de 18/02/2020, ambas da Reitoria da Universidade Federal do Cariri, portador da matrícula funcional nº 1772643, considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS nº 38/2020, publicada no ..... de ...../...../20....., processo administrativo nº 23507.002141/2020-56, RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no edital, sujeitando-se as partes às normas constantes na Lei nº 8.666, de 21 de junho de 1993 e suas alterações, no Decreto nº 7.892, de 23 de janeiro de 2013, e em conformidade com as disposições a seguir:

## 1. DO OBJETO

1.1. A presente Ata tem por objeto o registro de preços para a eventual prestação de serviço de fornecimento de licenças para expansão do sistema de gerenciamento de rede e de solução de proteção de dados (Firewall), especificado(s) no(s) item(ns)..... do ..... Termo de Referência, anexo ..... do edital de Pregão nº ...../20..., que é parte integrante desta Ata, assim como a proposta vencedora, independentemente de transcrição.

## 2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. O preço registrado, as especificações do objeto e as demais condições ofertadas na(s) proposta(s) são as que seguem:

| Prestador do serviço *(razão social, CNPJ/MF, endereço, contatos, representante)* | | | | |
|---|---|---|---|---|
| ITEM | DESCRIÇÃO/ ESPECIFICAÇÃO | Unidade de Medida | Quantidade | Valor Unitário |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| ... | | | | |

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

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

3.1. O órgão gerenciador será a Universidade Federal do Cariri – UFCA.

## 4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

4.1 Não será admitida a adesão à ata de registro de preços decorrente desta licitação.

## 5. VALIDADE DA ATA

5.1. A validade da Ata de Registro de Preços será de 12 meses, a partir da data de sua publicação, não podendo ser prorrogada.

## 6. REVISÃO E CANCELAMENTO

6.1. A Administração realizará pesquisa de mercado periodicamente, em intervalos não superiores a 180 (cento e oitenta) dias, a fim de verificar a vantajosidade dos preços registrados nesta Ata.

6.2. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo do objeto registrado, cabendo à Administração promover as negociações junto ao(s) fornecedor(es).

6.3. Quando o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, a Administração convocará o(s) fornecedor(es) para negociar(em) a redução dos preços aos valores praticados pelo mercado.

6.4. O fornecedor que não aceitar reduzir seu preço ao valor praticado pelo mercado será liberado do compromisso assumido, sem aplicação de penalidade.

6.4.1. *A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação original.*

***Nota Explicativa**: Suprimir o item quando inexistirem outros fornecedores classificados registrados na ata.*

6.5. Quando o preço de mercado tornar-se superior aos preços registrados e o fornecedor não puder cumprir o compromisso, o órgão gerenciador poderá:

6.5.1. liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados; e

6.5.2. convocar os demais fornecedores para assegurar igual oportunidade de negociação.

6.6. Não havendo êxito nas negociações, o órgão gerenciador deverá proceder à revogação desta ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

6.7. O registro do fornecedor será cancelado quando:

6.7.1. descumprir as condições da ata de registro de preços;

6.7.2. não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, sem justificativa aceitável;

6.7.3. não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado; ou

6.7.4. sofrer sanção administrativa cujo efeito torne-o proibido de celebrar contrato administrativo, alcançando o órgão gerenciador e órgão(s) participante(s).

6.8. O cancelamento de registros nas hipóteses previstas nos itens 6.7.1, 6.7.2 e 6.7.4 será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa.

6.9. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados:

6.9.1. por razão de interesse público; ou

6.9.2. a pedido do fornecedor.

## 7. DAS PENALIDADES

7.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no Edital.

7.1.1. 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, nos termos do art. 49, §1º do Decreto nº 10.024/19.

7.2. É da competência do órgão gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço (art. 5º, inciso X, do Decreto nº 7.892/2013), exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos participantes, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 6º, Parágrafo único, do Decreto nº 7.892/2013).

7.3. O órgão participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no art. 20 do Decreto nº 7.892/2013, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

## 8. CONDIÇÕES GERAIS

8.1. As condições gerais do fornecimento, tais como os prazos para entrega e recebimento do objeto, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, ANEXO AO EDITAL.

8.2. É vedado efetuar acréscimos nos quantitativos fixados nesta ata de registro de preços, inclusive o acréscimo de que trata o § 1º do art. 65 da Lei nº 8.666/93, nos termos do art. 12, §1º do Decreto nº 7.892/13.

8.3. A ata de realização da sessão pública do pregão, contendo a relação dos licitantes que aceitarem cotar os bens ou serviços com preços iguais ao do licitante vencedor do certame, será anexada a esta Ata de Registro de Preços, nos termos do art. 11, §4º do Decreto n. 7.892, de 2013.

Para firmeza e validade do pactuado, a presente Ata foi lavrada em 02 (duas) vias de igual teor, que, depois de lida e achada em ordem, vai assinada pelas partes.

Local e data
Assinaturas

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

**MINISTÉRIO DA EDUCAÇÃO**
**UNIVERSIDADE FEDERAL DO CARIRI**
**Pró-Reitoria de Administração**
**ANEXO IV DO EDITAL**
**SISTEMA DE REGISTRO DE PREÇOS – SRP**
**PREGÃO ELETRÔNICO Nº 38/2020**
**Minuta**
**Termo de Contrato**
**(pode ser substituído por instrumento equivalente)**

**TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº ...../...., QUE FAZEM ENTRE SI A UNIVERSIDADE FEDERAL DO CARIRI – UFCA E A EMPRESA .....**

**A UNIVERSIDADE FEDERAL DO CARIRI – UFCA**, com sede na Av. Tenente Raimundo Rocha, nº 1639, Bairro Cidade Universitária, na cidade de Juazeiro do Norte/CE, inscrita no CNPJ sob o nº 18.621.825/0001-99, neste ato representada pelo seu Pró-Reitor de Administração, o Sr. SILVÉRIO DE PAIVA FREITAS JÚNIOR, nomeado pela Portaria nº 1.362, de 11/11/2016, publicada no Diário Oficial da União de 16/11/2016, no exercício das competências que lhe foram subdelegadas pela Portaria nº 062 de 18/02/2020, ambas da Reitoria da Universidade Federal do Cariri, portador da matrícula funcional nº 1772643, 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 23507.002141/2020-56e 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 7.892, de 23 de janeiro de 2013, 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 por Sistema de Registro de Preços nº 38/2020, mediante as cláusulas e condições a seguir enunciadas.

## 1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de serviços de fornecimento de

licenças para expansão do sistema de gerenciamento de rede e de solução de proteção de dados (Firewall), que serão prestados nas condições estabelecidas no Termo de Referência, anexo do Edital.

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

1.3. Objeto da contratação:

| ITEM | DESCRIÇÃO/ ESPECIFICAÇÃO | Unidade de Medida | Quantidade | Valor Unitário |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| ... | | | | |

## 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 ...../...../.....

2.1.1. A vigência poderá ultrapassar o exercício financeiro, desde que as despesas referentes à contratação sejam integralmente empenhadas até 31 de dezembro, para fins de inscrição em restos a pagar, conforme Orientação Normativa AGU n° 39, de 13/12/2011.

2.2.1. A execução dos serviços será realizada de acordo com os prazos e condições estabelecidos no subitem 4.7 e no item 6, ambos do Termo de Referência (Requisitos Temporais e Modelo de Execução do Contrato) e na(s) Ordem(ns) de Serviço e/ou Ordem(ns) de Fornecimento de Bens.

2.3. A prorrogação dos prazos de execução e vigência do contrato será precedida da correspondente adequação do cronograma físico-financeiro, bem como de justificativa e autorização da autoridade competente para a celebração do ajuste, devendo ser formalizada nos autos do processo administrativo.

2.4. A CONTRATADA não tem direito subjetivo à prorrogação contratual.

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

## 3. CLÁUSULA TERCEIRA – PREÇO

**3.1** O valor total 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.

## 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. Não haverá exigência de garantia de execução para a presente contratação.

## 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 – SANÇÕES ADMINISTRATIVAS.**

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

**11. CLÁUSULA DÉCIMA PRIMEIRA – RESCISÃO**

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.

12.2.1. 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.

12.2.2. 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 – 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 Subseção Judiciária de Juazeiro do Norte-CE - Justiça Federal, 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 2 (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-