SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA - CONFEA

SEPN 508, Bloco A Ed. Confea - Engenheiro Francisco Saturnino de Brito Filho - Bairro Asa Norte, Brasília/DF, CEP 70740-541

Contato: - http://www.confea.org.br

EDITAL DE LICITAÇÃO

PROCESSO Nº 00.003325/2023-49

PREGÃO ELETRÔNICO Nº 18/2023	**Data de Abertura:** 29/11/2023 às 8h30 no sítio https://www.gov.br/compras/pt-br

OBJETO				
Contratação de empresa especializada em serviços integrados de segurança cibernética de ponta, incluindo a provisão de um sistema de proteção de perímetro robusto e avançado, para atender as necessidades do Conselho Federal de Engenharia e Agronomia - Confea.				
VALOR ESTIMADO				
R$ 3.384.624,43 (três milhões, trezentos e oitenta e quatro mil seiscentos e vinte e quatro reais e quarenta e três centavos).				
REGISTRO DE PREÇO	**VISTORIA**	**INSTRUMENTO CONTRATUAL**	**GARANTIA**	**FORMA DE ADJUDICAÇÃO**

Não	Não	Termo de Contrato	Sim	Global

DOCUMENTOS DE HABILITAÇÃO *O detalhamento dos documentos/requisitos de habilitação deve ser consultado na seção do instrumento convocatório acima indicado	
Requisitos Básicos: - SICAF; - Certidão Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União; e - Demais documentos de habilitação jurídica, fiscal e trabalhista e qualificação econômico-financeira.	Requisitos Específicos: - Documentos para comprovação de habilitação técnica.

LEGISLAÇÃO				**LIC. EXCLUSIVA ME/EPP?**	**RESERV. COTA ME/EPP?**	**EXIGE AMOSTRA/DEM.?**	**DEC. Nº 7.174/2010?**
X	**LEI Nº 8.666/93**		**LEI Nº 14.133/2021**	Não	Não	Não	Sim

PRAZO PARA ENVIO DA PROPOSTA/DOCUMENTAÇÃO	
Até 02 hora(s) após a convocação realizada pelo (a) pregoeiro (a)	
PEDIDOS DE ESCLARECIMENTOS	**IMPUGNAÇÕES**
Até o dia 24/11/2023 para o endereço licitacao@confea.org.br	Até o dia 24/11/2023 para o endereço licitacao@confea.org.br
OBSERVAÇÕES GERAIS	
A disputa dar-se-á pelo modo ABERTO e os lances deverão respeitar o INTERVALO MÍNIMO de diferença de valores entre os lances de 0,05%.	

EDITAL DO PREGÃO ELETRÔNICO Nº 18/2023

UASG CONFEA: 925175

O **Conselho Federal de Engenharia e Agronomia - Confea**, a Gerência de Tecnologia da Informação - GTI e este Pregoeiro, designado pela Portaria nº 248, de 30 de agosto de 2023, levam ao conhecimento dos interessados que farão realizar licitação, na modalidade Pregão Eletrônico, tipo menor preço global, em regime de empreitada por preço global, de acordo com o disposto na Lei nº 10.520, de 17 de julho de 2002, no Decreto nº 10.024, de 20 de setembro de 2019, na Lei Complementar n°123/2016, na IN SEGES/MP nº 5/2017, na IN SGD/ME nº 94/2022, na Lei nº 8.666, de 21 de junho de 1993, e demais legislações subsidiárias e as exigências estabelecidas neste Edital e seus Anexos.

DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO:

DIA: 29/11/2023

HORÁRIO: 8h30 (horário de Brasília/DF)

ENDEREÇO ELETRÔNICO: https://www.gov.br/compras/pt-br

1. **DO OBJETO**

1.1. Contratação de empresa especializada em serviços integrados de segurança cibernética de ponta, incluindo a provisão de um sistema de proteção de perímetro robusto e avançado, para atender as necessidades do Conselho Federal de Engenharia e Agronomia - Confea, conforme especificações técnicas, quantidades e condições gerais constantes no Termo de Referência e seus Anexos.

ITEM	DESCRIÇÃO	QUANT.	UNIDADE	CATSER
1	*Appliance* com capacidade para suportar um *throughput* mínimo de 12 Gb/s.	2	*Hardware*	393277
2	Licença de uso de *software* a ser utilizada no equipamento do Item 01, incluindo garantia, atualização de versões e suporte técnico por 36 meses.	2	*Software*	27464
3	Solução de Zero Trust Network Access (ZTNA) com capacidade para suportar 500 usuários.	500	*Software*	27464
4	Treinamento da Solução Ofertada.	3	Serviço	21172

1.2. O pacote deve incluir o fornecimento de *hardware* (*appliance*), licença de uso e atualizações de versões por um período de 36 meses.

1.3. Em caso de discordância existente entre as especificações deste objeto descritas no Comprasnet e as especificações constantes deste Edital, prevalecerão as últimas.

2. **DO CREDENCIAMENTO**

2.1. O Credenciamento é o nível básico do registro cadastral no Sistema de Cadastramento Unificado de Fornecedores - Sicaf, que permite a participação dos interessados na modalidade licitatória **Pregão**, em sua forma eletrônica.

2.2. O Cadastro no Sicaf deverá ser feito no Portal de Compras do Governo Federal, no sítio https://www.gov.br/compras/pt-br, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira - ICP - Brasil.

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

2.4. A 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.

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

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

3. DAS CONDIÇÕES PARA PARTICIPAÇÃO

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

3.1.1. Para ter acesso ao sistema eletrônico, as interessadas em participar deste **Pregão** deverão dispor de chave de identificação e senha pessoal, informando-se a respeito do funcionamento e regulamento do sistema.

3.1.2. O uso da senha de acesso pela licitante é de sua responsabilidade exclusiva, incluindo qualquer transação por ela efetuada diretamente, ou por seu representante, não cabendo ao provedor do sistema ou ao Confea responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

3.2. Não poderão participar deste Pregão:

3.2.1. Empresa suspensa de participar de licitação e impedida de contratar com o Confea, durante o prazo da sanção aplicada;

3.2.2. Empresa declarada inidônea para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação;

3.2.3. Empresa impedida de licitar e contratar com a União, durante o prazo da sanção aplicada;

3.2.4. Empresa proibida de contratar com o Poder Público, em razão do disposto no art.72, § 8º, V, da Lei nº 9.605/98;

3.2.5. Empresa proibida de contratar com o Poder Público, nos termos do art. 12 da Lei nº 8.429/92;

3.2.6. Quaisquer interessados enquadrados nas vedações previstas no art. 9º da Lei nº 8.666/93;

3.2.6.1. Entende-se por "participação indireta" a que alude o art. 9º da Lei nº 8.666/93 a participação no certame de empresa em que uma das pessoas listadas no mencionado dispositivo legal figure como sócia, pouco importando o seu conhecimento técnico acerca do objeto da licitação ou mesmo a atuação no processo licitatório.

3.2.7. Sociedade estrangeira não autorizada a funcionar no País;

3.2.8. Empresa cujo estatuto ou contrato social não seja pertinente e compatível com o objeto deste **Pregão**;

3.2.9. Empresa que se encontre em processo de dissolução, recuperação judicial, recuperação extrajudicial, falência, concordata, fusão, cisão ou incorporação;

3.2.10. Sociedades integrantes de um mesmo grupo econômico, assim entendidas aquelas que tenham diretores, sócios ou representantes legais comuns, ou que utilizem recursos materiais, tecnológicos ou humanos em comum, exceto se demonstrado que não agem representando interesse econômico em comum;

3.2.11. Consórcio de empresa, qualquer que seja sua forma de constituição;

3.2.12. Cooperativa de mão de obra, conforme disposto no art. 5 da Lei n.º 12.690, de 19 de julho de 2012;

3.2.13. Organização da Sociedade Civil de Interesse Público - OSCIP, em conformidade com o Acórdão nº 746/2014 - TCU - Plenário.

3.3. Como condição para participação no **Pregão**, a licitante deverá encaminhar, em campo próprio do sistema eletrônico, as seguintes declarações:

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

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

3.3.3. que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências deste Edital e seus anexos;

3.3.4. ciente da obrigatoriedade de declarar ocorrências posteriores;

3.3.5. 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 7º, XXXIII, da Constituição;

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

3.3.7. 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;

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

3.4. A declaração falsa relativa ao cumprimento de qualquer condição sujeitará a licitante às sanções previstas em lei e neste edital.

4. DO ENVIO DAS PROPOSTAS E DOS DOCUMENTOS DE HABILITAÇÃO

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

4.1.1. A licitante deverá, na forma expressa no sistema eletrônico, consignar o **valor global da proposta**, o qual incluirá todos os custos e despesas relacionadas à execução e necessários ao cumprimento integral do objeto deste Edital e seus anexos, tais como custos diretos e indiretos, tributos incidentes, materiais, encargos sociais, trabalhistas, transporte diversos, seguros, lucro, taxas e demais despesas.

4.2. As propostas ficarão disponíveis no sistema eletrônico.

4.2.1. Qualquer elemento que possa identificar a licitante importa a desclassificação da proposta, sem prejuízo das sanções previstas nesse edital.

4.2.2. Até a abertura da sessão, a licitante poderá retirar ou substituir a proposta anteriormente encaminhada.

4.3. As propostas terão validade de 90 (noventa) dias, contados da data de abertura da sessão pública estabelecida no preâmbulo deste edital.

4.3.1. Decorrido o prazo de validade das propostas, sem convocação para assinatura do instrumento de contrato, fica a licitante liberada do compromisso assumido.

5. DA CLASSIFICAÇÃO DAS PROPOSTAS

5.1. O Pregoeiro verificará as propostas apresentadas e desclassificará, motivadamente, aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital e seus anexos.

5.2. As propostas serão desclassificadas quando se opuserem a quaisquer dispositivos legais vigentes, quando forem consideradas inexequíveis, e/ou quando forem omissas ou apresentem irregularidades ou defeitos capazes de dificultar o julgamento.

5.2.1. Também será desclassificada proposta que identifique a licitante.

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

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

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

6. DA FORMULAÇÃO DOS LANCES

6.1. O valor a ser considerado para efeito de lances é o **MENOR PREÇO GLOBAL.**

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

6.3. As licitantes poderão oferecer lances sucessivos, observados o horário fixado e as regras de aceitação.

6.4. Só serão aceitos os lances cujos valores forem inferiores ao último lance ofertado e registrado no sistema.

6.5. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de **0,05% (zero vírgula zero cinco por cento).**

6.6. Será adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto”, em que as licitantes apresentarão lances públicos e sucessivos, com prorrogações.

6.7. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

6.8. A prorrogação automática da etapa de lances, de que trata o item anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

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

6.10. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o Pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

6.11. 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 da Economia;

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

6.12. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em 1º (primeiro) lugar.

6.13. Durante o transcurso da sessão pública, as licitantes serão informadas, em tempo real, do valor do menor lance registrado, vedada a identificação do detentor do lance.

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

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

7. DO EXERCÍCIO DO DIREITO DE PREFERÊNCIA (LEI COMPLEMENTAR Nº 123/2006)

7.1. Após a fase de lances, se a proposta mais bem classificada não tiver sido apresentada por microempresa ou empresa de pequeno porte, e houver proposta de microempresa ou empresa de pequeno porte que seja igual ou até 5% (cinco por cento) superior à proposta mais bem classificada, proceder-se-á da seguinte forma:

7.1.1. A microempresa ou a empresa de pequeno porte mais bem classificada poderá no prazo de 05 (cinco) minutos, apresentar proposta de preço inferior à da licitante mais bem classificada e, se atendidas às exigências deste edital, ser contratada.

7.1.2. Não sendo contratada a microempresa ou empresa de pequeno porte mais bem classificada, na forma do subitem anterior, e havendo outras licitantes que se enquadram na condição prevista no caput estas serão convocadas, na ordem classificatória, para o exercício do mesmo direito.

7.1.3. O convocado que não apresentar proposta dentro do prazo de 05 (cinco) minutos, controlados pelo Sistema, decairá do direito previsto nos arts. 44 e 45 da Lei Complementar nº 123/2006.

7.1.4. As propostas apresentadas pelas microempresas ou empresas de pequeno porte e pelas demais empresas deverão ser apresentadas nos mesmos moldes, sem benefícios do Simples Nacional para fins de classificação, conforme o disposto no art. 19, XXIII, da IN nº 02/2008.

7.1.5. Na hipótese de não contratação nos termos previstos nesta seção, o procedimento licitatório prossegue com as demais licitantes.

8. DA NEGOCIAÇÃO

8.1. Encerrada a etapa de envio de lances da sessão pública, o Pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta à licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital e seus anexos.

8.1.1. A negociação será realizada por meio do sistema, podendo ser acompanhada pelas demais licitantes.

8.1.2. O Pregoeiro solicitará à licitante melhor classificada que, no prazo de 02 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste edital e já apresentados.

8.1.2.1. Em caso de instabilidade do sistema Comprasnet que impeça o envio da proposta por meio do campo "CONVOCAR ANEXO", a proposta poderá ser encaminhada para o e-mail licitacao@confea.org.br.

9. DA ACEITABILIDADE DA PROPOSTA

9.1. Encerrada a etapa de negociação, o Pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos.

9.2. A licitante classificada provisoriamente em primeiro lugar deverá encaminhar sua proposta, adequada ao último lance, devidamente preenchida na forma do **Anexo III - Modelo de Proposta de Preços,** em arquivo único, no prazo de 02 (duas) horas, contado da convocação efetuada pelo Pregoeiro.

9.2.1. O Pregoeiro poderá solicitar que a licitante apresente justificativa e/ou memória de cálculo para os percentuais de encargos sociais, tributos ou para quaisquer outros valores e/ou itens informados em suas planilhas.

9.2.2. Em caso de instabilidade do sistema Comprasnet que impeça o envio da proposta por meio do campo "CONVOCAR ANEXO", a proposta poderá ser encaminhada para o e-mail licitacao@confea.org.br.

9.3. Os documentos remetidos por meio da opção “Enviar Anexo” do sistema Comprasnet poderão ser solicitados em original ou por cópia autenticada a qualquer momento, em prazo a ser estabelecido pelo Pregoeiro.

9.4. Os originais ou cópias autenticadas, **caso sejam solicitados**, deverão ser encaminhados a Gerência de Contratações - GEC, situado no SEPN 508, Bloco A, Edifício Confea - Eng. Francisco Saturnino de Brito Filho, Asa Norte, 70.740-541, Brasília - DF.

9.5. A licitante que abandonar o certame, deixando de enviar a documentação indicada nesta seção, será desclassificada e sujeitar-se-á às sanções previstas neste edital.

9.6. O Pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do Confea ou, ainda, de pessoas físicas ou jurídicas estranhas a ele, para orientar sua decisão.

9.7. Não se considerará qualquer oferta de vantagem não prevista neste edital, inclusive financiamentos subsidiados ou a fundo perdido.

9.8. Não se admitirá proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade da licitante, para os quais ela renuncie à parcela ou à totalidade de remuneração.

9.9. O Pregoeiro poderá fixar prazo para o reenvio do anexo contendo a proposta quando o preço total ofertado for aceitável, mas os preços unitários que o compõem necessitem de ajustes aos valores estimados pelo Confea.

9.10. Não serão aceitas propostas com valores **unitários e globais superiores** aos estimados pelo Confea, nos moldes do que consta no **Anexo II - Orçamento Estimativo.**

9.11. Não serão aceitas propostas com preços manifestamente inexequíveis.

9.11.1. Considerar-se-á inexequível a proposta que não venha a ter demonstrada sua viabilidade por meio de documentação que comprove que os custos envolvidos na contratação são coerentes com os de mercado do objeto deste Pregão.

9.11.2. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderá ser efetuada diligência, na forma do § 3º do art. 43 da Lei nº 8.666/93, para efeito de comprovação de sua exequibilidade, podendo-se adotar, dentre outros, os seguintes procedimentos:

9.11.2.1. Questionamentos junto à proponente para a apresentação de justificativas e comprovações em relação aos custos com indícios de inexequibilidade;

9.11.2.2. Levantamento de informações junto aos órgãos públicos competentes;

9.11.2.3. Pesquisas em órgãos públicos ou empresas privadas;

9.11.2.4. Verificação de outros contratos que a proponente mantenha com a Administração ou com a iniciativa privada;

9.11.2.5. Pesquisa de preço com fornecedores dos insumos utilizados, tais como: atacadistas, lojas de suprimentos, supermercados e fabricantes;

9.11.2.6. Verificação de notas fiscais dos produtos adquiridos pela proponente;

9.11.2.7. Estudos setoriais;

9.11.2.8. Consultas às Secretarias de Fazenda Federal, Distrital, Estadual ou Municipal;

9.11.2.9. Análise de soluções técnicas escolhidas e/ou condições excepcionalmente favoráveis que a proponente disponha para a prestação dos serviços;

9.11.2.10. Demais verificações que porventura se fizerem necessárias.

9.12. O não atendimento à solicitação do Pregoeiro no prazo fixado ou a recusa em fazê-lo implica a desclassificação da proposta.

9.12.1. O ajuste da proposta não poderá implicar aumento do seu valor global.

9.13. Será desclassificada a proposta que não corrigir ou não justificar eventuais falhas apontadas pelo Pregoeiro.

9.14. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita da unidade demandante.

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

10. DA HABILITAÇÃO

10.1. A habilitação das licitantes será verificada por meio do Sicaf (habilitação parcial) e da documentação especificada neste edital.

10.1.1. As licitantes que não atenderem às exigências de habilitação parcial no Sicaf deverão apresentar documentos que supram tais exigências.

10.2. O Pregoeiro poderá consultar sítios oficiais de órgãos e entidades emissores de certidões, para verificar as condições de habilitação das licitantes, constituindo a consulta meio legal de prova.

10.3. Ao Pregoeiro ou à autoridade superior é assegurado o direito de solicitar à licitante vencedora, a qualquer tempo, no curso da licitação, quaisquer esclarecimentos sobre os documentos já entregues, fixando-lhes prazo para atendimento.

10.4. Como condição prévia ao exame da documentação de habilitação da licitante detentora da proposta classificada em primeiro lugar, o(a) pregoeiro(a) 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:

10.4.1. Sistema Unificado de Cadastramento de Fornecedores - Sicaf;

10.4.2. Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União (https://certidoes-apf.apps.tcu.gov.br/).

10.5. As consultas previstas na condição anterior realizar-se-ão em nome da sociedade empresária licitante e também de eventual matriz ou filial e de seu sócio majoritário.

10.6. Constatada a existência de sanção, o Pregoeiro reputará a licitante inabilitada, por falta de condição de participação.

10.7. O Pregoeiro consultará o Sicaf em relação à habilitação jurídica, à regularidade fiscal e à qualificação econômica financeira, conforme disposto nos arts. 4º, caput, 8º, § 3º, 13 a 18 e 43, III, da Instrução Normativa SLTI/MPOG nº 2, de 2010.

10.7.1. Também poderão ser consultados os sítios oficiais emissores de certidões, especialmente quando a licitante esteja com alguma documentação vencida junto ao Sicaf;

10.7.2. Caso o Pregoeiro não logre êxito em obter a certidão correspondente por meio do sítio oficial, ou na hipótese de se encontrar vencida no referido sistema, a licitante será convocada a encaminhar, no prazo de 02 (duas) horas, documento válido que comprove o atendimento das exigências deste edital, sob pena de inabilitação, ressalvado o disposto quanto à comprovação da regularidade fiscal das microempresas, empresas de pequeno porte ou sociedade cooperativa a elas equiparada, conforme estatui o art. 43, § 1º da LC nº 123, de 2006.

10.8. As licitantes que não estiverem cadastradas no Sicaf, além do nível de credenciamento exigido pela Instrução Normativa SLTI/MPOG nº 2, de 2010, deverão apresentar a seguinte documentação relativa à Habilitação Jurídica e à Regularidade Fiscal e Trabalhista e Qualificação Econômico-financeira, conforme descrito nos itens **10.9., 10.10. e 10.11.** a seguir.

10.9. Habilitação Jurídica:

10.9.1. Para Empresa Individual: Registro comercial;

10.9.2. Para Sociedade Comercial: Ato constitutivo (estatuto ou contrato social em vigor), devidamente registrado no órgão competente e acompanhado de todas as alterações ou da consolidação respectiva;

10.9.3. Para Sociedades Por Ações: Ato constitutivo (estatuto ou contrato social em vigor), devidamente registrado no órgão competente, acompanhado de documento comprobatório da eleição dos atuais administradores e acompanhado de todas as alterações ou da consolidação respectiva;

10.9.4. Para Sociedades Civis: Inscrição do ato constitutivo, acompanhada de prova de designação da diretoria em exercício e de todas as alterações ou da consolidação respectiva;

10.9.5. Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

10.10. Regularidade fiscal e trabalhista:

10.10.1. Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ);

10.10.2. Prova de regularidade fiscal com a Receita Federal, Estadual/Distrital, Municipal e Dívida Ativa da União;

10.10.3. Prova de regularidade com o Fundo de Garantia por Tempo de Serviço (FGTS);

10.10.4. Prova de regularidade trabalhista (CNDT).

10.10.5. As microempresas e empresas de pequeno porte deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição.

10.10.5.1. Havendo alguma restrição na comprovação da regularidade fiscal, será assegurado o prazo de 05 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que a licitante for declarada vencedora do certame, prorrogáveis por igual período, a critério da Administração, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

10.10.6. A não regularização da documentação, no prazo previsto no subitem anterior, implicará decadência do direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei no 8.666, de 21 de junho de 1993, sendo facultado à Administração convocar as licitantes remanescentes, na ordem de classificação, para a assinatura do contrato, ou revogar a licitação.

10.11. Qualificação Econômico-financeira:

10.11.1. Certidão negativa de falência, recuperação judicial ou recuperação extrajudicial, expedida pelo distribuidor da sede da licitante.

10.11.2. Balanço Patrimonial do último exercício social exigível, apresentado na forma da lei e regulamentos na data de realização deste **Pregão**, vedada sua substituição por balancetes ou balanços provisórios, podendo ser atualizado por índices oficiais quando encerrados há mais de 3 (três) meses da data da sessão pública de abertura deste processo licitatório;

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

10.11.3. Demonstração do Resultado do Exercício (DRE) relativa ao último exercício social exigível, apresentado na forma da lei;

10.11.4. As empresas deverão complementar a comprovação da qualificação econômico-financeira por meio de:

10.11.4.1. Índices de Liquidez Geral (LG), Liquidez Corrente (LC) e Solvência Geral (SG) superiores a 1;

10.11.4.2. Patrimônio Líquido (PL) igual ou superior a 10% (dez por cento) do valor da proposta;

10.11.4.3. Patrimônio Líquido igual ou superior a 1/12 (um doze avos) do valor total dos contratos firmados com a Administração Pública e com a iniciativa privada, vigentes na data da sessão pública de abertura deste **Pregão**.

10.11.4.3.1. Quando houver divergência percentual superior a 10% (dez por cento), para mais ou para menos, entre a declaração aqui tratada e a receita bruta discriminada na Demonstração do Resultado do Exercício (DRE), deverão ser apresentadas, concomitantemente, as devidas justificativas.

10.11.5. Comprovação de patrimônio líquido no limite equivalente a 10% (dez por cento) do valor estimado da contratação, a qual será exigida somente no caso de a licitante apresentar resultado inferior a 1 (um) em qualquer dos índices Liquidez Geral, Liquidez corrente e Solvência Geral, calculados e informados pelo Sicaf;

10.11.6. O balanço patrimonial e as demonstrações contábeis deverão estar assinados por Contador ou por outro profissional equivalente, devidamente registrado no Conselho Regional de Contabilidade.

10.11.7. A boa situação financeira será avaliada pelos Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), que deverão ser iguais ou superiores a 1,00 (um), resultantes da aplicação das seguintes fórmulas:

$$LG = \frac{\text{ATIVO CIRCULANTE + REALIZÁVEL A LONGO PRAZO}}{\text{PASSIVO CIRCULANTE + EXIGÍVEL A LONGO PRAZO}}$$

$$SG = \frac{\text{ATIVO TOTAL}}{\text{PASSIVO CIRCULANTE + EXIGÍVEL A LONGO PRAZO}}$$

$$LC = \frac{\text{ATIVO CIRCULANTE}}{\text{PASSIVO CIRCULANTE}}$$

10.11.8. As fórmulas deverão estar devidamente aplicadas em memorial de cálculos juntado ao balanço;

10.11.8.1. Caso o memorial não seja apresentado, a unidade de licitação reserva-se o direito de efetuar os cálculos;

10.11.9. Se necessária a atualização do balanço e do capital social, deverá ser apresentado, junto aos documentos em apreço, o memorial de cálculo correspondente.

10.12. Habilitação Técnica:

10.12.1. A habilitação técnica será comprovada por meio de:

10.12.1.1. Atestado(s) ou declarações de capacidade técnica emitido(s) por pessoa jurídica de direito público ou privado, lavrados e assinado(s) por servidor/funcionário competente do respectivo órgão ou empresa, que comprove(em) ter a licitante prestado serviço da mesma natureza e compatível com objeto que se pretende.

10.12.1.1.1. Por serviços de mesma natureza e compatível com objeto entender-se-á: fornecimento, instalação, configuração e suporte de Firewall NGFW combinado com solução de ZTNA e/ou Proxy com solução de ZTNA.

10.12.1.2. Declaração de que na data prevista para assinatura do contrato possuirá profissional devidamente e tecnicamente habilitado para responsabilizar-se pela execução de serviços de características semelhantes aos licitados.

10.12.1.3. Apresentação de Planilha Ponto-a-Ponto contendo as Especificações Técnicas Requeridas e a correlação com o Manual/Site do Fabricante.

10.12.1.3.1. A planilha a ser apresentada deverá ser organizada da seguinte maneira:

10.12.1.3.1.1. Coluna 1 "Item": Listar cada item individualmente de acordo com as especificações técnicas mencionadas no Edital e seus anexos;

10.12.1.3.1.2. Coluna 2 "Descrição do Item": Providenciar uma breve descrição de cada item, com foco em como se alinha com as especificações exigidas;

10.12.1.3.1.3. Coluna 3 "Referência no Manual do Fornecedor": Indicar a página ou seção específica do manual do fornecedor onde se demonstra a capacidade da empresa vencedora de fornecer o item em questão, de acordo com as especificações requeridas.

10.12.1.3.2. A conferência será realizada de forma detalhada, item por item, entre a aquisição pretendida e o fornecido pela licitante vencedora, alinhando-se estritamente com as especificações técnicas delineadas neste Edital e seus anexos.

10.12.1.4. Declaração assinada pelo representante legal da licitante que ateste a não ocorrência de registro de oportunidade, nos termos do item 1.7 do Anexo da Instrução Normativa SGD/ME nº 94, de 2022.

10.12.2. 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;

10.12.3. Fica facultado ao Confea, a qualquer momento, realizar diligências, inclusive nas dependências da licitante, com o objetivo de verificar se os atestado(s)/certidão(ões)/declaração(ões) são adequados e atendem as exigências contidas em edital e seus anexos.

10.12.4. Poderá ser exigida a apresentação dos respectivos contratos e aditivos de prestação de serviços relativos aos atestados/certidões/declarações apresentados pela licitante.

10.12.5. Sendo identificadas declarações ou atestados inverídicos, acarretará na desclassificação da licitante.

10.12.6. Constatado o atendimento às exigências fixadas neste edital, a licitante será declarada vencedora.

10.13. A documentação deverá:

10.13.1. estar em nome da empresa licitante;

10.13.2. estar em plena validade na data da sessão;

10.13.3. referir-se a apenas uma das filiais ou apenas a empresa matriz, ou seja, os documentos apresentados deverão referir-se a um mesmo CNPJ/MF, o qual corresponderá àquele constante da proposta, à exceção dos documentos que só possam ser fornecidos por empresa matriz, sob pena de inabilitação ou desclassificação.

10.14. Ao Pregoeiro reserva-se o direito de solicitar o original de qualquer documento, sempre que tiver dúvida ou julgar necessário.

10.14.1. Os originais ou cópias autenticadas, **caso sejam solicitados**, deverão ser encaminhados a Gerência de Contratações - GEC, situado no SEPN 508, Bloco “A”, Edifício Confea - Engenheiro Francisco Saturnino de Brito Filho, Asa Norte, 70.740-541, Brasília - DF.

10.14.2. As licitantes que deixarem de apresentar quaisquer dos documentos exigidos para a habilitação na presente licitação ou os apresentarem em desacordo com o estabelecido neste edital ou com irregularidades, serão inabilitadas, não se admitindo complementação posterior, salvo na forma do art. 43 da Lei Complementar nº 123, de 2006.

11. DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO AO EDITAL

11.1. Até **três dias úteis** antes da data fixada para abertura da sessão pública, qualquer pessoa, física ou jurídica, poderá impugnar o ato convocatório deste **Pregão Eletrônico** mediante petição a ser enviada exclusivamente para o endereço eletrônico licitacao@confea.org.br.

11.2. Caberá ao Pregoeiro, auxiliado pelos setores técnicos competentes, decidir sobre a impugnação **no prazo de dois dias úteis**, contado do data de recebimento da impugnação.

11.3. Acolhida a impugnação contra este edital, será designada nova data para a realização do certame, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

11.4. Os pedidos de esclarecimentos referentes a este procedimento licitatório devem ser enviados ao Pregoeiro, até **três dias úteis** anteriores à data fixada para abertura da sessão pública, exclusivamente para o endereço eletrônico licitacao@confea.org.br.

11.5. Caberá ao Pregoeiro, auxiliado pelos setores técnicos competentes, responder os pedidos de esclarecimentos **no prazo de dois dias úteis**, contado do data de recebimento do pedido.

11.5. As respostas às impugnações e aos esclarecimentos solicitados serão disponibilizadas no sistema eletrônico para os interessados.

12. DOS RECURSOS

12.1. Declarada a vencedora, o Pregoeiro abrirá prazo de até 30 (trinta) minutos, durante o qual qualquer licitante poderá, de forma imediata e motivada, em campo próprio do sistema, manifestar sua intenção de recorrer.

12.2. O Pregoeiro fará juízo de admissibilidade da intenção de recorrer manifestada, aceitando-a ou, motivadamente, rejeitando-a, em campo próprio do sistema.

12.3. Declarada aceita a intenção de recorrer, será concedido o prazo de 03 (três) dias, para apresentar as razões de recurso, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões em igual prazo, que começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses. Ao Pregoeiro será concedido prazo máximo de 5 (cinco) dias para decidir sobre os recursos interpostos.

12.3.1. A falta de manifestação imediata e motivada das empresas licitantes quanto à intenção de recorrer, nos termos do **subitem 12.1**, importará na decadência desse direito, ficando o Pregoeiro autorizado a adjudicar o objeto à empresa licitante vencedora.

12.3.2. A não apresentação das razões de recurso, em meio eletrônico, em campo próprio do sistema Comprasnet, retornará ao Pregoeiro a responsabilidade de adjudicar o certame licitatório.

12.4. O acolhimento do recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

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

12.6. As razões e contrarrazões de recurso, bem como a decisão do Pregoeiro e da autoridade competente, deverão ser feitas em campo próprio do sistema Comprasnet, no endereço https://www.gov.br/compras/pt-br.

13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

No julgamento das propostas, será(ão) considerada(s) vencedora(s) a(s) licitante(s) que ofertar(em) o **menor preço global**, proposto para o fornecimento do objeto da licitação, desde que atendidas as especificações constantes do edital, após decididos os recursos, quando houver, sujeito à homologação do Ordenador de Despesas.

14. DO INSTRUMENTO CONTRATUAL

14.1. A contratação formalizar-se-á mediante a assinatura eletrônica de instrumento particular, observadas as cláusulas e condições deste Edital e da proposta vencedora, conforme a minuta do Contrato que integra este edital.

14.2. Após homologado o resultado deste pregão, será a licitante vencedora notificada, por escrito, para assinatura eletrônica do termo de Contrato, do qual serão parte integrante, ainda que não transcritas total ou parcialmente no referido instrumento, as condições estabelecidas neste edital, a proposta da empresa vencedora e todos os elementos técnicos que serviram de base à licitação.

14.3. A assinatura eletrônica do Contrato pela adjudicatária dar-se-á por meio do Sistema Eletrônico de Informações (SEI) do Confea e no prazo de **até 5 (cinco) dias úteis**, a contar da data de sua convocação.

14.4. O prazo de convocação poderá ser prorrogado, uma única vez, por igual período, quando solicitado pela licitante vencedora, por escrito, durante o seu transcurso e desde que ocorra motivo justificado e aceito pelo Confea.

14.5. É de responsabilidade da licitante vencedora proceder com seu **cadastro** como usuário externo no mencionado Sistema Eletrônico de Informações (SEI) do Confea, conforme suas normas próprias, em tempo hábil para a assinatura do Contrato no prazo estabelecido, acessando a página de Acesso a Usuário Externo no link a seguir: http://processoeletronico.confea.org.br/usuarioexterno/.

14.5.1. A liberação de acesso do usuário externo será efetuada em **até 5 (cinco) dias úteis** contados a partir do recebimento da documentação, que deverá seguir as orientações contidas na página de Acesso a Usuário Externo.

14.6. A assinatura do Contrato ficará vinculada à manutenção das condições da habilitação, à plena regularidade fiscal e trabalhista da empresa vencedora e à inexistência de registro perante o Sistema de Cadastramento Unificado de Fornecedores - Sicaf que caracterize impedimento à contratação com o Confea, sendo aplicáveis as penalidades definidas no **item 15**, em caso de descumprimento.

14.7. É vedada a contratação de empresa privada que tenha em seu quadro societário servidor público da ativa, ou empregado de empresa pública, ou sociedade de economia mista, com fundamento no art. 18, inciso VIII, da Lei nº 13.080, de 2 de janeiro de 2015 (LDO 2015).

14.8. Se a licitante vencedora não comprovar as condições de habilitação consignadas no Edital, ou recusar-se, injustificadamente, a assinar eletronicamente o termo de Contrato no prazo estabelecido, poderá ser convocado outro licitante, respeitada a ordem de classificação, para, após comprovados os requisitos habilitatórios e feita a negociação, assinar o Contrato, sem prejuízo das penalidades previstas neste edital e no Contrato e das demais cominações legais.

14.9. O Confea realizará consultas ao Sicaf, CEIS, CNJ e Lista dos Inidôneos do TCU, para identificar possível impedimento para contratar junto ao poder público, antes da emissão de nota de empenho bem como da assinatura de contrato.

15. DAS SANÇÕES ADMINISTRATIVAS

15.1. A licitante será sancionada com o impedimento de licitar e contratar com o Confea e será descredenciado no Sicaf e no cadastro de fornecedores do Confea, pelo prazo de 02 (dois) anos e multa de 10% (dez por cento) sobre o valor adjudicado, sem prejuízo das demais cominações legais, nos seguintes casos:

15.1.1. Cometer fraude fiscal;

15.1.2. Apresentar documento falso;

15.1.3. Fizer declaração falsa;

15.1.4. Comportar-se de modo inidôneo.

15.2. A licitante será sancionada com o impedimento de licitar e contratar com o Confea e será descredenciado no Sicaf e no cadastro de fornecedores do Confea, pelo prazo de 01 (um) ano e multa de 5% (cinco por cento) sobre o valor adjudicado, nos seguintes casos:

15.2.1. Deixar de entregar a documentação exigida no certame;

15.2.2. Não mantiver a proposta, salvo por motivo justo decorrente de fato superveniente e aceito pelo(a) pregoeiro(a);

15.2.3. Não assinar o contrato.

15.3. A licitante será sancionada com multa de 2,5% (dois vírgula cinco por cento) sobre o valor adjudicado no caso de não assinar o contrato no prazo estabelecido.

15.4. Para os fins do **subitem 15.1.4**, reputar-se-ão inidôneos atos como os descritos nos arts. 90, 92, 93, 94, 95 e 97 da Lei nº 8.666, de 1993.

15.5. Caberá ao Ordenador de Despesa, após o devido processo legal, garantido o contraditório e a ampla defesa, decidir pela aplicação da sanção administrativa cabível.

16. DA DOTAÇÃO ORÇAMENTÁRIA

16.1. A despesa orçamentária para a contratação do objeto deste instrumento correrá a cargo das seguintes Contas Orçamentárias nº: 6.2.2.1.1.02.01.03.006 - Equipamentos de Processamento de Dados, 6.2.2.1.1.01.04.09.005 - Serviços de Informática e 6.2.2.1.1.01.04.09.011 - Serviços de Seleção e Treinamento de Pessoal, do

Centro de Custo 3.3.02 - TI Atividades de Tecnologia da Informação.

16.2. No exercício seguinte, as despesas correrão à conta de dotações orçamentárias próprias, consignadas nos respectivos Orçamentos Anuais, ficando o Confea obrigado a apresentar, no início do exercício, a respectiva Nota de Empenho estimativa e, havendo necessidade, emitir Nota de Empenho complementar, respeitada a mesma classificação orçamentária.

17. DO PRAZO DE EXECUÇÃO E VIGÊNCIA DO CONTRATO

O contrato terá vigência de **36 (trinta e seis) meses** contados da data da assinatura do Contrato pelo CONTRATANTE, podendo ser prorrogado nos moldes da legislação vigente.

18. DAS DISPOSIÇÕES FINAIS

18.1. É facultada ao Pregoeiro ou à autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo.

18.2. Fica assegurado ao Confea, o direito de revogar a licitação por razões de interesses públicos, decorrentes de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado.

18.2.1. A anulação do **Pregão** induz à do Contrato.

18.3. É parte integrante deste Edital e seus anexos, independente de sua transcrição, a integralidade do **Processo nº 00.003325/2023-49** vinculado aos termos do **Pregão Eletrônico nº 18/2023,** cuja realização decorre da autorização da autoridade superior deste Conselho, e da proposta da CONTRATADA**.**

18.4. São partes integrantes deste edital os seguintes anexos:

Anexo I - Termo de Referência

Anexo II - Orçamento Estimativo

Anexo III - Modelo de Proposta de Preços

Anexo IV - Termo de Compromisso e Manutenção de Sigilo

Anexo V - Termo de Ciência e Manutenção de Sigilo

Anexo VI - Termo de Recebimento Provisório (TRP)

Anexo VII - Termo de Recebimento Definitivo (TRD)

Anexo VIII - Minuta de Contrato

O presente documento segue assinado pela autoridade responsável por sua aprovação, com fulcro no Regimento Interno do CONFEA, cujos fundamentos passam a integrar a presente decisão por força do art. 50, § 1º, da Lei nº 9.784, de 29 de janeiro de 1999.

Visto Jurídico sobre os aspectos formais:

João de Carvalho Leite Neto (OAB/DF 19.914)

Chefe da Subprocuradoria Consultiva - mat. 592

Documento assinado eletronicamente por **João de Carvalho Leite Neto**, **Chefe da Subprocuradoria Consultiva**, em 06/11/2023, às 14:01, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Walace Francisco Ferreguetti**, **Gerente**, em 06/11/2023, às 15:06, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.confea.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0850114** e o código CRC **2FAC00B8**.

EDITAL DO PREGÃO ELETRÔNICO Nº 18/2023

ANEXO I - TERMO DE REFERÊNCIA DE TIC GTI Nº 0809206/2023

1. **OBJETO**

1.1. Contratação de empresa especializada em serviços integrados de segurança cibernética de ponta, incluindo a provisão de um sistema de proteção de perímetro robusto e avançado. O pacote deve incluir o fornecimento de *hardware* (*appliance*), licença de uso e atualizações de versões por um período de 36 meses.

2. **CATMAT OU CATSER**

2.1. Consoante artigo 12 da Instrução Normativa nº 94, de 23 de dezembro de 2022, "O Termo de Referência ou Projeto Básico será elaborado pela Equipe de Planejamento da Contratação a partir do Estudo Técnico Preliminar da Contratação, incluindo, no mínimo, as seguintes informações: [...] II - código(s) do Catálogo de Materiais - Catmat ou do Catálogo de Serviços - Catser relacionado(s) a cada item da contratação, disponíveis no Portal de Compras do Governo Federal".

2.2. Através de consulta à Planilha CATMAT-CATSER disponível no Portal de Compras do Governo Federal, infere-se que o CATSER mais apropriado para o presente Termo de Referência conforme tabela abaixo:

Item	CatSer	Descrição	Quantidade
1	393277	*Appliance* com capacidade para suportar um *throughput* mínimo de 12 Gb/s.	2
2	27464	Licença de uso de *software* a ser utilizada no equipamento do Item 01, incluindo garantia, atualização de versões e suporte técnico por 36 meses.	2
3	27464	Solução de Zero Trust Network Access (ZTNA) com capacidade para suportar 500 usuários.	500
4	21172	Treinamento da Solução Ofertada.	3

3. DESCRIÇÃO E JUSTIFICATIVA PARA A CONTRATAÇÃO/AQUISIÇÃO

3.1. A Tecnologia da Informação é um elemento vital para o funcionamento eficiente do Confea e para a realização de sua missão institucional. A segurança das redes é um pilar fundamental nesse processo, pois protege as informações estratégicas do Conselho e garante a continuidade de suas operações.

3.2. Atualmente, o Confea utiliza o *firewall* da Palo Alto Networks, modelo 5250, que tem desempenhado com eficiência o papel de proteger e controlar os acessos entre os computadores do Conselho e a *Internet*, além de manter uma VPN (Virtual Private Network) segura.

3.3. No entanto, esse dispositivo entrará em estado de *End-Of-Sale* (Fim de Vendas) em 31 de Agosto de 2023, o que significa que ele não será mais comercializado pela empresa fabricante e em decorrência disso as atualizações, suporte e peças de reposição poderão ficar escassas. Isso acarreta um risco de segurança significativo, pois implica que qualquer nova ameaça de segurança poderá não ser abordada pelo fabricante através de atualizações de *software* ou *firmware.* Por esta razão é importante planejar com antecedência e considerar a aquisição de um novo *firewall*.

3.4. As razões para isso são várias. Em primeiro lugar, a evolução constante das ameaças de segurança torna necessária a atualização regular das ferramentas de proteção. Os *firewalls* mais recentes oferecem capacidades aprimoradas de detecção e prevenção de ameaças, bem como melhor desempenho e escalabilidade para lidar com volumes de tráfego cada vez maiores.

3.5. Além disso, um novo *firewall* pode proporcionar recursos e capacidades que não estão presentes na solução atual, como melhores funcionalidades de inteligência de ameaças, automação de políticas e integração com outras soluções de segurança. Esses benefícios podem melhorar ainda mais a proteção oferecida pelo Confea e proporcionar uma segurança de rede mais holística e eficaz.

3.6. Adicionalmente, a transição para uma nova solução de *firewall* permite uma abordagem estratégica para avaliar e selecionar a melhor opção de acordo com as necessidades atuais e futuras do Confea. Isso pode incluir a consideração de outros fornecedores além da Palo Alto Networks que podem oferecer recursos e funcionalidades que melhor atendam às necessidades específicas do Conselho.

3.7. A contratação de Suporte Técnico Especializado para a administração operacional da nova solução de segurança é também uma parte crucial deste processo. Empresas especializadas nesta área possuem a experiência e o conhecimento necessários para gerir adequadamente estas soluções, proporcionando ao Confea maior tranquilidade e segurança em suas operações.

3.8. Desta forma, apesar do *firewall* atual ainda não estar oficialmente em fim de vida, a aquisição de um novo dispositivo e a contratação de suporte técnico especializado são investimentos essenciais para garantir a segurança contínua dos sistemas corporativos, dados e equipamentos do Confea. Eles não apenas fornecerão proteção contra as ameaças atuais e futuras, mas também garantirão a disponibilidade, integridade e confidencialidade das informações, redes e sistemas do Confea, proporcionando um ambiente operacional seguro e estável para o Conselho continuar a desempenhar suas funções de forma eficiente e segura.

4. DEFINIÇÃO E ESPECIFICAÇÃO DE REQUISITOS

4.1. **a1) de negócio**, que independem de **características tecnológicas** e que definem as necessidades e os aspectos funcionais da solução de TIC;

4.1.1. Segurança de Rede: O *firewall* deve ser capaz de proteger a rede do Confea de ataques externos e internos, tais como tentativas de intrusão, ataques de negação de serviço (DoS), entre outros;

4.1.2. Controle de Acesso: A solução deve permitir a configuração e a administração de regras de acesso à rede, permitindo que apenas usuários e sistemas autorizados tenham acesso a recursos específicos da rede;

4.1.3. Monitoramento e Relatórios: A solução deve fornecer funcionalidades robustas de monitoramento e relatórios, para permitir a análise de tráfego de rede, detecção de ameaças e análise de incidentes de segurança;

4.1.4. Atualizações e Suporte: O fornecedor da solução deve ser capaz de fornecer atualizações regulares de segurança e suporte contínuo para garantir que a solução esteja sempre atualizada e protegida contra as mais recentes ameaças de segurança;

4.1.5. Conformidade: A solução deve estar em conformidade com os padrões de segurança e governança, quando aplicáveis;

4.1.6. Custo-Efetividade: A solução deve ser custo-efetiva, ou seja, deve fornecer um alto nível de segurança e funcionalidade pelo preço mais razoável possível;

4.1.7. Facilidade de Integração e Uso: A solução deve ser fácil de integrar com outros sistemas e soluções de TIC existentes, e deve ser fácil de usar para administradores de rede e outros usuários.

4.2. **b1) de capacitação**, que definem a necessidade de treinamento, de carga horária e de materiais didáticos;

4.2.1. Em função do Confea não possuir um corpo técnico conhecedor da solução a ser adquirida, se faz necessária capacitação/treinamento formal acerca da solução pretendida. Muito embora qualquer intervenção necessária em função de falhas de *hardware*/*software* estará coberta pela garantia do fabricante estipulada em Contrato, ainda assim, o corpo técnico do Conselho precisará ter domínio da tecnologia para fins de definição de topologia, apoio à instalação, operação diária e integração com o restante da rede;

4.2.2. Local: O treinamento deverá ser ministrado em uma localização central e de fácil acesso em Brasília - Distrito Federal;

4.2.3. Quantitativo: Deverá habilitar 1 (um) profissional na tecnologia objeto destes Requisitos;

4.2.4. Estima-se que o Confea habilite 3 (três) profissionais na tecnologia.

4.2.5. Carga Horária: O treinamento deve totalizar uma carga horária mínima de 40 horas, dividida em sessões de 8 horas ao longo de uma semana. O treinamento deve ser ministrado em um horário que seja conveniente os participantes;

4.2.6. Materiais Didáticos: O fornecedor do treinamento deve fornecer todos os materiais didáticos necessários, incluindo manuais, guias de estudo e recursos online. Todos os materiais devem ser atualizados e relevantes para o conteúdo do treinamento;

4.2.7. Ambiente Tecnológico: O ambiente de treinamento deve incluir acesso a computadores e *software* necessários, bem como uma conexão de *internet* estável e de alta velocidade;

4.2.8. Instrutores: Os instrutores devem ter experiência comprovada na área de treinamento e ser capazes de fornecer instruções claras e eficazes. Eles também devem estar disponíveis para responder a perguntas e oferecer suporte durante o treinamento e devem possuir certificação oficial da Fabricante da Solução;

4.2.9. No caso de soluções que não disponibilizam uma certificação oficial do fabricante, será aceito um comprovante equivalente que demonstre o conhecimento e a competência da equipe de instrutores com a solução em questão. Isso pode incluir, mas não limitado a: referências de clientes anteriores, portfólio de projetos passados ou demonstrações de experiência prática. Nesses casos, solicitamos que a empresa submeta uma descrição detalhada do método alternativo de validação, para que possamos avaliar sua adequação.

4.2.10. Avaliação: Deve haver um processo para avaliar o entendimento e a retenção de conhecimento dos participantes ao longo do treinamento. Isso pode incluir testes, *quizzes*, ou projetos práticos;

4.2.11. Certificado: Ao final do treinamento, o participante deve receber um certificado de conclusão que comprove sua participação e aprendizado.

4.3. **c1) legais**, que definem as normas com as quais a solução de TIC deve estar em conformidade;

4.3.1. Decreto-Lei 200/67 - Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências;

4.3.2. Lei nº 8.666 de 21 de junho de 1993 - estabelece normas gerais sobre licitações e contratos administrativos pertinentes a obras, serviços, inclusive de publicidade, compras, alienações e locações no âmbito dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios;

4.3.3. Decreto Nº 3.505, de 13 de junho de 2000 - Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

4.3.4. Decreto Nº 3.555, de 08 de agosto de 2000 - Aprova o Regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns;

4.3.5. Decreto Nº 10.024, de 20 de setembro de 2019 - Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências;

4.3.6. Decreto Nº 7.174, de 12 de maio de 2010 - Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;

4.3.7. Decreto nº 7.845, de 14 de novembro de 2012 - regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

4.3.8. Lei Nº 10.520, de 17 de julho de 2002 - Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns;

4.3.9. Lei Nº 11.077, de 30 de dezembro de 2004 - Altera a Lei no 8.248, de 23 de outubro de 1991, a Lei no 8.387, de 30 de dezembro de 1991, e a Lei no 10.176, de 11 de janeiro de 2001, dispondo sobre a capacitação e competitividade do setor de informática e automação e dá outras providências;

4.3.10. Instrução Normativa n° 94/2022, da Secretaria de Governo Digital do Ministério Economia - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

4.3.11. Plano Diretor de Tecnologia da Informação - PDTI do Conselho Federal de Engenharia e Agronomia - Confea;

4.3.12. A solução a ser contratada também deverá estar alinhada à ISO/IEC 20000, às normas de segurança ABNT 27001 e 27002, bem como às diretrizes do Confea em relação ao uso de recursos de Tecnologia da Informação.

4.3.13. General Data Protection Regulation (GDPR): Regulamento Geral de Proteção de Dados da União Europeia que estabelece requisitos para a proteção de dados pessoais e privacidade de indivíduos na UE.

4.3.14. Cybersecurity Information Sharing Act (CISA): Lei dos EUA que estabelece um quadro para compartilhamento de informações de segurança cibernética entre agências governamentais e empresas privadas.

4.3.15. ISO 27001: Padrão internacional de segurança da informação que estabelece requisitos para um sistema de gestão de segurança da informação eficaz.

4.3.16. NIST Cybersecurity Framework: Quadro de segurança cibernética do Instituto Nacional de Padrões e Tecnologia dos EUA que fornece orientação sobre a identificação, proteção, detecção, resposta e recuperação de ameaças cibernéticas.

4.4. **d1) de manutenção**, que independem de configuração tecnológica e que definem a necessidade de serviços de manutenção preventiva, corretiva, adaptativa e evolutiva (melhoria funcional);

4.4.1. Manutenção Preventiva: É essencial que a solução escolhida inclua serviços regulares de manutenção preventiva, com o objetivo de detectar e prevenir possíveis problemas antes que eles ocorram. Isso pode incluir a atualização regular de *software*, revisões de configuração e auditorias de segurança.

4.4.2. Manutenção Corretiva: Este requisito se refere à necessidade de serviços de reparo para corrigir falhas e defeitos no *firewall*. Isso pode incluir suporte técnico para solução de problemas e reparo ou substituição de componentes de *hardware*, se aplicável.

4.4.3. Manutenção Adaptativa: A solução de *firewall* deve permitir alterações para se adaptar a novas circunstâncias ou requisitos, como mudanças na infraestrutura de rede, novos padrões de segurança ou regulamentações, ou a introdução de novas tecnologias.

4.4.4. Manutenção Evolutiva (Melhoria Funcional): Além de manter a funcionalidade existente, é importante que a solução de *firewall* escolhida seja capaz de evoluir e melhorar ao longo do tempo. Isso pode incluir a adição de novos recursos, melhorias de desempenho e capacidade de se adaptar a novas ameaças e cenários de segurança.

4.4.5. **d.1.1) preventiva:**

4.4.6. Atualizar os *firmwares* e/ou *softwares* das soluções que compõe a solução e das respectivas consoles de gerenciamento;

4.4.7. Realizar os ajustes e melhorias constantes, de acordo com as melhores práticas dos fabricantes; mantê-las documentas e acessíveis no *website* (portal do cliente);

4.4.8. Propor melhorias no ambiente de forma proativa, periodicamente, mantê-las documentadas no site (portal do cliente) e submetê-las para a aprovação do CONTRATANTE;

4.4.9. **Gerenciamento do ambiente;**

4.4.10. Entregar mensalmente, até o 5º dia útil do mês, os relatórios gerenciais (níveis de serviço, atualizações de versões, incidentes, estatísticas sobre desempenho e melhorias propostas, entre outras recomendações);

4.4.11. Entregar os níveis de serviço (SLA) através de informativos eletrônicos através do *website* (portal do cliente) da CONTRATADA;

4.4.12. A CONTRATADA deverá identificar regras duplicadas ou que podem ser otimizadas para aumentar a performance dos equipamentos;

4.4.13. Caso a CONTRATADA identifique regras com risco elevado ao negócio, a mesma orientará o CONTRATANTE sobe os riscos de execução da regra;

4.4.14. Identificação e bloqueio de arquivos com conteúdo sensível a organização;

4.4.15. Todas as atualizações que envolvam indisponibilidade do ambiente, devem ser agendadas com a equipe técnica do CONTRATANTE;

4.4.16. A CONTRATADA deverá gerar relatórios mensais (enviados por e-mail a todas as pessoas pré-definidas pela equipe do CONTRATANTE), e quando solicitados pelo CONTRATANTE, extraídos da solução de *Next Generation Firewall*, contendo atividades detectadas conforme os itens abaixo:

4.4.17. Ameaças;

4.4.18. Filtro de Conteúdo Bloqueado;

4.4.19. Análises do *Sandbox*;

4.4.20. Acesso a VPN;

4.4.21. Falhas detectadas na solução;

4.4.22. Arquivos que foram analisados pela solução NGF;

4.4.23. Disponibilização de painéis na Solução:

4.4.24. A CONTRATADA deverá realizar a configuração de painéis e relatórios de monitoramento na Solução fornecida, de modo a permitir o acompanhamento do status diário da solução pelo CONTRATANTE;

4.4.25. A CONTRATADA deve configurar um conjunto básico de painéis, contendo indicadores definidos de acordo as bases específicas para monitoramento, podendo as mesmas serem customizadas para o ambiente do CONTRATANTE.

4.4.26. **Gerência de Serviços;**

4.4.27. Confeccionar e entregar relatórios mensais dos resultados dos serviços prestados, com análise crítica clara elaborada pelos times técnicos da contratada;

4.4.28. Confecção e disponibilização de *dashboards* diários apresentando indicadores D-1;

4.4.29. Agendar reunião para apresentação presencial dos resultados dos serviços prestados mensalmente ou de acordo com a disponibilidade do CONTRATANTE;

4.4.30. Realizar pesquisa de qualidade operacional periodicamente, documentando e disponibilizando os resultados para a contratante em reunião presencial;

4.4.31. Apoio consultivo para melhoria continua da segurança do ambiente;

4.4.32. Confecção de relatórios técnicos pontuais sob demanda;

4.4.33. Alinhamento e negociação dos indicadores de serviço;

4.4.34. Desenvolvimento e manutenção do plano de comunicação;

4.4.35. O gerenciamento dos parâmetros da solução de *Next Generation Firewall*, em fase posterior a implantação deverão obrigatoriamente ser executados conforme o seguinte sempre que solicitado:

4.4.36. Criação de regras de *firewall*;

4.4.37. A CONTRATADA deverá identificar regras duplicadas ou que podem ser otimizadas para aumentar a performance dos equipamentos;

4.4.38. A CONTRATADA deverá sugerir melhorias nas regras para melhor organização; Caso a CONTRATADA identifique regras com risco elevado ao negócio, a mesma orientará o CONTRATANTE sobe os riscos de execução da regra;

4.4.39. Criação de objetos;

4.4.40. Criação de regras de NAT;

4.4.41. Criação de rotas;

4.4.42. Controle de acesso a VPN;

4.4.43. Criação de túnel IPSEC;

4.4.44. Configuração de túnel IPSEC;

4.4.45. Configuração de novas interfaces;

4.4.46. Revisão de regras;

4.4.47. Backup de configurações.

4.4.48. Atividades diferenciadas:

4.4.49. Mitigação de *malwares* em *endpoints* infectados;

4.4.50. Identificação de movimentação lateral de tráfego, onde o fluxo de dados não é controlado pela solução de FW;

4.4.51. Identificação e bloqueio de arquivos com conteúdo sensível a organização;

4.4.52. Para o gerenciamento de ativos deverão ser aplicadas todas as recomendações da fabricante;

4.4.53. Todas as atualizações que envolvam indisponibilidade do ambiente, devem ser agendadas com a equipe técnica da fabricante;

4.5. **e1) temporais**, que definem datas de entrega da solução de TIC contratada;

4.5.1. Data de Início: A implementação da solução de *firewall* deve começar dentro de 10 dias corridos a partir da emissão da Ordem de Serviço pelo Confea.

4.5.2. Cronograma de Implementação: A instalação do *hardware*, configuração e integração do sistema com a infraestrutura de TI existente deve ser concluída dentro de um período de 60 dias a partir da data de início.

4.5.3. Data de Conclusão: A solução de *firewall* deve estar totalmente operacional e integrada ao ambiente de TI do Confea dentro de 90 (noventa) dias a partir da data de emissão da Ordem de Serviço.

4.5.4. Período de Suporte: Após a data de conclusão, o fornecedor deve fornecer suporte e manutenção contínuos por um período mínimo de 36 (trinta e seis) meses. Este suporte deve incluir todas as formas de manutenção - preventiva, corretiva, adaptativa e evolutiva (melhoria funcional).

4.5.5. Janelas de Manutenção: As atividades de manutenção devem ser realizadas em períodos acordados para minimizar o impacto na operação do sistema. Por exemplo, as atualizações de sistema podem ser agendadas para serem realizadas durante as horas de menor atividade, como nos finais de semana ou durante a noite.

4.6. **f1) de segurança e privacidade;**

4.6.1. Proteção de Dados: O *firewall* deve ser capaz de proteger os dados sensíveis e pessoais processados e armazenados pelo Confea, aplicando mecanismos de criptografia de dados em repouso e em trânsito, além de prevenir a exposição de dados sensíveis e a violação de privacidade.

4.6.2. Prevenção de Intrusões: A solução deve ser capaz de prevenir intrusões indesejadas, detectar atividades suspeitas e possuir recursos de mitigação de ataques como DDoS.

4.6.3. Autenticação e Autorização: O *firewall* deve permitir o controle rigoroso de acesso aos recursos do sistema, implementando a autenticação de usuários e a atribuição de direitos de acesso com base no princípio do mínimo privilégio.

4.6.4. Conformidade Legal: O *firewall* deve ajudar o Confea a cumprir todas as leis e regulamentos relevantes, como a Lei Geral de Proteção de Dados (LGPD), garantindo a privacidade e a proteção dos dados pessoais dos usuários.

4.6.5. Atualizações e *Patches* de Segurança: A solução deve permitir a aplicação fácil e rápida de atualizações e patches de segurança para corrigir vulnerabilidades que possam surgir.

4.6.6. Registros e Auditoria: O *firewall* deve permitir o registro e a auditoria detalhados de todas as atividades, para permitir a detecção de quaisquer eventos de segurança e apoiar investigações e conformidade.

4.6.7. Resiliência: A solução deve garantir alta disponibilidade e capacidade de recuperação rápida em caso de falhas ou ataques, para minimizar a interrupção dos serviços.

4.7. **g1) sociais, ambientais e culturais;**

4.7.1. Sociais: A solução de *firewall* deve respeitar as normas e leis locais, bem como a privacidade dos usuários;

4.7.2. Ambientais: A solução de *firewall* deve obedecer a uma política de responsabilidade ambiental, contribuindo para a redução do consumo de energia e do desperdício. O *hardware* deve ser fabricado de maneira sustentável, utilizando materiais reciclados quando possível, e deve ter opções de reciclagem ou descarte ecologicamente correto no final da vida útil. Além disso, a empresa fornecedora deve estar comprometida com a minimização das emissões de carbono, o que pode ser demonstrado por meio de certificações ambientais;

4.7.3. Culturais: A solução escolhida deve estar em conformidade com os idiomas oficiais do Brasil, com a documentação técnica e suporte ao cliente disponíveis em português. Além disso, deve-se respeitar as normas e valores culturais do país e da organização;

4.7.4. Nesse contexto, também é importante observar o Guia Nacional de Contratações Sustentáveis, e suas atualizações, elaborado pela Câmara Nacional de Sustentabilidade da Controladoria Geral da União/Advocacia Geral da União, para garantir que a solução esteja em conformidade com as práticas recomendadas de sustentabilidade.

4.8. **a) de arquitetura tecnológica, composta de *hardware*, *software*, padrões de interoperabilidade, linguagens de programação, interfaces, dentre outros;**

4.9. **Características específicas do equipamento *Next Generation Firewall*:**

4.10. O *firewall* deve ser capaz de manter um *throughput* (taxa de transferência de dados) de pelo menos 12 Gbps quando a funcionalidade de "Threat Prevention" (Prevenção de Ameaças) está habilitada. Essa funcionalidade deve incluir os serviços de: *Firewall*, IPS (Sistema de Prevenção de Intrusões), Controle de

Aplicação e Antivírus;

4.10.1. Isto significa que o *firewall* deve ser capaz de examinar o tráfego de rede e aplicar todas essas funções de segurança, mantendo um alto nível de desempenho de pelo menos 12 *gigabits* por segundo. Em outras palavras, ele precisa ser capaz de processar uma grande quantidade de dados rapidamente, mesmo quando está executando várias tarefas de segurança intensivas ao mesmo tempo.

4.11. O *firewall* deve ser capaz de manter um *throughput* (taxa de transferência de dados) de pelo menos 35 Gbps quando estiver realizando criptografia e descriptografia de tráfego de rede usando o protocolo VPN IPSec:

4.11.1. IPSec é um conjunto de protocolos usados para proteger comunicações de *internet*, autenticando e criptografando cada pacote de dados em uma sessão de comunicação. Ele é comumente usado para criar VPNs, ou redes privadas virtuais, que permitem aos usuários criar uma conexão segura e criptografada através de uma rede menos segura, como a internet;

4.11.2. Portanto, essa especificação significa que o *firewall* precisa ser capaz de processar um alto volume de dados criptografados e descriptografados rapidamente, mantendo um desempenho de pelo menos 35 *gigabits* por segundo.

4.12. O *firewall* deve estar licenciado para, ou ser capaz de suportar sem a necessidade de uma licença adicional, 2000 túneis VPN IPSec Site-to-Site simultâneos:

4.12.1. Um túnel VPN Site-to-Site é uma conexão segura entre duas redes localizadas em locais diferentes. Neste caso, o *firewall* deve ser capaz de manter simultaneamente 2000 dessas conexões seguras, seja por meio de uma licença inclusa na aquisição ou pelo suporte inerente do equipamento a esta capacidade, sem a necessidade de licenças adicionais.

4.13. Estar licenciado para, ou suportar sem o uso de licença, 5.000 túneis de VPN IPSec Client-to-Site:

4.13.1. O *firewall* precisa ser capaz de estabelecer até 5.000 conexões seguras de rede privada virtual (VPN) entre a rede da organização e os clientes individuais (geralmente dispositivos de usuários finais, como computadores ou celulares) que estão fora da rede principal, sem a necessidade de aquisição de uma licença extra para essa funcionalidade.

4.14. O *firewall* deverá ter capacidade para lidar com um elevado volume de tráfego na rede, apresentando suporte para estabelecer e gerenciar, no mínimo, 500 mil novas conexões por segundo. Essa habilidade é essencial para assegurar um alto desempenho e a segurança da rede, mesmo em cenários de alto tráfego, onde um grande número de dispositivos estará buscando estabelecer conexões simultâneas com a rede;

4.15. A solução de *firewall* deve oferecer uma capacidade de inspeção SSL (Secure Sockets Layer) com *throughput* de, no mínimo, 8 Gbps. Essa capacidade é crucial para o processo de inspeção e filtragem do tráfego de rede criptografado, sem comprometer a performance da rede. Dessa maneira, a segurança das comunicações é mantida, mesmo em situações onde o volume de tráfego de dados criptografados é elevado;

4.16. A solução de *firewall* deve contar com, no mínimo, 8 interfaces Ethernet Gigabit (1 GE) com conector RJ45. Essas interfaces são essenciais para a conexão de dispositivos na rede e para a realização de configurações de rede específicas;

4.17. Deve ter disponível, no mínimo, 8 interfaces Gigabit Ethernet (1 GE) do tipo SFP (Small Form-factor Pluggable) com *transceivers* incluídos. Estas interfaces são fundamentais para a flexibilidade de conexões de fibra óptica ou cobre;

4.18. A solução deve dispor de, no mínimo, 8 interfaces 10 Gigabit Ethernet (10 GE) do tipo SFP+ com *transceivers* inclusos, oferecendo velocidades de transmissão maiores para suportar requisitos de alta largura de banda;

4.19. Deve possuir ao menos 2 *interfaces* 100 Gigabit Ethernet (100 GE) QSFP28 / 40 Gigabit Ethernet (40 GE) QSFP+ com *transceivers* inclusos, permitindo conectividade de alta velocidade e desempenho para aplicações intensivas de dados;

4.20. A solução deve ser capaz de suportar a criação de, no mínimo, 10 instâncias virtuais. Isso permite maior flexibilidade na configuração e gestão de ambientes de rede virtualizados;

4.21. Deve incluir armazenamento interno de, no mínimo, 480 GB, configurado com dois discos em arranjo RAID 1 (Redundant Array of Independent Disks) para cada equipamento. Isso proporciona maior confiabilidade de dados através da redundância;

4.22. A solução de *firewall* precisa ter uma fonte de alimentação interna, redundante e que permita substituição em funcionamento (hot-swap), garantindo a continuidade das operações mesmo em caso de falha de uma das fontes de alimentação;

4.23. Deve ser compatível com instalação em *racks* padrão de 19 polegadas, padrão amplamente utilizado em *data centers* e armários de rede, facilitando a instalação e o gerenciamento dos equipamentos.

4.24. **Características gerais dos equipamento *Next Generation Firewall*:**

4.25. A solução deve consistir em plataforma de proteção de rede baseada em *appliance* físico com funcionalidades de *Next Generation Firewall* (NGFW), não sendo permitido *appliances* virtuais ou solução *open-source* (produto montado);

4.26. Os *hardwares* e os *softwares* que compõem a solução devem ser do mesmo fabricante;

4.27. As funcionalidades de NGFW devem ser ofertadas no mesmo *appliance*, não sendo permitido a composição de equipamentos separados para cada uma das funções;

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

4.27.2. Reconhecimento de aplicações: Também conhecido como controle baseado em aplicação, essa funcionalidade permite que o NGFW identifique e controle o tráfego de rede com base nas aplicações específicas que estão sendo usadas. Isso é importante porque, ao contrário dos *firewalls* tradicionais, que geralmente bloqueiam ou permitem o tráfego com base apenas no número da porta, os NGFWs podem reconhecer e tomar decisões baseadas na aplicação real que está sendo usada;

4.27.3. Prevenção de ameaças: Os NGFWs têm a capacidade de detectar e bloquear ameaças avançadas, como *malware*, *ransomware* e outras ameaças que os *firewalls* tradicionais podem não ser capazes de lidar. Isso é muitas vezes alcançado através da integração com outras tecnologias de segurança, como sistemas de prevenção de intrusões (IPS), proteção avançada contra *malware* (AMP) e *sandboxing;*

4.27.4. Identificação de usuários: Esta funcionalidade permite que o NGFW identifique usuários individuais ou grupos de usuários na rede. Isso é útil para a aplicação de políticas de segurança baseadas em usuários e para rastrear a atividade do usuário na rede;

4.27.5. Controle granular de permissões: Esta funcionalidade permite que os administradores de segurança definam permissões muito específicas para o tráfego de rede. Por exemplo, um administrador pode permitir que um grupo de usuários acesse uma aplicação específica, mas apenas em determinados horários do dia. Isso proporciona um alto nível de controle e personalização para as políticas de segurança da rede;

4.28. A plataforma deve ser otimizada para análise de conteúdo de aplicações em Camada 7;

4.29. Para todos os equipamentos deverá ser fornecido bandeja ou suporte para montagem em *rack*;

4.30. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

4.31. Deverá suportar *tags* de VLAN (802.1Q);

4.32. Deverá possuir suporte a agregação de *links* via 802.3ad LACP;

4.33. Deverá possuir ferramenta de diagnóstico do tipo *tcpdump* e ainda dispor de ferramenta integrada à *interface web* para capturar informações dos pacotes em tempo real, podendo aplicar filtros, tais como: IPs e portas, e ainda ter disponível a possibilidade de exportar a captura para um arquivo do tipo PCAP visando estender a análise para um *software* terceiro, tal como *Wireshark*;

4.34. Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

4.35. Deverá possuir integração com *tokens* para autenticação de duplo fator;

4.36. Deverá suportar *single-sign-on*;

4.37. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT;

4.38. Deverá suportar roteamento estático para IPv4 e IPv6;

4.39. Deverá suportar roteamento dinâmico para IPv4 e IPv6 (OSPF, BGP, RIP);

4.40. Deverá suportar ECMP;

4.41. Os dispositivos de proteção de rede devem possuir suporte a roteamento *multicast* (PIM-SM e PIM-DM);

4.42. Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;

4.43. Deverá suportar aplicações multimídia, tais como: H.323 e SIP;

4.44. Deverá suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo;

4.45. Deverá permitir o funcionamento em modo transparente tipo "*bridge*";

4.46. Deverá suportar PBR – Policy Based Routing;

4.47. Deverá possuir conexão entre estação de gerência e *appliance* criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

4.48. Deverá possuir mecanismo de *anti-spoofing*;

4.49. Deverá permitir criação de regras definidas pelo usuário;

4.50. Deverá suportar *sFlow* ou *Netflow*;

4.51. Os dispositivos de proteção de rede devem possuir suporte a *Jumbo Frames*;

4.52. Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

4.53. Deverá permitir funcionamento em modo *bridge* em Camada 2, roteador em Camada 3, *proxy* explícito e *sniffer* via espelhamento;

4.54. Deverá possuir mecanismo de tratamento de sessão (session-helpers ou ALGs);

4.55. Deve possuir suporte a criação de sistemas virtuais no mesmo *appliance* e que possam ser administrados por equipes distintas;

4.56. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

4.57. Deve suportar o protocolo padrão da indústria VXLAN;

4.58. Permitir, para o gerenciamento da solução, interface de administração via *web* no próprio dispositivo;

4.59. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do *cluster*, eventos de segurança e estatísticas das verificações de saúde da camada SD-WAN;

4.60. Deve disponibilizar controle, inspeção e de-criptografia de SSL para tráfego de entrada e saída, sendo que deve suportar ainda o controle dos certificados individualmente dentro de cada sistema virtual, ou seja; isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais;

4.61. Em caso de ser gerenciado de forma centralizada, o equipamento ofertado deverá continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos com a solução de gerência centralizada;

4.62. Deverá possuir conectores de SDN e dessa forma ser capaz de sincronizar de forma automática objetos;

4.63. Deverá suportar ambientes *multi-cloud*;

4.64. Deverá possuir a capacidade de criar automações através de gatilhos e ações, possibilitando uma atuação mais proativa;

4.65. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

4.66. A configuração em alta disponibilidade deve sincronizar:

4.66.1. Sessões;

4.66.2. Configurações, incluindo, mas não limitado às políticas de *Firewall*, NAT, QoS e objetos de rede;

4.66.3. Associações de Segurança das VPNs;

4.66.4. Tabelas FIB;

4.66.5. Assinaturas de IPS, Antivírus e *Anti-Spyware*;

4.67. A configuração de alta disponibilidade deve possibilitar monitoração de falha de *link*;

4.68. 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;

4.68.1. Caso o licenciamento/funcionalidade não seja permanente, o fornecedor deverá prover as funcionalidades por 12 (doze) meses;

4.69. Deve possuir ferramenta de classificação de segurança e monitoramento em tempo real para analisar e identificar possíveis vulnerabilidades, destacar as melhores práticas que podem ser usadas para melhorar a segurança e o desempenho da solução;

4.70. Esta ferramenta deve ser capaz de avaliar continuamente se as configurações estão funcionando de forma eficaz e alertar as equipes de segurança sobre riscos e vulnerabilidades que podem afetar as operações diárias;

4.71. O serviço analisa e relata continuamente as alterações na topologia da rede, simplifica a identificação e correção de dispositivos de alto risco e fornece planos de ação e relatórios de progresso para as partes interessadas em nível técnico e de gerenciamento;

4.72. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de *End-of-Life e End-of-Sale*;

4.73. **Funcionalidades de Firewall:**

4.74. Deverá possuir controle de acesso à *Internet* por endereço IP de origem e destino;

4.75. Deverá possuir controle de acesso à *Internet* por subrede;

4.76. Deverá ter a capacidade de criar políticas de *firewall* baseando-se em endereços MAC;

4.77. Deverá suportar controles por zonas de segurança;

4.78. Deverá suportar controles de políticas por porta e protocolo;

4.79. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

4.80. Controle de políticas por usuários, grupos de usuários, IPs, range de IPs, subrede, FQDN e zonas de segurança;

4.81. Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

4.82. Deve possibilitar a visualização dos países de origem e destino nos *logs* dos acessos;

4.83. Deve ser viável criar políticas com exceções, onde seja possível especificar que uma política será aplicada somente caso a origem ou destino do tráfego não seja um determinado objeto, tal como uma subrede, por exemplo, ou seja, se a subrede não for 192.168.0.0/24, o tráfego deverá ser tratado;

4.84. Controle, inspeção e de-criptografia de SSL por política para tráfego de saída;

4.85. Deve ser possível realizar um espelhamento do tráfego de-criptografado;

4.86. Deve de-criptografar tráfego de saída em conexões negociadas com TLS 1.2 e TLS 1.3;

4.87. A inspeção SSL deve ser compatível com HTTP3. Tal inspeção é essencial uma vez que uma grande quantidade de sítios públicos está utilizando o protocolo em questão, tais como serviços de compartilhamento de vídeos, sites de busca e redes sociais, os quais estão sendo diariamente consumidos por usuários corporativos e externos;

4.88. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

4.89. Deve suportar objetos de endereço IPv4 e IPv6 consolidados na mesma política de *firewall;*

4.90. Suporte a objetos e regras *multicast*;

4.91. Deve ser possível criar políticas de *firewall* utilizando serviços de ameaças de terceiros, onde o *firewall* receberá uma lista de endereços IPs maliciosos, por exemplo, a qual poderá ser utilizada para bloqueio do tráfego;

4.92. Deve ser possível criar política de *firewall* em modo de aprendizado, onde o equipamento deverá monitorar o tráfego que transita nas interfaces de origem e destino e registrar *logs* de eventos;

4.93. Deve possuir base com objetos contendo endereços IPs de serviços da *Internet* como, a citar, mas não se limitando a AWS S3, Microsoft Azure, Oracle, SAP, Google e Microsoft Office 365, atualizados dinamicamente pela solução;

4.94. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos *firewalls*. Suportar, pelo menos, a tomada de ações como execução de *scripts*, envio de e-mails, notificações via Teams e APIs mediante *hosts* comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

4.95. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

4.96. Deve dispor de ferramenta para auxiliar a descobrir quais políticas correspondem a um determinado perfil de tráfego, facilitando assim a administração diária da solução e facilmente encontrando quais políticas estão sendo atribuídas a um determinado IP, por exemplo.

4.97. **Controle de Aplicações:**

4.98. Os equipamentos destinados à segurança da rede devem apresentar a habilidade de identificar aplicações, independentemente de restrições relativas a portas ou protocolos utilizados;

4.99. A solução deve permitir a permissão ou restrição de aplicações específicas sem que haja a obrigação de liberar ou bloquear portas e protocolos específicos; a gestão de segurança deve ser centrada nas aplicações, independentemente dos detalhes técnicos subjacentes à sua execução;

4.100. A solução deverá ter a capacidade de identificar no mínimo 2.000 (duas mil) diferentes aplicações, com a inclusão, mas não se restringindo, ao tráfego associado a comunicação *peer-to-peer*, interações em redes sociais, conexões remotas, atualizações de *software*, diversos protocolos de rede, VoIP, transmissões de áudio e vídeo, serviços de *proxy*, mensagens instantâneas, partilha de arquivos, comunicação por e-mail, entre outras aplicações. Além disso, o sistema deverá possuir a

capacidade de adaptar-se a novas aplicações e comportamentos de rede, garantindo a segurança e a integridade da rede independente das constantes evoluções do cenário de aplicações digitais;

4.101. Deve ser capaz de reconhecer pelo menos as seguintes aplicações: *google-docs, evernote, webex, gotomeeting, rpc over http, snmp, ntp, msrpc, wins, dns, ftp, dhcp, itunes, radius, ldap, kerberos, active directory, oracle, mysql, db2, skydrive, google drive, dropbox, 4shared, whatsapp, gmail chat, facebook chat, http-tunnel, http-proxy, youtube, gmail, vnc, ms-rdp, teamviewer, logmein, citrix, twitter, linked-in, facebook, skype, gnutella, bittorrent*.

4.102. Deve realizar uma análise minuciosa do conteúdo de pacotes de dados (*payload*) para identificar padrões correspondentes a aplicações conhecidas pelo fabricante, independentemente da porta ou protocolo utilizados;

4.103. Deve ter a habilidade de detectar e controlar aplicações e ameaças que empregam estratégias evasivas através de comunicações criptografadas, como, por exemplo, o *Skype* e o uso da *rede Tor*;

4.104. Para tráfego SSL criptografado, deve decifrar pacotes a fim de possibilitar a inspeção do conteúdo do *payload* para verificação de assinaturas de aplicações familiarizadas ao fabricante;

4.105. Deve decodificar protocolos com o intuito de detectar aplicações escondidas dentro do protocolo e verificar se o tráfego está em conformidade com a especificação do protocolo. A decodificação de protocolos também deve ser capaz de identificar funcionalidades específicas de uma aplicação;

4.106. Deve detectar a implementação de estratégias evasivas através de comunicações criptografadas;

4.107. Deve atualizar a base de dados de assinaturas de aplicações de maneira automática;

4.108. Os dispositivos de proteção de rede devem ser capazes de identificar o usuário da rede com integração ao Microsoft Active Directory, sem necessidade de instalar um agente no Controlador de Domínio, nem nas estações dos usuários;

4.109. Deve ser viável incluir o controle de aplicações em várias regras de segurança do dispositivo, não limitando a habilitação do controle de aplicações a apenas algumas regras;

4.110. Deve suportar diversos métodos de identificação e classificação de aplicações, utilizando pelo menos a verificação de assinaturas e decodificação de protocolos;

4.111. Deve permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na interface gráfica da solução, sem a necessidade de intervenção do fabricante;

4.112. O fabricante deve aceitar pedidos para inclusão de aplicações na base de assinaturas de aplicações;

4.113. Deve informar o usuário quando uma aplicação for bloqueada;

4.114. Deve permitir a diferenciação e controle de tráfego *Peer2Peer* (bittorrent, emule, etc), com níveis detalhados de controle/políticas para essas aplicações;

4.115. Deve permitir a diferenciação e controle de tráfego de mensagens instantâneas (AIM, Hangouts, Facebook Chat, etc), com níveis detalhados de controle/políticas para essas aplicações;

4.116. Deve possibilitar a distinção e controle de componentes específicos de aplicações, como, por exemplo, autorizar o *Hangouts* e bloquear as chamadas de vídeo;

4.117. Deve possibilitar a distinção e controle de aplicações de *proxy* (psiphon, freegate, etc), com níveis detalhados de controle/políticas para essas aplicações;

4.118. Deve permitir a criação de grupos dinâmicos de aplicações com base em características das aplicações, como a tecnologia utilizada (Cliente-Servidor, Baseado em Navegação, Protocolo de Rede, etc);

4.119. Deve permitir a criação de grupos dinâmicos de aplicações baseados em características das aplicações, como o nível de risco da aplicação e a categoria da aplicação;

4.120. Deve ser possível substituir uma ação específica para uma aplicação e para um filtro, onde os filtros podem ser adicionados com base no comportamento da aplicação, como aplicações com alto uso de banda, evasivas ou com comportamento de *botnet*;

4.121. Deve ser possível editar uma aplicação associando parâmetros para análise, como parâmetros associados a comandos na aplicação FTP.

4.122. **Prevenção de Ameaças:**

4.123. Para a defesa ambiental contra adversidades, os dispositivos de segurança precisam ter integrados ao *appliance* de *firewall*, um módulo de Sistema de Prevenção de Intrusões (IPS), Antivírus e Anti-Spyware;

4.124. Deve compreender assinaturas de IPS para prevenir intrusões e bloquear arquivos danosos (Antivírus e Anti-Spyware);

4.125. Deverá integrar um antivírus em tempo real, voltado para o *gateway* da Internet, à estrutura de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP;

4.126. Deve atualizar as assinaturas de *IPS, Antivírus, Anti-Spyware* em caso de alta disponibilidade;

4.127. Deverá adotar as seguintes ações em resposta a ameaças identificadas pelo IPS: permitir, permitir e registrar *log*, bloquear e colocar em quarentena o IP do atacante por um período;

4.128. As assinaturas devem poder ser ativadas, desativadas ou apenas monitoradas;

4.129. Deve ser possível formular políticas por usuário, grupos de usuários, IPs, redes ou zonas de segurança;

4.130. Devem ser possíveis exceções por IP de origem ou destino nas regras ou assinatura;

4.131. Deve suportar a definição de políticas detalhadas de IPS, Antivírus e Anti-Spyware, permitindo a formação de políticas distintas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos estes fatores;

4.132. Deve habilitar o bloqueio de vulnerabilidades;

4.133. Deve possibilitar o bloqueio de explorações conhecidas;

4.134. Deve incluir defesa contra ataques de negação de serviço;

4.135. Deve ser resistente e capaz de barrar ataques básicos como: *Syn flood, ICMP flood, UDP flood,* etc;

4.136. Detectar e barrar a origem de varreduras de porta;

4.137. Bloquear ataques realizados por *worms* conhecidos;

4.138. Deve ter assinaturas específicas para a mitigação de ataques DoS e DDoS;

4.139. Deverá ter assinaturas para bloqueio de ataques de *buffer overflow*;

4.140. Deve permitir a criação de assinaturas customizadas através da interface gráfica do produto;

4.141. Deve permitir o uso de operadores de negação na criação de assinaturas customizadas de IPS ou *Anti-spyware*, possibilitando a formação de exceções com detalhamento nas configurações;

4.142. Identificar e barrar a comunicação com *botnets;*

4.143. Registrar no painel de monitoramento as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

4.144. Deve possuir a função de proteger a resolução de endereços via DNS, identificando solicitações de resolução de nome para domínios mal-intencionados de *botnets* conhecidas;

4.145. Os eventos devem identificar o país de onde a ameaça se originou;

4.146. Deve incluir defesa contra vírus em conteúdo HTML e *javascript, spyware e worms;*

4.147. Precisa ter proteção contra *downloads* não intencionais usando HTTP de arquivos executáveis e mal-intencionados;

4.148. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques com base em políticas do *firewall* considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc;

4.149. Deve ser capaz de mitigar Ameaças Avançadas Persistentes (APT) através de análises dinâmicas para identificação de *malwares* desconhecidos;

4.150. Entre as análises realizadas, a solução deve suportar antivírus, consulta na nuvem, emulação de código, *sandboxing* e verificação de *call-back;*

4.151. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado de *sandbox*. Deve ainda disponibilizar um relatório completo da análise realizada em cada arquivo submetido;

4.152. Deve ser possível filtrar assinaturas com base no identificador CVE;

4.153. Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE, bem como um "*wildcard*" do CVE para abranger mais de um identificador;

4.154. As assinaturas devem dispor de um resumo explicando o ataque associado, nível de severidade, impacto e uma possível recomendação, bem como deve vincular o(s) CVE(s) correspondente(s) quando aplicável;

4.155. Deve incluir defesa contra ataques de negação de serviço;

4.156. Registrar no painel de monitoramento as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

4.157. **Filtro de URL's;**

4.158. Deverá oferecer a capacidade de determinar políticas conforme o tempo, isto é, estabelecer normas para horários ou intervalos específicos (dia, mês, ano, dia da semana e hora);

4.159. A criação de políticas por agrupamentos de usuários, endereços IP, redes ou áreas de segurança deverá ser possível;

4.160. Deve ter a competência para criar políticas baseadas na visibilidade e controle de quem usa quais URLs, integrando com serviços de diretório, *Active Directory* e banco de dados local;

4.161. A identificação através do *Active Directory* deve habilitar SSO, de modo que os usuários não tenham que fazer *login* novamente na rede para passar pelo *firewall*;

4.162. Deve suportar a criação de políticas baseadas no controle por URL e categoria de URL;

4.163. Deve ter categorias de URLs pré-estabelecidas pelo fabricante que podem ser atualizadas a qualquer momento;

4.164. Deve ter no mínimo 50 categorias de URLs;

4.165. Deve contar com a função para excluir URLs do bloqueio;

4.166. Deverá permitir a personalização da página de bloqueio;

4.167. Deve possibilitar a limitação do acesso a canais específicos do YouTube, permitindo a configuração de uma lista de canais permitidos ou uma lista de canais bloqueados;

4.168. Deve impedir o acesso a conteúdo inadequado quando se utiliza a pesquisa em sites como Google, Bing e Yahoo, independentemente da opção *Safe Search* estar ativada no navegador do usuário;

4.169. Deve contar com recurso de prevenção contra *phishing* de credenciais, analisando quais estão sendo submetidas em sites externos, e ainda bloquear ou alertar o usuário;

4.170. Deve proporcionar a opção de estabelecer uma cota diária de uso web baseada em categoria, podendo estabelecer a cota com base, pelo menos, no tempo de uso e volume de tráfego;

4.171. Deverá ser possível bloquear tráfego HTTP POST, método usado para envio de informação a um *website* específico;

4.172. Deverá ser capaz de filtrar e remover *Java applets, ActiveX e cookies* do tráfego *web* inspecionado;

4.173. Deve possuir em sua base de dados uma lista de bloqueio contendo URLs de certificados mal-intencionados;

4.174. A filtragem de tráfego de vídeo com base na categoria e até mesmo no identificador de um canal do YouTube, por exemplo, deve ser possível;

4.175. Além de suportar *Web Proxy* explícito, deverá permitir *Proxy Web* transparente;

4.176. **Identificação de usuários:**

4.177. 7.1. Deve incorporar a habilidade de formular políticas baseadas na visibilidade e controle de quem está usando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, *Active Directory, E-directory* e banco de dados local;

4.178. 7.2. Deve dispor de integração com *Microsoft Active Directory* para identificação de usuários e grupos, possibilitando o controle detalhado/políticas com base em usuários e grupos de usuários;

4.179. 7.3. Deve contar com integração e suporte a *Microsoft Active Directory* para o sistema operacional Windows Server 2012 R2;

4.180. 7.4. Deve proporcionar integração com *Microsoft Active Directory* para identificação de usuários e grupos, possibilitando o controle detalhado/políticas com base em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve ter limites licenciados de usuários;

4.181. 7.5. Deve disponibilizar integração com *Radius* para identificação de usuários e grupos, possibilitando o controle detalhado/políticas com base em usuários e grupos de usuários;

4.182. 7.6. Deve oferecer integração com LDAP para identificação de usuários e grupos, possibilitando o controle detalhado/políticas com base em Usuários e Grupos de usuários;

4.183. 7.7. Deve possibilitar o controle, sem necessidade de instalação de cliente de *software*, em equipamentos que solicitem acesso à *internet*, para que antes do início da navegação, seja expandido um portal de autenticação residente no *firewall* (Captive Portal);

4.184. 7.8. Deve apresentar suporte para identificação de vários usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, proporcionando visibilidade e controle detalhado por usuário sobre o uso das aplicações que estão nesses serviços;

4.185. 7.9. Deve implementar a formação de grupos personalizados de usuários no *firewall*, baseado em atributos do LDAP/AD;

4.186. 7.10. Deve comportar *Security Assertion Markup Language* (SAML), atuando como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP);

4.187. **Filtro de dados:**

4.188. 8.1. Deve oferecer a capacidade de identificar e, se necessário, impedir a transferência de diversos tipos de arquivos (MS Office, PDF, etc) reconhecidos sobre aplicações (HTTP, FTP, SMTP, etc);

4.189. 8.2. Deve ser capaz de identificar arquivos comprimidos ou aplicar políticas sobre o conteúdo desses tipos de arquivos;

4.190. 8.3. Deve fornecer suporte para a identificação de arquivos criptografados e a implementação de políticas sobre o conteúdo desses tipos de arquivos;

4.191. 8.4. Deve possibilitar a identificação e, se necessário, a prevenção da transferência de informações delicadas, incluindo, mas não se limitando a números de cartão de crédito, possibilitando a elaboração de novos tipos de dados por meio de expressão regular.

4.192. **Geolocalização:**

4.192.1. Deve possibilitar a elaboração de políticas baseadas em geolocalização, permitindo o bloqueio de tráfego proveniente de determinado(s) país(es);

4.192.2. Deve permitir a exibição dos países de origem e destino nos registros de acesso;

4.193. **Rede Virtual Privada (VPN):**

4.193.1. Deve prover suporte para VPN IPSec Site-to-Site;

4.193.2. A VPN IPSEC deve oferecer suporte para criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);

4.193.3. A VPN IPSEc deve oferecer suporte para autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

4.193.4. A VPN IPSEc deve oferecer suporte para os Grupos Diffie-Hellman 1, 2, 5, 14, de 15 até 21 e de 27 até 32;

4.193.5. A VPN IPSEc deve prover suporte para o Algoritmo de Troca de Chaves da Internet (IKEv1 e v2);

4.193.6. A VPN IPSEc deve suportar autenticação via certificado IKE PKI;

4.193.7. Deve ter interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

4.194. **VPN Cliente para Site:**

4.194.1. Deve fornecer suporte para VPN IPSec;

4.194.2. Deve oferecer suporte para VPN SSL;

4.194.3. A VPN SSL deve permitir que o usuário realize a conexão através de cliente instalado no sistema operacional do equipamento ou através de interface WEB;

4.194.4. As funcionalidades de VPN SSL devem ser disponibilizadas com ou sem a utilização de um agente;

4.194.5. Deve ser possível canalizar todo o tráfego dos usuários remotos de VPN para dentro do túnel de VPN, prevenindo comunicação direta com dispositivos locais como proxies;

4.194.6. Deve ser possível a atribuição de DNS nos clientes remotos de VPN, incluindo DNS split tunnel;

4.194.7. Deve permitir a criação de políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

4.194.8. Deve oferecer suporte para autenticação via AD/LDAP, certificado e base de usuários local;

4.194.9. Deve fornecer suporte para leitura e verificação de CRL (lista de revogação de certificados);

4.194.10. Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que trafegam dentro dos túneis SSL;

4.194.11. A VPN SSL deve permitir a mudança de senha no Active Directory pelos usuários remotos;

4.194.12. A VPN SSL deve permitir a personalização da tela em sessões RDP;

4.194.13. O *firewall* deve permitir que seja configurado como um cliente VPN SSL, permitindo que o tráfego de usuários locais seja canalizado por essa VPN;

4.194.14. O agente de VPN SSL ou IPSEC cliente-para-site deve ser compatível com, no mínimo: Windows 7 (32 e 64 bits), Windows 8.1 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.14 e superior).

4.195. **Zero Trust Network Access:**

4.195.1. A solução de ZTNA deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um *proxy* de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas;

4.195.2. A solução deve estar licenciada para um total de 500 (quinhentos) usuários;

4.195.3. A solução de ZTNA deve prover um método de controlar o acesso identificando o dispositivo do usuário, autenticação e postura com base em *tags* de Zero Trust;

4.195.4. A solução de ZTNA deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão;

4.195.5. A solução de *proxy* de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por cada usuário;

4.195.6. Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem;

4.195.7. A solução deve ser escalável até 50.000 agentes;

4.195.8. O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante;

4.195.9. Deve ser compatível com pelo menos os seguintes sistemas operacionais: Microsoft Windows: 7 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11 (64 bits), Microsoft Windows Server: 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022, Mac OS X: versões 13, 12, 11 e 10.15, Linux: Ubuntu 18.04 e posterior, Debian 11 e posterior, CentOS Stream 8, CentOS 7.4 e posterior, RedHat 7.4 e posterior, Fedora 36 e posterior;

4.195.10. A solução de ZTNA deve dispor de mecanismos para analisar a requisição *TLS Client hello* e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel;

4.195.11. A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.3;

4.195.12. Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação *multifator*) no processo de autenticação dos usuários;

4.195.13. A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso;

4.195.14. Deve ser possível revogar o certificado de um agente por meio da console central;

4.195.15. O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao *proxy* de acesso;

4.195.16. No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o *proxy* de acesso conhece. Caso algum desses dados esteja diferente, o acesso deverá ser bloqueado por padrão;

4.195.17. Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional;

4.195.18. A solução deve prover *backup* automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até cinco dias anteriores ao ocorrido;

4.195.19. Deve ser possível determinar para quais funcionalidades o *log* deve estar habilitado e permitir que esses dados sejam enviados para a console central;

4.195.20. Deve suportar pelo menos os seguintes níveis de log: emergência, alerta, crítico, erro, aviso, informativo, *debug*;

4.195.21. Deve ser possível exportar os *logs* diretamente a nível de agente;

4.195.22. Deve ser possível exigir uma senha para desconectar o agente da console central;

4.195.23. Deve existir a possibilidade de restringir o usuário de realizar *backup* da configuração do agente;

4.195.24. Deve ser possível evitar que o usuário realize um *shutdown* do agente após estar registrado à console central;

4.195.25. Deve ser possível enviar os *logs* para uma ferramenta de consolidação de *logs* do mesmo fabricante, visando consolidar os *logs* do proxy de acesso ZTNA em conjunto com os *logs* dos agentes. Deve ser possível ainda atribuir *tags* aos *endpoints* de acordo com o índice de comprometimento detectado pela solução de consolidação de *logs*, desde que haja licenciamento instalado para tal;

4.195.26. Deve ser possível configurar o agente para usar *Proxy*;

4.195.27. O agente deve permitir a configuração local via XML (eXtensible Markup Language);

4.195.28. Deve existir a possibilidade de criar um convite para que os usuários realizem o registro do agente à console central;

4.195.29. Este convite deve gerar um código a ser inserido no passo de registro do agente e deve ser possível ainda adicionar um passo de verificação da autenticação do usuário, podendo associar a autenticação via base de dados local, LDAP e SAML;

4.195.30. Deverá ser possível enviar uma notificação por e-mail contendo o código de registro para os usuários finais informados, bem como um *link* para *download* do instalador do agente;

4.195.31. Deve ser possível especificar a validade do código de registro;

4.195.32. A console central de agentes deve dispor de métodos para determinar se um usuário está *on-net ou off-net*, ou seja, dentro ou fora da rede corporativa. Deve ser possível ainda criar perfis de configurações distintos para os usuários *on-net e off-net*;

4.195.33. A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4;

4.195.34. Deve ser possível agrupar agentes em grupos;

4.195.35. Deve ser possível atribuir grupos de agentes a perfis de políticas específicos;

4.195.36. Deve ser possível atribuir um nível de prioridade a um perfil de política visando priorizar qual política será utilizada caso um grupo de agentes esteja associado a mais de um perfil de política;

4.195.37. A console central deve apresentar um resumo das informações de cada *endpoint*, tais como nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede cabeada e WiFi, detalhes do hardware como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão de agente está em uso em um respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA;

4.195.38. O *proxy* de acesso deve atuar como *proxy reverso* para aplicações baseadas em HTTP, HTTPS, RDP, SMB, CIFS, SSH, SMTP, SMTPS, IMAP, IMAPS, POP3 e POP3S;

4.195.39. Para aplicações HTTP e HTTPS deve ser possível realizar um balanceamento de carga entre os servidores cadastrados usando algoritmos como round robin, por peso, baseado no host field do cabeçalho HTTP ou baseado em disponibilidade do servidor;

4.195.40. Para regras de encaminhamento de tráfego TCP, deve ser possível vincular o servidor com um FQDN visando ofuscar o endereço IP privado do servidor. Deste modo, o agente deve manipular o host file do endpoint visando criar entradas DNS;

4.195.41. Deve ser possível definir um pool de IPs no proxy de acesso como IPs de origem para comunicação interna com as aplicações privadas;
12.42. A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa;

4.195.42. Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas;

4.195.43. As regras de conformidade devem gerar tags que são sincronizadas entre os elementos da solução de ZTNA visando controlar a postura de um determinado endpoint diretamente no proxy de acesso;

4.195.44. A postura deve ser monitorada continuamente para que, caso ocorra uma alteração, o proxy de acesso termine e passe a bloquear a conexão em desacordo com as regras de compliance definidas;

4.195.45. Deve ser possível construir tags com verificações no endpoint, as quais podem variar de acordo com o suporte ao sistema operacional, tais como se o endpoint está logado no domínio, versão do sistema operacional, chave de registro, processo, nível de vulnerabilidade, CVEs, arquivos existentes em um caminho específico e até mesmo se o antivírus está instalado e sendo executado, além de ser possível validar se as assinaturas estão atualizadas;

4.195.46. A console central deve permitir exportar e importar tags entre sistemas diferentes por meio de um arquivo JSON;

4.195.47. Deve ser possível verificar quais endpoints estão associadas com cada tag;

4.195.48. Deve ser possível criar regras no proxy de acesso determinando se um dispositivo necessita estar de acordo com uma ou mais de uma tag simultaneamente, caso a política possua vínculo com diversas tags;

4.195.49. Deve ser possível criar regras no proxy de acesso vinculando interface de origem, IP de origem, IP de destino, servidor ZTNA, tag ZTNA, grupo de usuários ou usuário;

4.195.50. Para validação da autenticação dos usuários em conjunto com as regras de proxy de acesso, a solução deve suportar SAML, LDAP, Radius ou base de dados local;

4.195.51. Deve possibilitar definir funções administrativas relacionadas às permissões dos endpoints, de políticas e de configurações gerais;

4.195.52. Deve possibilitar aos usuários definirem suas identidades mediante inserção manual, vínculo com LinkedIn, Google ou Salesforce, podendo ainda notificá-los para que esse vínculo possa ser realizado;

4.195.53. A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de endpoint, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional;

4.195.54. Deverá ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows;

4.195.55. Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda diretamente no agente;

4.195.56. Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos;

4.195.57. Caso não seja possível aplicar um patch automático para corrigir uma vulnerabilidade, requerendo assim um patch manual, deve ser possível excluir essa aplicação da verificação de *compliance*;

4.195.58. Deve ser possível excluir determinadas aplicações da verificação de *compliance* e até mesmo desabilitar o patch automático;

4.195.59. O agente deve dispor de um sistema de notificação do tipo *popup* visando alertar o usuário;

4.195.60. Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas, severidade, bem como o CVE correspondente;

4.195.61. Deve suportar a criação de várias versões de pacotes de instalação;

4.195.62. As vulnerabilidades encontradas devem ser exibidas diretamente no agente com um link para análise de mais detalhes, englobando nome da vulnerabilidade, severidade, produtos afetados, CVE IDs, descrição, informação do fabricante do software e, quando disponível, link para download do patch no site público do fabricante do software;

4.195.63. Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas, bem como disponibilizar ainda a possibilidade de aplicar a remediação imediatamente;

4.195.64. Deve possuir módulo para execução de filtro web a nível de endpoint mediante uso do agente local, realizando a filtragem diretamente no endpoint, podendo ainda ser possível bloquear, permitir, alertar ou monitorar o tráfego web com base na categoria de URL ou filtro de URL customizado;

4.195.65. O agente deve realizar consultas online ao centro de inteligência do próprio fabricante para determinar a categoria de uma determinada URL visando aplicar o controle de acesso à Internet;

4.195.66. Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as opções de permitir, bloquear ou monitorar;

4.195.67. O agente para Windows deve permitir inspeção de tráfego HTTPS mediante instalação de plugin disponibilizado pelo mesmo fabricante do agente, o qual deve ser compatível com Google Chrome, Mozilla Firefox e Microsoft Edge;

4.195.68. Deve ser possível verificar as violações de filtro web diretamente no agente, especificando ainda a URL, categoria, quando a violação ocorreu e usuário;

4.195.69. Deve ser possível determinar quando o filtro web entrará em ação no agente, se o mesmo deverá estar sempre ativo ou somente quando o usuário estiver fora da rede corporativa;

4.195.70. Deve ser possível configurar o proxy de acesso para atuar como CASB (Cloud Access Security Broker) em linha, inline do inglês, visando controlar o acesso a aplicações SaaS;

4.195.71. O proxy de acesso deve manter uma base de aplicações dinâmica, a qual deve ser compartilhada pelo centro de inteligência do fabricante da solução;

4.196. **Centralizador de Logs e Relatórios para os equipamentos NGFW**

4.196.1. A solução deve ser baseada em máquina virtual ou appliance físico do mesmo fabricante da solução de NGFW, e ter como objetivo a centralização de logs e geração de relatórios para a solução;

4.196.2. Poderá ser entregue em formato de appliance físico ou appliance virtual;

4.196.3. Deverá estar devidamente licenciada para:

4.196.4. Suportar a coleta de, no mínimo, 100 GB de logs diários;

4.196.5. Caso a solução seja entregue como appliance virtual, este deve suportar:

4.196.6. Deve ser compatível com os hypervisor VMWare 6.5 e superiores, Hyper-V 2016 e superiores, e KVM;

4.196.7. Não deverá existir limite para o número de vCPUs no appliance virtual;

4.196.8. Não deverá existir limite para a expansão da memória RAM no appliance virtual;

4.196.9. Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;

4.196.10. Caso a solução seja entregue como appliance físico, este deve suportar:

4.196.11. Pelo menos duas interfaces 1GE padrão RJ45;

4.196.12. Suportar a configuração de RAID 0 e 1 para os discos internos;

4.196.13. Possuir fonte de alimentação interna, redundante e hot-swap;

4.196.14. 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;
13.6. Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito;

4.196.15. Realizar agregação via pontuação, para geração de um veredito sobre máquinas comprometidas na rede e atividades suspeitas;

4.196.16. Utilizar técnicas de *machine learning* para a captura de índices de comprometimento, através de URLs, domínios e endereços IPs maliciosos;

4.196.17. Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes etc.;

4.196.18. Deve suporta a visualização de logs e geração de relatórios;

4.196.19. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

4.196.20. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

4.196.21. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

4.196.22. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

4.196.23. Deve possuir mecanismos de remoção automática para logs antigos;

4.196.24. Permitir importação e exportação de relatórios

4.196.25. Deve ter a capacidade de criar relatórios no formato HTML, PDF, XML e CSV;

4.196.26. Deve permitir exportar os logs no formato CSV;

4.196.27. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

4.196.28. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor *Syslog* externo ou similar;

4.196.29. A solução deve ter relatórios predefinidos;

4.196.30. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

4.196.31. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

4.196.32. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

4.196.33. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

4.196.34. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

4.196.35. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

4.196.36. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

4.196.37. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

4.196.38. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

4.196.39. Permitir o envio por e-mail relatórios automaticamente;

4.196.40. Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;

4.196.41. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

4.196.42. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

4.196.43. Deve permitir o uso de filtros nos relatórios;

4.196.44. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

4.196.45. Permitir especificar o idioma dos relatórios criados;

4.196.46. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

4.196.47. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

4.196.48. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

4.196.49. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

4.196.50. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

4.196.51. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

4.196.52. Deve permitir visualizar em tempo real os logs recebidos;

4.196.53. Deve permitir o encaminhamento de log no formato syslog;

4.196.54. Deve permitir o encaminhamento de log no formato CEF (Common Event Format);

4.196.55. Deve permitir gerar alertas de eventos a partir de logs recebidos;

4.196.56. Deve suportar o serviço de Indicadores de Compromisso (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredito (classificação geral da ameaça), o número de ameaças detectadas;

4.196.57. Deve ser capaz de visualizar alertas de surtos e baixar automaticamente manipuladores de eventos e relatórios relacionados;

4.196.58. Deve permitir o time de resposta a incidentes identificar se um artefato malicioso de "Zero Day" encontrado na rede faz parte de alguma campanha específica de malware, se foi visto até o momento somente na rede da instituição;

4.196.59. Caso o *malware* faça parte de alguma campanha, deve ser detalhado qual o objetivo dela, tipos de indústria que já foram alvo do malware, comportamento malicioso conhecido sobre o *malware* e quais são os autores;

4.196.60. A solução deve possuir garantia, suporte e atualizações ao *software* durante a vigência do contrato;

4.197. **b) de projeto e de implementação, que estabelecem o processo de desenvolvimento de software, técnicas, métodos, forma de gestão, de documentação, dentre outros;**

4.198. A CONTRATADA deverá elaborar e apresentar, em até 10 (dez) dias corridos, contados da data de assinatura do contrato, um Projeto de Implementação da Solução;

4.199. O projeto deverá conter minimamente:

4.199.1. Identificação e descrição de todas as atividades necessárias para a implantação dos equipamentos e serviços contratados, incluindo eventuais atividades para preparação da infraestrutura pelo Confea;

4.199.2. Identificação dos responsáveis por cada atividade;

4.199.3. Duração de cada atividade, que deverá ser estabelecida em dias e deverá considerar as restrições de horário estabelecidas pelo Confea em reunião preliminar;

4.199.4. Cronograma com o sequenciamento das atividades e suas dependências;

4.199.5. Mecanismo de Acompanhamento e Avaliação: A CONTRATADA deve fornecer relatórios semanais de progresso, incluindo atualizações de status de cada atividade, principais realizações, próximos passos e possíveis problemas ou riscos;

4.199.6. Estratégia de Backup: A CONTRATADA deverá elaborar e implementar uma estratégia de *backup* robusta para garantir a recuperação de dados em caso de falha do sistema;

4.199.7. Plano de Comunicação: A CONTRATADA deve estabelecer um plano de comunicação que indique os principais pontos de contato para a comunicação do projeto, a frequência das atualizações e o método de comunicação (por exemplo, e-mail, reuniões de status);

4.199.8. O impacto de cada atividade na operação dos demais serviços de TI do Confea, como, por exemplo, se a atividade em questão gera indisponibilidade ou traz riscos aos demais serviços, precisando por isso ser agendada para horários não comerciais;

4.199.9. Aceitação e *Sign-off*: Após a conclusão de cada fase do projeto, a CONTRATADA deverá fornecer um relatório detalhado para o Confea para revisão. Após a revisão e aprovação do Confea, o *sign-off* será fornecido para a fase concluída;

4.199.10. O Projeto de Implementação deverá contemplar e detalhar todos os serviços de instalação, configuração e treinamento previstos, bem como estabelecer procedimentos de testes de conexão e desempenho da Solução, para cada etapa de instalação e configuração concluída;

4.199.11. Caso o Confea esteja de acordo com o plano submetido pela CONTRATADA, definirá a data de início da implementação e convocará a CONTRATADA para iniciar a implementação.

4.200. **c) de implantação, que definem o processo de disponibilização da solução em ambiente de produção, dentre outros;**

4.200.1. Preparação da Infraestrutura: A CONTRATADA deve garantir que a infraestrutura existente seja adequada para a implantação da nova solução. Isso pode incluir verificações de compatibilidade de hardware e software, avaliações de segurança e preparação de qualquer equipamento necessário.

4.200.2. Migração de Dados e Configurações: Caso haja um sistema antigo em uso, a CONTRATADA deve fornecer suporte na migração segura de todas as configurações e dados relevantes para a nova solução. Isso deve ser feito de forma a minimizar o tempo de inatividade e garantir que nenhum dado seja perdido ou comprometido.

4.200.3. Testes de Implantação: Após a instalação e configuração da nova solução, a CONTRATADA deve realizar uma série de testes para garantir que tudo esteja funcionando conforme esperado. Isso deve incluir testes de conectividade, desempenho, segurança e funcionalidade.

4.200.4. Treinamento de Pessoal: A CONTRATADA deve fornecer treinamento adequado ao pessoal do Confea em como operar e gerenciar a nova solução. Este treinamento deve incluir instruções sobre como solucionar problemas comuns e como manter o sistema atualizado e seguro.

4.200.5. Plano de Retorno (Rollback): Em caso de problemas graves durante a implantação que possam afetar negativamente as operações do Confea, um plano de retorno deve estar pronto para reverter as mudanças e restaurar o sistema ao seu estado anterior, minimizando assim as perturbações.

4.200.6. Suporte Pós-Implantação: Após a conclusão bem-sucedida da implantação, a CONTRATADA deve fornecer um período de suporte dedicado durante o qual o Confea pode levantar quaisquer questões ou problemas encontrados. A CONTRATADA deve então trabalhar para resolver esses problemas em um tempo de resposta acordado.

4.201. **d) de garantia e manutenção, que definem a forma como será conduzida a manutenção, acionamento da garantia e a comunicação entre as partes envolvidas;**

4.202. Garantia: Todos os componentes da solução devem ter uma garantia de 36 (trinta e seis) meses, a contar da data de aceitação do produto. Esta garantia deve cobrir todos os defeitos de fabricação e problemas de desempenho. Além disso, o prazo de garantia poderá ser renovado conforme a lei, se necessário.

4.202.1. Acionamento da Garantia: O acionamento da garantia deve ser simples e sem complicações. A CONTRATADA deve fornecer um processo claro e eficiente para o acionamento da garantia, que deve incluir um ponto de contato dedicado para questões relacionadas à garantia.

4.202.2. Manutenção: A CONTRATADA deve oferecer serviços de manutenção preventiva, corretiva, adaptativa e evolutiva (melhoria funcional). A manutenção preventiva deve incluir verificações regulares de desempenho e atualizações de software, quando disponíveis. A manutenção corretiva deve ser realizada em caso de falhas ou defeitos.

4.202.3. Tempo de Resposta para Manutenção: Em caso de falha ou defeito, a CONTRATADA deve iniciar ações corretivas de acordo com os Níveis Mínimos de Serviço.

4.202.4. Comunicação: Deve haver uma comunicação clara e eficaz entre o Confea e a CONTRATADA. A CONTRATADA deve fornecer atualizações regulares sobre o status da garantia e dos serviços de manutenção e estar disponível para responder a quaisquer perguntas ou preocupações.

4.202.5. Relatórios de Manutenção: A CONTRATADA deve fornecer relatórios de manutenção regulares, detalhando todas as atividades de manutenção realizadas, os problemas encontrados e as ações tomadas para resolver esses problemas.

4.202.6. Formação: A CONTRATADA deve fornecer formação adequada ao pessoal do Confea em como acionar a garantia e solicitar serviços de manutenção, para garantir uma operação eficiente e eficaz da solução.

4.203. **e) de capacitação, que definem o ambiente tecnológico dos treinamentos a serem ministrados, os perfis dos instrutores, dentre outros;**

4.204. Conforme Item b1).

4.205. **f) de experiência profissional da equipe que executará os serviços relacionados à solução de TIC, que definem a natureza da experiência profissional exigida e as respectivas formas de comprovação dessa experiência, dentre outros;**

4.206. A equipe de implantação da CONTRATADA deve apresentar um histórico comprovado de profissionalismo e competência técnica na instalação, configuração e suporte de soluções de Tecnologia da Informação e Comunicação (TIC), especificamente com relação a sistemas de firewall e segurança da rede.

4.206.1. Os requisitos específicos incluem:

4.206.2. Certificação: Todos os membros da equipe técnica envolvidos no projeto devem possuir certificações relevantes das organizações ou fabricantes de tecnologia pertinentes ao projeto. Essas certificações podem incluir, mas não estão limitadas a, Cisco Certified Network Professional (CCNP) Security, Certified Information Systems Security Professional (CISSP), CompTIA Security+, entre outros.

4.206.3. Experiência: A equipe deve ter experiência comprovada na implantação e manutenção de soluções de segurança de rede, incluindo firewalls, sistemas de detecção de intrusões, VPNs, entre outros. A CONTRATADA deve fornecer um portfólio de projetos anteriores, incluindo referências de clientes anteriores.

4.206.4. Formação: Os profissionais envolvidos devem possuir diplomas em campos relevantes, como Ciência da Computação, Engenharia da Computação, Sistemas de Informação ou campos relacionados.

4.206.5. Habilidades Específicas: A equipe deve demonstrar proficiência em aspectos-chave da implantação, incluindo configuração e solução de problemas de firewalls, implementação de políticas de segurança, gestão de projetos de TI e serviços de suporte pós-implantação.

4.206.6. As formas de comprovação de experiência profissional incluem, mas não se limitam a, apresentação de certificados, portfólio de projetos, referências de clientes anteriores e descrições detalhadas de projetos anteriores realizados pela equipe.

4.207. **g) de formação da equipe que projetará, implementará e implantará a solução de TIC, que definem cursos acadêmicos e técnicos, formas de comprovação dessa formação, dentre outros;**

4.208. Conforme Item f).

4.209. **h) de metodologia de trabalho;**

4.210. Os requisitos de metodologia de trabalho se referem à abordagem sistemática que a CONTRATADA deve empregar durante a execução do projeto. A metodologia escolhida pode variar, mas deve ser adequada para o tipo de trabalho que está sendo feito e deve assegurar uma execução eficiente e eficaz do projeto. Descrição dos requisitos:

4.210.1. Abordagem Metodológica: A CONTRATADA deve adotar uma metodologia de trabalho claramente definida e comprovada para a implantação da solução de TIC. Isso pode incluir, por exemplo, metodologias ágeis, DevOps, ITIL, PMBOK ou uma combinação dessas, conforme seja mais adequado ao contexto do projeto.

4.210.2. Planejamento e Execução do Projeto: A CONTRATADA deve apresentar um plano de projeto detalhado que descreva as etapas, atividades, recursos necessários, prazos e marcos do projeto. Este plano deve estar alinhado com a metodologia de trabalho adotada.

4.210.3. Gestão de Riscos: A CONTRATADA deve demonstrar uma abordagem robusta para a identificação, análise e mitigação de riscos do projeto. Isso deve incluir a preparação de um plano de gestão de riscos e a implementação de controles de mitigação de riscos adequados.

4.210.4. Gestão de Mudanças: Dada a natureza dinâmica dos projetos de TIC, a CONTRATADA deve dispor de um processo eficaz de gestão de mudanças que permita lidar com alterações nos requisitos, prazos, recursos e outros aspectos do projeto de maneira controlada e estruturada.

4.210.5. Comunicação e Reporte: A CONTRATADA deve fornecer atualizações regulares sobre o progresso do projeto, incluindo relatórios de status, revisões de marcos e reuniões de atualização. O formato, a frequência e o conteúdo dessas comunicações devem ser acordados com o Confea.

4.210.6. Qualidade e Controle: A CONTRATADA deve aplicar procedimentos de garantia e controle de qualidade durante todo o ciclo de vida do projeto, para garantir que o trabalho esteja de acordo com os padrões de qualidade definidos e que os resultados finais atendam aos requisitos especificados.

4.210.7. Os detalhes da metodologia de trabalho devem ser apresentados em forma de documentos como: plano de projeto, plano de gestão de riscos, plano de comunicação, plano de qualidade, entre outros.

4.211. **i) de segurança da informação e privacidade;**

4.211.1. Conforme Item f1).

5. **BEM E/OU SERVIÇO COMUM**

5.1. (X) Sim**.**

5.2. O serviço que se pretende contratar é considerado comum, pois a especificação do objeto estabelece padrões objetivos de desempenho e qualidade, capaz de ser atendida por vários fornecedores, já que reconhecidas e usuais no mercado, consoante disciplina o art. 1º, parágrafo único, da Lei nº 10.520, de 2002, o art. 9º, § 2º, do Decreto nº 7.174, de 2010 e o art. 3º, II, do Decreto nº 10.024, de 2019.

6. **CARACTERIZAÇÃO DO OBJETO**

6.1. **Serviço continuado:** (X) Sim.

6.2. Entende-se que o serviço em questão é de natureza continuada pois é **essencial** à manutenção dos serviços deste Federal conforme disposto nas justificativas do Estudo Técnico e Preliminar da Contratação - ETP e do Termo de Referência - TR.

6.3. Não obstante, observa-se que a essencialidade atrela-se à necessidade de existência e manutenção do contrato, pelo fato de eventual paralisação da atividade contratada implicar em prejuízo à segurança ao exercício das atividades da Administração contratante, podendo trazer prejuízos não mensuráveis ao Confea.

6.4. Nesse sentido, é apresentada a definição no Anexo I da **Instrução Normativa nº 2/2008** da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão:

6.5. "*I – SERVIÇOS CONTINUADOS são aqueles cuja interrupção possa comprometer a continuidade das atividades da Administração e cuja necessidade de contratação deva estender-se por mais de um exercício financeiro e continuamente*".

6.6. Segue o mesmo raciocínio o conceito atribuído pelo Tribunal de Contas da União:

6.7. "Voto do Ministro Relator

6.8. […] 29. Na realidade, o que caracteriza o caráter contínuo de um determinado serviço é sua **essencialidade para assegurar a integridade do patrimônio público de forma rotineira e permanente ou para manter o funcionamento das atividades finalísticas do ente administrativo, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional**." (TCU. Acórdão n° 132/2008 – Segunda Câmara. Relator: Ministro Aroldo Cedraz. Data do julgamento: 12/02/2008.)"

6.9. A digitalização dos sistemas, atividades e processos administrativos tornou-se uma realidade incontornável no cenário atual, abrindo caminho para uma série de inovações, eficiências e potenciais de alcance global. No entanto, junto com as vantagens inerentes à digitalização, surgem também ameaças cibernéticas, que têm a capacidade de comprometer informações vitais, sistemas essenciais e até mesmo a integridade da infraestrutura organizacional.

6.10. Dentro desse panorama, o Confea, ao manter e expandir suas atividades digitalmente, inevitavelmente se expõe a tais ameaças. Por isso, torna-se imperativo garantir uma infraestrutura segura e resiliente que possa combater ameaças cibernéticas, evitando interrupções nas operações e protegendo dados e informações valiosas.

6.11. Contratar uma empresa especializada em serviços integrados de segurança cibernética é, portanto, não apenas uma questão de precaução, mas uma necessidade iminente. Um sistema de proteção de perímetro robusto e avançado, como um *firewall* de ponta, não somente serve como barreira contra invasões e tentativas maliciosas de acesso, mas também garante a continuidade dos serviços, prevenindo interrupções inesperadas e possíveis consequências catastróficas.

6.12. Quando se considera a natureza contínua do serviço, é crucial que o Confea tenha à sua disposição um sistema que esteja constantemente atualizado, para que possa enfrentar ameaças emergentes e técnicas de invasão em constante evolução. A provisão de hardware (appliance), licença de uso e atualizações de versões por um período de 36 meses garante essa atualização contínua, dando ao Confea a paz de espírito de que seu ambiente digital está protegido com as mais recentes soluções de segurança cibernética.

6.13. Em suma, a contratação de uma empresa especializada e a implementação de uma solução de firewall são cruciais para assegurar a continuidade, integridade e resiliência das operações digitais do Confea, alinhando-se perfeitamente à necessidade de manter os serviços sem interrupção, conforme definido pelo Anexo I da Instrução Normativa nº 2/2008 e pelo entendimento do TCU.

6.14. Pelo exposto, entende-se a necessidade da continuidade do serviço.

6.15. Ademais, como o serviço é de natureza continuada, verifica-se vantajosidade no aumento do prazo de vigência, tendo em vista que o fornecedor, sabendo de antemão a duração do contrato, pode praticar um preço melhor, o que traria economicidade ao Confea.

6.16. Considerando ainda o quadro exíguo da GTI, o número de atividades técnicas desenvolvidas e o número de Contratos de Fiscalização, é prudente que tenhamos contratos continuados de duração mais longa para evitar a necessidade de alocação praticamente contínua de um Analista para o trato processual constante de um único processo, o que ensejaria possíveis horas extras, redefinições de prioridades na unidade e perda da qualidade do fiel cumprimento das obrigações funcionais.

7. FORMA DE CONTRATAÇÃO (MODALIDADE LICITATÓRIA)

7.1. Pregão Eletrônico Tradicional.

8. CRITÉRIO DE JULGAMENTO / ESCOLHA DO LICITANTE

8.1. Menor preço global.

9. REGIME DE EXECUÇÃO

9.1. Empreitada por preço global.

10. FORMALIZAÇÃO DA CONTRATAÇÃO

10.1. Termo de Contrato

11. VALOR ESTIMADO PARA CONTRATAÇÃO

11.1. O valor global para a contratação é de **R$ 3.384.624,43** (três milhões, trezentos e oitenta e quatro mil seiscentos e vinte e quatro reais e quarenta e três centavos) para o período de 36 (trinta e seis) meses, conforme pesquisa de preço realizada pela unidade demandante demonstrada no quadro abaixo e conforme a tabela global de preços.

Pesquisa de Preços para Aquisição de Bens e Contratação de Serviços em Geral										
Item	**Descrição**	**Quantidade**	**Empresa 01 (doc. 0803295)**		**Empresa 02 (doc. 0803298)**		**Empresa 03 (doc. 0803300)**		**Valor Final Médio**	
			Valor Unitário	**Valor Total**	**Valor Unitário**	**Valor Total**	**Valor Unitário**	**Valor Total**	**Valor Unitário**	**Valor Total**
1	*Appliance* com capacidade para suportar um *throughput*	2	R$ 772.000,00	R$ 1.544.000,00	R$ 759.000,00	R$ 1.518.000,00	R$ 785.404,84	R$ 1.570.809,68	R$ 772.134,95	R$ 1.544.269,89

Pesquisa de Preços para Aquisição de Bens e Contratação de Serviços em Geral										
Item	**Descrição**	**Quantidade**	**Empresa 01 (doc. 0803295)**		**Empresa 02 (doc. 0803298)**		**Empresa 03 (doc. 0803300)**		**Valor Final Médio**	
			Valor Unitário	**Valor Total**	**Valor Unitário**	**Valor Total**	**Valor Unitário**	**Valor Total**	**Valor Unitário**	**Valor Total**
	mínimo de 12 Gb/s.									
2	Licença de uso de *software* a ser utilizada no equipamento do Item 01, incluindo garantia, atualização de versões e suporte técnico por 36 meses.	2	R$ 828.000,00	R$ 1.656.000,00	R$ 841.000,00	R$ 1.682.000,00	R$ 843.928,71	R$ 1.687.857,42	R$ 837.642,90	R$ 1.675.285,81
3	Solução de Zero Trust Network Access (ZTNA) com capacidade para suportar 500 usuários.	500	R$ 240,00	R$ 120.000,00	R$ 230,00	R$ 115.000,00	R$ 236,35	R$ 118.175,00	R$ 235,45	R$ 117.725,00
4	Treinamento da Solução Ofertada.	3	R$ 16.500,00	R$ 49.500,00	R$ 15.000,00	R$ 45.000,00	R$ 15.843,73	R$ 47.531,19	R$ 15.781,24	R$ 47.343,73

Pesquisa de Preços para Aquisição de Bens e Contratação de Serviços em Geral										
Item	Descrição	Quantidade	Empresa 01 (doc. 0803295)		Empresa 02 (doc. 0803298)		Empresa 03 (doc. 0803300)		Valor Final Médio	
			Valor Unitário	Valor Total	Valor Unitário	Valor Total	Valor Unitário	Valor Total	Valor Unitário	Valor Total
Total			R$ 1.616.740,00	R$ 3.369.500,00	R$ 1.615.230,00	R$ 3.360.000,00	R$ 1.645.413,63	R$ 3.424.373,29	R$ 1.625.794,54	R$ 3.384.624,43

Metodologia para obtenção do prelo de referência para contratação - Art. 6º da IN nº 73, de 5 de agosto de 2020		
PREÇO MÉDIO	PREÇO MEDIANO	PREÇO MÍNIMO
R$ 3.384.624,43	R$ 3.369.500,00	R$ 3.360.000,00

11.2. Ademais, registra-se que não houve gastos com bens e serviços da mesma natureza que se pretende contratar mediante a modalidade que será adotada para o presente exercício.

12. **DOTAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO**

12.1. A despesa orçamentária para a contratação do objeto deste instrumento correrá ao Centro de Custo nº 9.03.09.04 - SUINF - Atividades de Tecnologia da Informação.

12.2. Informa-se que não houve aquisições/contratações do objeto pretendido no exercício.

12.3. Ademais, consoante Instrução Normativa nº 94, de 23 de dezembro de 2022, que dispõe "Art. 21. A adequação orçamentária e o cronograma físico-financeiro serão elaborados pelos Integrantes Requisitante e Técnico, contendo: [...] II - cronograma de execução física e financeira, contendo o detalhamento das etapas ou fases da solução a ser contratada, com os principais serviços ou bens que a compõem, e a previsão de desembolso para cada uma delas", registra-se abaixo o cronograma de execução físico-financeiro com a previsão de desembolso em 2023.

LOTE ÚNICO

ITENS	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO R$	VALOR TOTAL R$
1	Appliance com capacidade para suportar um *throughput* mínimo de 12 Gb/s.	2	R$ 772.134,95	R$ 1.544.269,89
2	Licença de uso de *software* a ser utilizada no equipamento do Item 01, incluindo garantia, atualização de versões e suporte técnico por 36 meses.	2	R$ 837.642,90	R$ 1.675.285,81
3	Solução de Zero Trust Network Access (ZTNA) com capacidade para suportar 500 usuários.	500	R$ 235,45	R$ 117.725,00
4	Treinamento da Solução Ofertada.	3	R$ 15.781,24	R$ 47.343,73
VALOR TOTAL				R$ 3.384.624,43

13. **LOCAL PARA EXECUÇÃO DOS SERVIÇOS E/OU ENTREGA DOS PRODUTOS**

13.1. Os produtos/serviços deverão ser entregues/executados na sede do Confea, localizado no SEPN 508, Bloco A, Edifício Engenheiro Francisco Saturnino de Brito Filho, Asa Norte, Brasília – DF.

13.2. O deslocamento de prestador de serviço da CONTRATADA para o Confea não implicará, de nenhuma forma, o acréscimo ou majoração nos valores dos serviços, bem como nenhum tipo de pagamento correspondente a deslocamentos, diárias, horas-extras ou adicionais noturnos.

13.3. A definição do horário de trabalho para a execução das atividades nas instalações do Confea deve ser acordada entre o Confea e a Contratada.

13.4. Como padrão e quando não especificado em contrário, considerar-se-á como dia útil o período de 10 horas úteis, das 8h às 18h, de segunda a sexta-feira, nos dias em que houver expediente no Confea.

13.4.1. Considerar-se-á hora útil o intervalo de uma hora dentro de um dia útil.

13.5. Os serviços eventualmente realizados fora do horário de expediente, aos sábados, domingos e feriados, sejam no ambiente da CONTRATADA ou no ambiente do Confea, não implicarão nenhum acréscimo ou majoração nos valores pagos à CONTRATADA.

14. **CRONOGRAMA DE EXECUÇÃO**

14.1. O cronograma de execução será elaborado e aprovado pela Contratante, podendo, após assinatura do contrato, sofrer alterações conforme os prazos estabelecidos.

14.2. O cronograma de execução será executado conforme os prazos estabelecidos entre a contratada e o Confea.

14.3. As datas poderão sofrer alterações em comum acordo entre o Contratante e a Contratada, desde que não prejudiquem o andamento e a entrega dos serviços no prazo estabelecido.

14.4. O atraso no cumprimento das etapas do cronograma ensejará multa conforme estabelecerá o edital de licitação relacionado ao Termo de Referência.

14.5. Etapa 1: Assinatura do Contrato

14.6. Quando ocorre: Dia 1

14.7. Prazos Estimados: Início - Dia 1

14.8. Etapa 2: Portaria de Fiscalização

14.9. Quando ocorre: No mínimo 7 dias corridos após a assinatura do contrato

14.10. Prazos Estimados: Início - Dia 1 + 7 dias corridos

14.11. Etapa 3: Emissão da Nota de Empenho

14.12. Quando ocorre: 5 dias corridos após a assinatura do contrato

14.13. Prazos Estimados: Início - Dia 1 + 5 dias corridos

14.14. Etapa 4: Reunião de *Kick-off*

14.15. Quando ocorre: Depende da disponibilidade das partes, mas idealmente dentro de 14 dias corridos após a assinatura do contrato

14.16. Prazos Estimados: Início - Dia 1 + 14 dias corridos

14.17. Etapa 5: Emissão da Ordem de Serviço

14.18. Quando ocorre: Após a reunião de Kick-off e a emissão da Nota de Empenho

14.19. Prazos Estimados: Início - Dia 1 + 19 dias corridos

14.20. Etapa 6: Implementação da Solução de Firewall

14.21. Quando ocorre: Dentro de 10 dias corridos a partir da emissão da Ordem de Serviço pelo Confea

14.22. Prazos Estimados: Início - Dia 1 + 29 dias corridos, Fim - Dia 1 + 89 dias corridos

14.23. Etapa 7: Conclusão da Implementação

14.24. Quando ocorre: A solução de *firewall* deve estar totalmente operacional e integrada ao ambiente de TI do Confea dentro de 90 dias a partir da data de emissão da Ordem de Serviço.

14.25. Prazos Estimados: Início - Dia 1 + 90 dias corridos

14.26. Etapa 8: Início do Período de Suporte e Manutenção Contínuos

14.27. Quando ocorre: Imediatamente após a Conclusão da Implementação

14.28. Prazos Estimados: Início - Dia 1 + 91 dias, Fim - Dia 1 + 1086 dias (36 meses)

14.29. Essas datas são estimativas e podem variar dependendo de vários fatores, incluindo a disponibilidade dos recursos necessários e as circunstâncias imprevistas que podem surgir durante a execução do contrato.

15. PRAZO DE VIGÊNCIA E EXECUÇÃO

15.1. A vigência e execução do contrato será de 36 (trinta e seis) meses contados da data da assinatura do contrato, podendo ser prorrogado nos moldes da legislação vigente.

15.2. Quanto ao prazo de vigência ser de 36 (trinta e seis) meses, esclarece-se que o período idealizado contribuirá para uma contratação mais atrativa pelo Sistema Confea/Crea, pois poderá proporcionar maior economicidade aos cofres públicos, visto prazos mais duradouros serem economicamente mais vantajosos do que prazos mais curtos, bem como competitividade ao certame licitatório, por possibilitar a participação de um número maior de interessados capazes de atender e fornecer o objeto pretendido neste certame, possibilitando que a melhor oferta seja declarada vencedora.

15.3. Além das dificuldades em se elaborar novos certames licitatórios a cada 12 meses, caso assim o fosse, existe a possibilidade de que a solução em uso seja descontinuada caso outra fornecedora vença a disputa, ocasionando na disponibilização de nova solução, nova curva de aprendizagem, maiores custos financeiros e de tempo despendido por todas as partes envolvidas. Dessa forma, caso a solução seja paralisada, ou até mesmo não se consiga licitar a tempo em prazo inferior, acarretará riscos ao Confea.

15.4. Ainda, a redução do prazo se mostra temerária e contrária ao interesse público, pois constantes alterações do cenário levam, consequentemente, a readequações por todas as parte interessadas, e a custos desnecessários, pois todos os procedimentos processuais envolvem várias unidades/setores para a sua completa execução.

15.5. Por fim, conclui-se que o prazo de 36 (trinta e seis) meses tornará o certame licitatório mais competitivo, gerando maior economicidade aos cofres públicos, tanto pela contratação da solução quanto pela atuação do corpo técnico em novos processos, mitigando os riscos de descontinuidade da solução e mantendo-se os conhecimentos adquiridos, justificando-se a vantajosidade para o interesse público.

16. CRITÉRIOS TÉCNICOS PARA SELEÇÃO DO FORNECEDOR

16.1. (X) Atestado de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, que comprove ter a licitante prestado serviço da mesma natureza e compatível com objeto pretendido.

16.2. (X) Comprovação experiência mínima na execução de serviços semelhantes ao objeto da licitação.

16.3. Por serviços de mesma natureza e compatível com objeto entende-se: fornecimento, instalação, configuração e suporte de Firewall NGFW, Proxy ou ZTNA.

16.4. O fornecimento de atestado contendo APENAS a solução de ZTNA não é critério de aceitabilidade. No entanto, serão aceitos atestados que incluam somente ZTNA combinado com Proxy e/ou NGFW.

16.5. (X) Declaração de que na data prevista para assinatura do contrato possuirá profissional devidamente e tecnicamente habilitado para responsabilizar-se pela execução de serviços de características semelhantes aos licitados.

16.6. (X) Planilha Ponto-a-Ponto das Especificações Técnicas Requeridas e correlação com o Manual/Site do Fabricante:

16.6.1. A conferência será realizada de forma detalhada, item por item, entre a aquisição pretendida e o fornecido pela licitante vencedora, alinhando-se estritamente com as especificações técnicas delineadas neste Edital e seus anexos.

16.6.2. Para facilitar e otimizar o processo de conferência, solicitamos que a empresa vencedora prepare um documento Excel, organizado da seguinte maneira:

16.6.3. Coluna 1 "Item": Listar cada item individualmente de acordo com as especificações técnicas mencionadas no Edital e seus anexos;

16.6.4. Coluna 2 "Descrição do Item": Providenciar uma breve descrição de cada item, com foco em como se alinha com as especificações exigidas;

16.6.5. Coluna 3 "Referência no Manual do Fornecedor": Indicar a página ou seção específica do manual do fornecedor onde se demonstra a capacidade da empresa vencedora de fornecer o item em questão, de acordo com as especificações requeridas.

16.6.6. Este formato de documento proporcionará uma revisão eficiente e eficaz da compatibilidade entre os itens pretendidos para aquisição e o que é oferecido pela licitante vencedora. Além disso, permite uma fácil referência às seções relevantes do manual do fornecedor para futuras consultas ou esclarecimentos adicionais.

17. VISTORIA OU VISITA TÉCNICA

17.1. A licitante poderá, a seu critério, realizar vistoria técnica facultativa nas instalações do Confea, com o objetivo de conhecer o ambiente e sanar possíveis dúvidas sobre a execução do objeto.

17.2. Caso opte por realizar a vistoria técnica, a licitante deverá agendar com antecedência mínima de 2 (dois) dias úteis, por meio do e-mail gti@confea.org.br, indicando nome dos profissionais que farão a visita, bem como a data e o horário previstos.

17.3. A vistoria técnica deverá ser realizada de segunda a sexta-feira, em dias úteis, no horário das 10h às 17h.

17.4. A não realização de vistoria técnica pela licitante não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a CONTRATADA assumir os ônus dos serviços decorrentes.

17.5. O Confea não se responsabilizará por despesas da licitante relativas à vistoria técnica facultativa.

18. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

18.1. O agrupamento dos itens do objeto do presente instrumento em lote tem por objetivo a padronização da contratação uma vez que os itens agrupados possuem a mesma natureza técnica, o que resulta ainda na otimização de recursos humanos e financeiros no desenvolvimento das atividades relacionadas à gestão contratual, uma vez que o gerenciamento de número variado de fornecedores traz ineficiência e custo na gestão e fiscalização da contratação.

18.2. Sobre essa questão, a Súmula nº 247 do TCU estabeleceu o seguinte:

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

18.3. Outrora esse entendimento, consideramos que não é possível afirmar sumariamente, sem a análise do caso concreto, que a licitação por itens ou por lote único seria mais eficiente. O próprio TCU já teve a oportunidade de se manifestar no sentido de que, no caso específico, a licitação por lote único seria a mais eficiente à administração:

> *"Cabe considerar, porém, que o modelo para a contratação parcelada adotado nesse parecer utilizou uma excessiva pulverização dos serviços ... Esta exagerada divisão de objeto pode maximizar a influência de fatores que contribuem para tornar mais dispendiosa a contratação (...) embora as estimativas numéricas não mostrem consistência, não há nos autos nenhuma evidência no sentido oposto, de que o parcelamento seria mais vantajoso para a Administração. Ao contrário, os indícios são coincidentes em considerar a licitação global mais econômica" (Acórdão no 3140/2006 do TCU).”*

18.4. A licitação em grupo consiste na reunião de itens em um mesmo lote, de modo que a disputa ocorra de forma global, resultando na contratação de um único fornecedor para provimento do conjunto da solução. Do ponto de vista técnico, consideramos que todos os itens da pretensão contratual fazem parte de uma solução integrada – de modo que sua divisão é prejudicial ao conjunto do objeto.

18.5. Portanto, embora a solução seja em tese divisível, há interesse técnico na manutenção da unicidade. Ainda, consideramos que não é a simples aplicação da regra geral que dirige o processo decisório, e sim a sua viabilidade técnica – de tal modo que a avaliação sob o aspecto técnico precede a avaliação sob o aspecto

econômico, uma vez que não se trata de contratar uma solução pelo menor preço simplesmente. Em nossa avaliação, o aspecto técnico da manutenção da unicidade (indivisibilidade) garante os benefícios da solução – sendo conveniente à Administração que assim seja licitado;

18.6. Entendemos que os serviços, objeto da contratação, bem como os insumos apresentados, são correlatos e devem ser geridos e executados pela mesma empresa, caso contrário, poderia implicar uma complexa e desnecessária demanda para os fiscais contratuais, uma vez que os serviços deixariam de apresentar um padrão de qualidade, gerando, inclusive, ingerência entre as diversas empresas, caso o objeto fosse dividido em lotes independentes.

18.7. A licitação para a contratação de que trata o objeto deste estudo técnico preliminar, por meio de preço global, nos moldes em que se encontra, permite à Administração uma maior economia com o ganho de escala, haja vista que os licitantes poderão vir a ofertar preços mais competitivos, sem restringir a competitividade.

18.8. Dessa forma, os itens foram agrupados em lote único por terem grande similaridade nas características e especificações, cuja execução em conjunto trará significativa redução de preço, comparando-se com a realização dos serviços em separado, por fornecedores diferentes. A contratação foi agrupada para permitir maior adesão e competitividade ao certame pelo mercado fornecedor, em razão da quantidade de serviço em cada item, ampliando o interesse do mercado, evitando-se assim a necessidade de iniciar nova licitação para o atendimento da demanda em questão.

19. GARANTIA DO CONTRATO

19.1. A contratada deverá apresentar à Administração do contratante, no prazo máximo de **10 (dez) dias úteis**, contado da data que a contratada recebeu a sua via do contrato assinada, comprovante de prestação de garantia de 5% (cinco por cento) sobre o valor anual do contrato, mediante a opção por uma das seguintes modalidades:

19.1.1. Caução em dinheiro ou títulos da dívida pública;

19.1.1.1. A garantia em apreço, quando em dinheiro, deverá ser efetuada na Caixa Econômica Federal, em conta específica, com correção monetária, em favor do Confea.

19.1.2. Seguro garantia; ou

19.1.3. Fiança bancária.

19.2. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 5% (cinco por cento).

19.3. O atraso superior a **25 (vinte e cinco) dias úteis** autoriza a Administração a promover o bloqueio dos pagamentos devidos à contratada, até o limite de 5% (cinco por cento) do valor anual do contrato, a título de garantia.

19.3.1. O bloqueio efetuado com base no item anterior não gera direito a nenhum tipo de compensação financeira à contratada.

19.3.2. A contratada, a qualquer tempo, poderá substituir o bloqueio efetuado com base no item anterior por quaisquer das modalidades de garantia, caução em dinheiro ou títulos da dívida pública, seguro garantia ou fiança bancária.

20. OBRIGAÇÕES DO CONTRATANTE

20.1. Fazer cumprir fielmente as cláusulas do contrato;

20.2. Designar fiscal para acompanhar e fiscalizar a execução do contrato;

20.3. Atestar a nota fiscal ou devolvê-la, em caso de desacordo ou por descumprimento ao pactuado, no prazo de **5 (cinco) dias úteis** após o seu recebimento e encaminhando-a para pagamento, desde que cumpridas todas as exigências pactuadas;

20.4. Efetuar o pagamento à contratada de acordo com as condições e prazos estabelecidos no instrumento contratual, desde que cumpridas todas às exigências pactuadas;

20.5. Prestar as informações e os esclarecimentos que venham a ser solicitados pela contratada;

20.6. Exigir o imediato afastamento e/ou substituição de empregado ou preposto da contratada que não mereça confiança no trato dos serviços, que produza complicações para a fiscalização ou que adote postura inconveniente ou incompatível com o exercício da função que lhe fora atribuída;

20.7. Notificar à contratada a ocorrência de serviços executados e/ou ausência destes que estiverem em desacordo com instrumento contratual;

20.8. Fiscalizar os documentos que comprovem a manutenção das condições de habilitação da contratada, solicitando os originais quando julgar necessário;

20.9. Permitir acesso dos empregados da contratada às suas dependências para a execução do serviço; e

20.10. Observar o cumprimento dos requisitos de qualificação profissional exigidos nas especificações técnicas e nas atribuições, solicitando à contratada as substituições e os treinamentos que se verificarem necessários.

21. **OBRIGAÇÕES DA CONTRATADA**

21.1. Cumprir e garantir o pleno cumprimento do instrumento de contrato;

21.2. Observar as normas e regulamentos internos do contratante, que serão repassados à contratada, bem como fazer com que seus empregados os observem;

21.3. Prestar garantia em favor do contratante no prazo de até **10 (dez) dias úteis**, contados da assinatura do instrumento contratual, correspondente a 5% (cinco por cento) do valor total do contrato, numa das modalidades previstas na Lei nº 8.666, de 21 de junho de 1993;

21.3.1. A reposição do valor da garantia que vier a ser utilizado pelo contratante deverá ocorrer no prazo máximo de **10 (dez) dias úteis**, contados da data da ciência à contratada.

21.4. Selecionar e preparar rigorosamente os empregados que irão prestar os serviços, tendo funções profissionais legalmente registradas em suas carteiras de trabalho;

21.5. Responsabilizar-se por todo e qualquer dano efetivamente comprovado que, por dolo ou culpa, os seus profissionais causarem às dependências, móveis, utensílios ou equipamentos do contratante, ou a terceiros;

21.6. Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho quando, em ocorrência da espécie, forem vítimas, os seus empregados ou prepostos alocados na execução dos serviços, ainda que verificados nas dependências do contratante;

21.7. Responsabilizar-se por todas as obrigações trabalhistas de seus funcionários, tais como: salários; seguros; benefícios; encargos sociais e previdenciários; assistência médica e quaisquer outros, em decorrência de sua condição de empregadora, ficando o contratante isento de qualquer vínculo empregatício;

21.8. Indicar/designar preposto ou empregado para manter entendimento e/ou receber comunicações, solicitações ou transmiti-las ao contratante;

21.9. Atender, por meio de preposto designado, as solicitações do contratante, prestando as informações referentes à prestação dos serviços, bem como as correções de eventuais irregularidades na execução do objeto contratado;

21.10. A contratada deverá providenciar a correção das deficiências apontadas pelo contratante, no prazo de até **3 (três) dias úteis**, sob pena de aplicação de sanções;

21.11. Comunicar ao contratante, por escrito, quando verificar condições inadequadas de execução dos serviços ou a iminência de fatos que possam prejudicar a sua execução;

21.12. Comunicar, por escrito, eventual atraso ou paralisação dos serviços, apresentando razões justificadoras que serão objeto de apreciação pelo contratante;

21.13. Manter, durante toda a execução do contrato, as condições de habilitação e qualificação exigidas para a contratação;

21.14. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto e documento de interesse do contratante, ou de terceiros, de que tomar conhecimento em razão da execução do objeto contratual, devendo orientar seus empregados a observar rigorosamente esta determinação;

21.15. Não reproduzir, divulgar ou utilizar em benefício próprio, ou de terceiros, quaisquer informações de que tenha tomado conhecimento em razão da execução dos serviços, sem consentimento, por escrito, do contratante; e

21.16. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

22. **PAGAMENTO**

22.1. Mediante a prestação dos serviços/entrega dos produtos, o pagamento será feito no prazo de **15 (quinze) dias úteis**, contado da data da atestação da nota fiscal.

22.2. No preço a ser pago deverão estar inclusas todas as despesas inerentes a salários, encargos sociais, tributários, trabalhistas, previdenciários, comerciais, deslocamento, materiais, equipamentos, além de outras, quando houver, enfim, todas as despesas necessárias ao fornecimento do objeto deste objeto;

22.3. O Confea reserva-se o direito de recusar o pagamento se, no ato da atestação, a prestação do serviço não estiver de acordo com a especificação apresentada e aceita.

22.4. O Confea efetivará a atestação da nota fiscal no prazo de **5 (cinco) dias úteis** contados do seu recebimento ou procederá à devolução quando aquela se encontrar em desacordo ao pactuado.

22.5. O aceite dos serviços prestados por força desta contratação será feito mediante ateste das notas fiscais, correspondendo tão somente aos serviços efetivamente prestados.

22.6. O Confea não se responsabilizará pelo pagamento de quaisquer serviços realizados sem a solicitação ou autorização do fiscal do contrato.

22.7. A nota fiscal deverá ser acompanhada dos documentos que comprovem a sua regularidade fiscal, compreendendo no mínimo o INSS, FGTS, Receita Federal/Municipal, Dívida Ativa da União e CNDT.

22.8. A nota fiscal será emitida sem rasura, legível, em nome do contratante e com CNPJ do qual constará o número do contrato e as informações para crédito em conta corrente:

22.8.1. Nome e número do banco, nome e número da agência e número da conta;

22.8.2. A primeira via do documento fiscal de eventual fornecedor; e

22.8.3. Os documentos de comprovação de serviços executados por terceiros, da execução dos serviços, e quando for o caso, do comprovante de sua entrega.

22.9. A nota fiscal deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta online 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 8.666/1993.

22.10. 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.

22.11. 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 o contratante.

22.12. A contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, 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.

23. **REAJUSTE**

23.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contados da data da assinatura do contrato, podendo ser prorrogado nos moldes da legislação vigente.

23.2. Uma vez prorrogado o contrato, a periodicidade anual para a concessão dos reajustes será considerada conforme rege a Lei nº 10.192/2001, art. 3°, §1°, com a finalidade de neutralizar os efeitos da inflação sobre a equação econômico-financeira estabelecida.

23.3. Para o reajuste será considerado o Índice de Custos de Tecnologia da Informação - ICTI, conforme previsão expressa contida no art. 24 da Instrução Normativa nº 94, de 23 de dezembro de 2022.

23.4. A prorrogação do prazo de vigência do contrato em exercícios subsequentes ficará condicionada à avaliação da qualidade dos serviços prestados, à comprovação da compatibilidade com os preços de mercado e inexistência de irregularidade contratual.

23.5. 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.

23.6. 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.

24. **PENALIDADES ADMINISTRATIVAS**

24.1. Com fundamento nos artigos 86 e 87, incisos I a IV, da Lei nº 8.666/1993, nos casos de retardamento ou de inexecução do objeto, garantida a ampla defesa, a contratada poderá ser apenada, isoladamente ou juntamente com demais multas, com as seguintes penalidades:

24.1.1. Advertência;

24.1.2. Suspensão temporária de participação em licitação e impedimento de contratar com a Administração do Confea, por prazo não superior a dois anos;

24.1.3. 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 Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior; ou

24.1.4. Impedimento de licitar e contratar com a Administração Pública e descredenciamento no Sicaf.

24.2. Em caso de inexecução parcial do objeto, a contratada fica sujeita à multa equivalente a 1% (um por cento) do valor unitário do bem em atraso, por dia, por unidade, até o limite de 20% (vinte por cento) do valor empenhado.

24.2.1. Considera-se inexecução parcial o atraso injustificado no prazo de entrega (para bens) ou no início da execução contratual (para serviços) até o limite de **20 (vinte) dias úteis**.

24.3. Em caso de inexecução total do objeto, a contratada fica sujeita à multa de, no máximo, 30% (trinta por cento) do valor anual do contrato.

24.3.1. Considera-se inexecução total o atraso injustificado no prazo de entrega (para bens) ou no início da execução contratual (para serviços) superior a **20 (vinte) dias úteis**.

24.4. O não cumprimento de obrigação contratual acessória, a exemplo da prestação da garantia contratual exigida, sujeitará a contratada à multa de até 10% (dez por cento) do valor empenhado.

24.5. A falha na execução do contrato estará configurada quando a contratada se enquadrar em qualquer das situações previstas na tabela º 02 do item a seguir.

24.6. Pelo descumprimento das obrigações contratuais, a Administração aplicará multas conforme a graduação estabelecida nas tabelas seguintes:

Tabela nº 01	
GRAU	**CORRESPONDÊNCIA (%)**
01	10%
02	5%
03	3%

Tabela nº 02			
ITEM	**DETALHAMENTO DA INFRAÇÃO**	**GRAU**	**INCIDÊNCIA**
A	Não reparar, corrigir, remover, reconstruir ou substituir às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções, no prazo estipulado no Termo de Referência.	03	Por ocorrência
B	Fornecer produtos/serviços com especificação e qualidade diversa e/ou inferior a demandada.	03	Por produtos/serviços
C	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratados.	03	Por dia
D	Recusar a execução de serviço determinado pela fiscalização, sem motivo justificado.	02	Por ocorrência
E	Manter funcionário na execução dos serviços demandados sem a qualificação especificada no Termo de Referência e seus anexos	02	Por empregado e por dia
F	Destruir ou danificar documentos por culpa ou dolo de seus agentes.	02	Por ocorrência
G	Permitir situação que crie a possibilidade de causar ou que cause dano físico, lesão corporal ou consequências letais.	02	Por ocorrência

H	Não manter as condições de habilitação originárias da contratação.	02	Por ocorrência e por dia
I	Descumprir qualquer das obrigações contratuais previstas no Termo de Referência e seus anexos.	01	Por ocorrência
J	Não executar os serviços e/ou entregar os produtos conforme as especificações e as qualificações estabelecidas no Termo de Referência e seus anexos.	01	Por ocorrência e por dia
K	Não observar os prazos para execução dos serviços e/ou entrega de produtos.	01	Por ocorrência e por dia
L	Permitir a presença de empregado não uniformizado ou com uniforme manchado, sujo, mal apresentado e/ou sem crachá.	01	Por empregado e por ocorrência
M	Não fornecer os materiais e ferramentas necessários à completa execução do objeto.	01	Por item não fornecido
N	Não prestar as informações e os esclarecimentos que venham a ser solicitados.	01	Por ocorrência e por dia
O	Prestar serviços que não estejam em conformidade com as especificações técnicas previstas no Termo de Referência, no Contrato e/ou na proposta da Contratada	03	Por serviço

24.7. O valor da multa poderá ser descontado das notas fiscais devidas à contratada.

24.7.1. Se o valor a ser pago à contratada não for suficiente para cobrir o valor da multa, a diferença será descontada da garantia contratual.

24.7.2. Se os valores das notas fiscais e da garantia forem insuficientes, fica a contratada obrigada a recolher a importância devida no prazo de **15 (quinze) dias úteis**, contado da comunicação oficial.

24.7.3. Caso o valor da garantia seja utilizado no todo ou em parte para o pagamento da multa, esta deve ser complementada no prazo de até **10 (dez) dias úteis**, contado da solicitação do contratante.

24.8. O contrato, sem prejuízo das multas e demais cominações legais previstas no contrato, poderá ser rescindido unilateralmente, por ato formal da Administração, nos casos enumerados no art. 78, incisos I a XII e XVII, da Lei nº 8.666/1993.

24.9. Comprovado impedimento ou reconhecida força maior, devidamente justificado e aceito pela Administração do contratante em relação a(s) penalidade(s) aplicada(s), a contratada ficará isenta desta(s).

24.10. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa, observando-se o procedimento previsto na Lei nº 8.666/1993 e subsidiariamente na Lei nº 9.784, de 29 de janeiro de 1999.

24.11. Caberá ao Ordenador de Despesa, após o devido processo legal, garantido o contraditório e a ampla defesa, decidir pela aplicação da sanção administrativa cabível.

25. MODELO DE EXECUÇÃO DO CONTRATO

25.1. A Instrução Normativa nº 94, de 23 de dezembro de 2022, dispõe que "Art. 18. O Modelo de Execução do Contrato definirá como o contrato deverá produzir os resultados pretendidos desde o seu início até o seu encerramento, observando, quando possível":

25.1.1. I - fixação das rotinas de execução, com a definição de processos e procedimentos de fornecimento da solução de TIC, envolvendo: a) prazos, horários de fornecimento de bens ou prestação dos serviços e locais de entrega, quando aplicáveis;

25.1.1.1. Consoante aos itens "Prazo de Vigência e Execução" e "Local para execução dos serviços e/ou entrega dos produtos" deste Termo de Referência.

25.1.2. I - fixação das rotinas de execução, com a definição de processos e procedimentos de fornecimento da solução de TIC, envolvendo: b) documentação mínima exigida, observando modelos adotados pelo contratante, padrões de qualidade e completude das informações, a exemplo de modelos de desenvolvimento de software, relatórios de execução de serviço e/ou fornecimento, controles por parte da contratada, ocorrências, etc.

25.1.2.1. Consoante aos itens "Critérios Técnicos para Seleção do Fornecedor" e "Definição e Especificação de Requisitos" deste Termo de Referência.

25.1.3. I - fixação das rotinas de execução, com a definição de processos e procedimentos de fornecimento da solução de TIC, envolvendo: c) papéis e responsabilidades, por parte do contratante e da contratada, quando couber;

25.1.3.1. Consoante item "Modelo de Gestão do Contrato" deste Termo de Referência.

25.1.4. II - quantificação ou estimativa prévia do volume de serviços demandados ou quantidade de bens a serem fornecidos, para comparação e controle;

25.1.4.1. Consoante ao item "Justificativa para a contratação/aquisição" deste Termo de Referência.

25.1.5. III - definição de mecanismos formais de comunicação a serem utilizados para troca de informações entre a contratada e a Administração, adotando-se preferencialmente as Ordens de Serviço ou Fornecimento de Bens;

25.1.5.1. Consoante ao item "Mecanismos formais de comunicação" deste Termo de Referência.

25.1.6. IV - forma de pagamento, que será efetuado em função dos resultados obtidos; e

25.1.6.1. Consoante ao item "Pagamento" deste Termo de Referência.

25.1.7. V - elaboração dos seguintes modelos de documentos, em se tratando de contratações de serviços de TIC: a) Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes no órgão ou entidade, a ser assinado pelo representante legal da contratada; e

25.1.7.1. Consoante ao Anexo II deste Termo de Referência.

25.1.8. V - elaboração dos seguintes modelos de documentos, em se tratando de contratações de serviços de TIC: b) Termo de Ciência da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão ou entidade, a ser assinado por todos os empregados da contratada diretamente envolvidos na contratação.

25.1.8.1. Consoante ao Anexo III deste Termo de Referência.

25.2. A empresa contratada deverá seguir o modelo de execução contratual conforme o objeto.

26. MODELO DE GESTÃO DO CONTRATO

26.1. A Instrução Normativa nº 94, de 23 de dezembro de 2022, dispõe que "Art. 19. O Modelo de Gestão do Contrato descreverá como a execução do objeto será acompanhada e fiscalizada pelo órgão ou entidade, observando, quando possível":

26.1.1. I - fixação dos critérios de aceitação dos serviços prestados ou bens fornecidos, abrangendo métricas, indicadores e níveis mínimos de serviços com os valores aceitáveis para os principais elementos que compõe a solução de TIC;

26.1.1.1. Consoante ao item "Definição e Especificação de Requisitos" deste Termo de Referência.

26.1.2. II - procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo, conforme disposto no art. 73 da Lei nº 8.666, de 1993, abrangendo: a) metodologia, formas de avaliação da qualidade e adequação da solução de TIC às especificações funcionais e tecnológicas, observando: 1. definição de mecanismos de inspeção e avaliação da solução, a exemplo de inspeção por amostragem ou total do fornecimento de bens ou da prestação de serviços; 2. adoção de ferramentas, computacionais ou não, para implantação e acompanhamento dos indicadores estabelecidos; 3. origem e formas de obtenção das informações necessárias à gestão e à fiscalização do contrato; 4. definição de listas de verificação e de roteiros de testes para subsidiar a ação dos Fiscais do contrato; e 5. previsão de inspeções e diligências, quando aplicáveis, e suas formas de exercício;

26.1.2.1. Consoante ao item "Definição e Especificação de Requisitos" deste Termo de Referência.

26.1.3. II - procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo, conforme disposto no art. 73 da Lei nº 8.666, de 1993, abrangendo: b) disponibilidade de 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;

26.1.3.1. Através da elaboração de Portaria com a designação de Equipe de Fiscalização do Contrato pelo Confea embasado nas especificações técnicas contidas no item "Definição e Especificação de Requisitos" deste Termo de Referência.

26.1.4. III - fixação dos valores e procedimentos para retenção ou glosa no pagamento, sem prejuízo das sanções cabíveis, que só deverá ocorrer quando a contratada: a) não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou b) deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

26.1.4.1. Consoante ao item "Pagamento" deste Termo de Referência.

26.1.5. IV - definição clara e detalhada das sanções administrativas, de acordo com os arts. 86, 87 e 88 da Lei nº 8.666, de 1993, juntamente com o art. 7º da Lei nº 10.520, de 2002, observando: a) vinculação aos termos contratuais; b) proporcionalidade das sanções previstas ao grau do prejuízo causado pelo descumprimento das respectivas obrigações; c) as situações em que advertências serão aplicadas; d) as situações em que as multas serão aplicadas, com seus percentuais correspondentes, que obedecerão a uma escala gradual para as sanções recorrentes; e) as situações em que o contrato será rescindido por parte da Administração devido ao não atendimento de termos contratuais, da recorrência de aplicação de multas ou outros motivos; f) as situações em que a contratada terá suspensa a participação em licitações e impedimento para contratar com a Administração; e g) as situações em que a contratada será declarada inidônea para licitar ou contratar com a Administração, conforme previsto em Lei;

26.1.5.1. Consoante ao item "Penalidades Administrativas" deste Termo de Referência.

26.1.6. V - procedimentos para o pagamento, descontados os valores oriundos da aplicação de eventuais glosas ou sanções.

26.1.6.1. Consoante aos itens "Pagamento" e "Penalidades Administrativas" deste Termo de Referência.

26.2. A fiscalização do cumprimento das obrigações contratuais será exercida por empregados devidamente designados pelo contratante, por meio de Portaria específica, nas funções de Gestor do Contrato, Fiscal Técnico, Fiscal Administrativo e Fiscal Requisitante, em conformidade com o art. 29 da Instrução Normativa nº 94, de 23 de dezembro de 2022.

26.3. A Equipe de Fiscalização do Contrato, atuando nos termos dos artigos 31 a 38 da Instrução Normativa nº 94, de 23 de dezembro de 2022, deverá acompanhar, fiscalizar, conferir e avaliar a execução do fornecimento/serviços, bem como dirimir e desembaraçar quaisquer dúvidas e pendências que surgirem, determinando medidas necessárias à regularização das faltas, falhas, problemas ou defeitos observados no curso do contrato, e de tudo dará ciência diretamente à contratada, conforme artigo 67, parágrafos, da Lei n.º 8.666/1993 e suas alterações.

26.3.1. A Equipe de Fiscalização do Contrato promoverá o acompanhamento e a fiscalização dos serviços, sob os aspectos qualitativo e quantitativo, anotando em registro próprio os fatos que, a seu critério, exijam medidas corretivas dos trabalhos, em relatórios formais, nos quais deverão ser apontadas as conformidades e as não conformidades.

26.3.2. A fiscalização acima mencionada não exclui e nem reduz a responsabilidade da empresa contratada, inclusive perante terceiros, por qualquer irregularidade na execução dos serviços.

26.3.3. A fiscalização não aceitará, sob nenhum pretexto, a transferência de qualquer responsabilidade da empresa contratada para outras entidades, sejam fabricantes, sejam técnicos, subempreiteiros, dentre outros.

26.3.4. A fiscalização poderá paralisar e/ou solicitar o refazimento de qualquer serviço que não seja executado em conformidade com as normas que regulam a matéria.

26.3.5. A fiscalização poderá esclarecer ou requerer correções de incoerências, falhas e omissões eventualmente constatadas.

26.3.6. A fiscalização exercerá rigoroso controle sobre o cronograma de execução dos serviços para evitar atraso no cumprimento dos trabalhos.

26.4. Para o caso de impedimento de qualquer dos empregados indicados para as funções de fiscalização, serão designados pelo contratante empregados para atuar como substitutos.

26.5. Conforme previsto no artigo 31, inciso I, da Instrução Normativa nº 94, de 23 de dezembro de 2022, cabe ao Gestor do Contrato a convocação para realização da reunião inicial, com a participação da Equipe de Fiscalização do Contrato, da contratada e dos demais intervenientes por ele identificados, cuja pauta observará, pelo menos:

26.5.1. Presença do representante legal da contratada, que apresentará o preposto;

26.5.2. Entrega, por parte da contratada, do Termo de Compromisso e dos Termos de Ciência, conforme art. 18, inciso V, da Instrução Normativa nº 94, de 23 de dezembro de 2022; e

26.5.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.

26.6. As faltas cometidas pela contratada deverão ser devidamente registradas no Processo de Execução pelo Gestor do Contrato, que deverá propor ao Ordenador de Despesas a aplicação das sanções que entender cabíveis para a regularização das faltas, nos termos do artigo 67, parágrafo 2.º e do artigo 87 da Lei n.º 8.666/1993.

26.7. Caberá à contratada o pronto atendimento às exigências inerentes ao objeto contratado feitas pelo Gestor do Contrato ou por seu substituto.

26.8. A contratada é responsável pelos danos causados diretamente à Administração ou à terceiros decorrentes de sua culpa ou dolo na execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento por parte do contratante (art. 70 da Lei nº 8.666/93).

26.9. O contratante se reserva o direito de rejeitar, no todo ou em parte, o serviço prestado em desacordo com o contrato (art. 76 da Lei nº 8.666/93).

26.10. Durante a execução do objeto, o fiscal do contrato deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à contratada a correção das faltas, falhas e irregularidades constatadas.

26.11. O fiscal do contrato deverá apresentar ao responsável ou preposto indicado pela contratada a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizada.

26.12. Em hipótese alguma, será admitido que a própria contratada materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

26.13. A contratada poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal do contrato, desde que comprovada a excepcionalidade da ocorrência resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador.

26.14. O fiscal do contrato poderá realizar avaliação diária, semanal ou mensal, desde que o período escolhido seja suficiente para avaliar ou, se for o caso, aferir o desempenho e qualidade da prestação dos serviços.

27. **MECANISMOS FORMAIS DE COMUNICAÇÃO**

27.1. Sempre que exigir-se a comunicação entre o Gestor do Contrato e o Preposto da contratada deverá ser formal, considerando-se como documentos formais, além de documentos do tipo Ofício, as comunicações por correio eletrônico e/ou por software de gestão de contratos.

27.2. O Gestor do Contrato e o Preposto responderão sobre todas as questões sobre o contrato a ser firmado, procurando solucionar todos os problemas que defrontarem, dentro dos limites legais e dentro da razoabilidade.

27.3. Caberá à contratada indicar formalmente o(s) e-mail(s) e telefone(s) de contato do(s) preposto(s) indicado(s), bem como o endereço de contato quando da realização da reunião inicial.

27.3.1. Na mesma ocasião, o contratante informará os contatos do Gestor e dos demais fiscais.

27.4. A Ordem de Serviço é o instrumento formal pelo qual o Confea encaminha a demanda de serviço para a contratada.

27.5. Todos os serviços demandados deverão ser executados pela contratada somente após a emissão de Ordens de Serviços, com a obrigatória autorização do contratante e em concordância com os processos e procedimentos técnicos definidos pelo demandante.

27.6. As Ordens de Serviço serão emitidas, acompanhadas, revisadas e recebidas/aceitas pelo Confea.

27.7. Em todas as Ordens de Serviços deverão ser definidas as datas de início e final da execução do serviço, conforme entendimentos entre contratante e contratada.

27.8. A obrigação de execução ocorrerá quando a contratada receber a Ordem de Serviço e a assinar, juntamente com as assinaturas de solicitação do demandante e aprovação dos fiscais e do gestor do contrato.

27.9. As Ordens de Serviço serão recebidas pelo Confea tanto em caráter provisório como em definitivo.

27.10. **Do Termo de Recebimento Provisório do objeto e da avaliação de qualidade e conformidade.**

27.10.1. O objeto contratado será recebido como parte do processo de monitoramento da execução, de forma provisória e definitiva, conforme prevê o artigo 2º da Instrução Normativa n° 94, de 23 de dezembro de 2022: "**Termo de Recebimento Provisório** - termo detalhado declarando que os serviços foram prestados ou declaração sumária de que as compras foram entregues, com verificação posterior da conformidade do material com as exigências contratuais, de acordo com a alínea "a" do inciso I, e alínea "a" do inciso II do art. 73 da Lei nº 8.666, de 1993";

27.11. Após a execução dos serviços previstos para a Ordem de Serviço, será emitido o Termo de Recebimento Provisório no prazo de até **5 (cinco) dias úteis**, contados do recebimento pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta de preços.

27.11.1. A contratada deverá emitir, mensalmente, relatório de acesso à base de conhecimento e utilização dos demais serviços vinculados à subscrição para cada licença contratada.

27.12. O recebimento provisório será realizado pelo fiscal técnico do contrato quando da entrega do objeto resultante de cada etapa de serviço.

27.13. Após o aceite, consistirá na emissão do Termo de Recebimento Provisório.

27.14. Os serviços entregues serão objeto de avaliação e aprovação pela Equipe de Fiscalização do Contrato do Confea.

27.15. Será comunicada formalmente à contratada a não conformidade dos produtos, caso existir.

27.16. Os bens ou serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta de preços, devendo ser substituídos, no prazo de até 15 (quinze) dias úteis, a contar da notificação do contratante.

27.17. O prazo para recebimento definitivo desses serviços será reiniciado após o recebimento dos produtos corrigidos e a emissão de novo Termo de Recebimento Provisório, quando então serão reavaliados quanto aos critérios de qualidade e de aceitação.

27.18. **Do Termo de Recebimento Definitivo.**

27.18.1. Após a realização das verificações e validações necessárias, e não havendo ajustes a realizar, o Confea emitirá o Termo de Recebimento Definitivo, conforme prevê o artigo 2º da Instrução Normativa n° 94, de 23 de dezembro de 2022: "**Termo de Recebimento Definitivo** - termo detalhado que comprove o atendimento das exigências contratuais, de acordo com a alínea "b" do inciso I, e alínea "b" do inciso II do art. 73 da Lei nº 8.666, de 1993".

27.18.2. Concluída a avaliação da conformidade dos serviços prestados de acordo com as especificações técnicas previstas neste Termo de Referência e na proposta da Contratada, o gestor do contrato efetuará o recebimento definitivo dos serviços por meio do Termo de Recebimento Definitivo, contendo a autorização para emissão de nota fiscal a ser encaminhada ao preposto da contratada.

27.18.3. No prazo de até **10 (dez) dias úteis**, contados do recebimento provisório, após a verificação da conformidade dos serviços prestados com as especificações técnicas constantes neste instrumento e na proposta da Contratada, o objeto será recebido definitivamente, a respectiva nota fiscal atestada e o processo encaminhado para pagamento.

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

27.18.5. O contratante irá comunicar a empresa para que emita a nota fiscal com o valor exato dimensionado pela fiscalização.

27.19. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

27.20. Caso a contratada não consiga executar a Ordem de Serviço conforme as condições demandas, deverá comunicar ao fiscal por escrito e com antecedência, justificando os fatos e motivos que impedirão sua execução, cabendo ao gestor acatar ou não a justificativa.

27.21. A Ordem de Serviço poderá ser replanejada a qualquer momento a critério do Confea, sendo registrada formalmente tal ação.

27.22. Para cada Ordem de Serviço executada, além do Relatório de Atividade Técnica executada, deverão ser entregues pela contratada os artefatos/documentações que se fizerem necessários quando da abertura da Ordem de Serviço.

28. **SIGILO DAS INFORMAÇÕES**

28.1. Na execução dos serviços descritos neste Termo de Referência, a contratada terá acesso a informações críticas do Sistema Confea/Crea, cabendo à contratada:

28.1.1. Assinar e cumprir o Termo de Compromisso e Manutenção do Sigilo, conforme modelo constante no Anexo II;

28.1.2. Guardar sigilo das informações que receber durante a execução do contrato; e

28.1.3. Responsabilizar-se pela divulgação não autorizada ou pelo uso indevido de qualquer informação pertinente ao Sistema Confea/Crea.

28.2. Caso se verifique a quebra de sigilo das informações disponibilizadas pelo Confea, serão aplicadas as sanções cabíveis.

29. **PROPOSTA DE PREÇOS**

29.1. A proposta de preços deverá ser apresentada com base nas especificações, prazos de entregas, obrigações e demais considerações contidas neste Termo de Referência.

30. **MAPA DE GERENCIAMENTO DE RISCOS**

30.1. A Instrução Normativa nº 94, de 23 de dezembro de 2022, dispõe que o Mapa de Gerenciamento de Riscos e um "instrumento de registro e comunicação da atividade de gerenciamento de riscos ao longo de todas as fases da contratação" e que "§ 4º O Mapa de Gerenciamento de Riscos deve ser juntado aos autos do processo administrativo, pelo menos: I - ao final da elaboração do Termo de Referência; II - ao final da fase de Seleção do Fornecedor; III - uma vez ao ano, durante a gestão do contrato; e IV - após eventos relevantes".

30.2. Dispõe, ainda, que "Art. 38. O gerenciamento de riscos deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão prevista na Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016, registrando-se o alinhamento no Mapa de Gerenciamento de Riscos. § 1º Durante a fase de planejamento, a equipe de Planejamento da Contratação deve proceder às ações de gerenciamento de riscos e produzir o Mapa de Gerenciamento de Riscos que deverá conter no mínimo: I - identificação e análise dos principais riscos, consistindo na compreensão da natureza e determinação do nível de risco, mediante a combinação do impacto e de suas probabilidades, que possam comprometer a efetividade da contratação, bem como o alcance dos resultados pretendidos com a solução de TIC; II - avaliação e seleção da resposta aos riscos em função do apetite a riscos do órgão; e III - registro e acompanhamento das ações de tratamento dos riscos".

30.3. Cumprindo com o disposto no artigo 38 da Instrução Normativa nº 94, de 23 de dezembro de 2022, serão analisados os riscos inerentes a três situações distintas relacionadas a este processo de contratação, que são as fases de Planejamento da Contratação, Seleção do Fornecedor e Contratação da Solução.

30.4. Dessa feita, o Mapa de Gerenciamento de Riscos se encontra no Anexo I deste Termo de Referência.

31. **UNIDADE ORGANIZACIONAL RESPONSÁVEL PELAS INFORMAÇÕES**

31.1. A Gerência de Tecnologia da Informação - GTI é a unidade organizacional responsável pelas informações constantes neste instrumento e adoção de providências necessárias à continuidade do processo de contratação.

EDITAL DO PREGÃO ELETRÔNICO Nº 13/2023

ANEXO II - ORÇAMENTO ESTIMATIVO

Item	CatSer	Descrição	Quant.	Unidade	Valor Unitário	Valor Total
01	393277	Appliance com capacidade para suportar um *throughput* mínimo de 12 Gb/s.	2	*Hardware*	R$ 772.134,95	R$ 1.544.269,89
02	27464	Licença de uso de *software* a ser utilizada no equipamento do Item 01, incluindo garantia, atualização de versões e suporte técnico por 36 meses.	2	*Software*	R$ 837.642,90	R$ 1.675.285,81
03	27464	Solução de Zero Trust Network Access (ZTNA) com capacidade para suportar 500 usuários.	500	*Software*	R$ 235,45	R$ 117.725,00
04	21172	Treinamento da Solução Ofertada.	3	Serviço	R$ 15.781,24	R$ 47.343,72

TOTAL	**R$ 3.384.624,43**

EDITAL DO PREGÃO ELETRÔNICO Nº 18/2023

ANEXO III - MODELO DE PROPOSTA DE PREÇOS

Proposta, que faz a empresa _____, inscrita no CNPJ (MF) sob o nº _____ e inscrição estadual nº _____, para a prestação de serviços integrados de segurança cibernética de ponta, incluindo a provisão de um sistema de proteção de perímetro robusto e avançado, para atender as necessidades do Conselho Federal de Engenharia e Agronomia - Confea, sediado em Brasília - DF, conforme especificações contidas neste Edital e seus anexos.

A proposta de preços deverá ser apresentada, com base nas especificações, prazos de entregas, obrigações e demais considerações contidas neste Edital e seus anexos.

PROPOSTA DE PREÇO						
Item	**CatSer**	**Descrição**	**Quant.**	**Métrica**	**Valor Unitário**	**Valor Total**
01	393277	Appliance com capacidade para suportar um *throughput* mínimo de 12 Gb/s.	2	*Hardware*	R$	R$
02	27464	Licença de uso de *software* a ser utilizada no equipamento do Item 01, incluindo garantia, atualização de versões e suporte técnico por 36 meses.	2	*Software*	R$	R$
03	27464	Solução de Zero Trust Network Access (ZTNA) com capacidade para suportar 500 usuários.	500	*Software*	R$	R$
04	21172	Treinamento da Solução Ofertada.	3	Serviço	R$	R$
TOTAL						**R$**

O orçamento a ser apresentado deverá contemplar os preços unitários descritos na tabela acima e consoante as especificações técnicas contidas no anexo.

a) A planilha final que será apresentada deverá apresentar valores **unitários e global** iguais ou inferiores aos estimados pelo Confea.

b) O preço proposto é de exclusiva responsabilidade da empresa, a qual não poderá pleitear quaisquer direitos, na vigência do contrato, e nenhuma alteração sob a alegação de erro, omissão ou qualquer outro pretexto.

c) Nos preços ofertados deverão já estar considerados e inclusos todos os custos e despesas relacionados à execução e necessários ao cumprimento integral do objeto, tais como custos diretos e indiretos, tributos incidentes, materiais, encargos sociais, trabalhistas, transporte diversos, seguros, lucro, taxas e demais despesas.

d) Validade mínima da proposta é de **90 (noventa) dias**.

e) Dados da empresa: Razão social; CNPJ; Endereço completo; Telefone; Nome do Banco; Número do Banco; Agência e Número da conta corrente.

f) Desde já, declararam-se cientes de que o **Confea** procederá à retenção de tributos e contribuições nas situações previstas em lei, se houver.

Observação:

1) Este documento deverá ser emitido em papel que identifique a licitante.

EDITAL DO PREGÃO ELETRÔNICO Nº 18/2023

ANEXO IV - TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

O **CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA - CONFEA**, sediado em Brasília - DF, SEPN Comércio Residencial Norte 508 - Asa Norte, Brasília/DF, 70740-541, CNPJ 33.665.647/0001-91, doravante denominada CONTRATANTE, e, de outro lado, a empresa <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ nº <CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO Nº <XX/XXXX> doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a **informações sigilosas** do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas **informações sigilosas**, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, referente ao Pregão Eletrônico nº XXX/2023, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA - DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei nº 12.527, de 18/11/2011 e os Decretos nº 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

CLÁUSULA SEGUNDA - DOS CONCEITOS E DEFINIÇÕES

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

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

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

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

CLÁUSULA TERCEIRA – DA INFORMAÇÃO SIGILOSA

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

CLÁUSULA QUARTA – DOS LIMITES DO SIGILO

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

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

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

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

CLÁUSULA QUINTA – DOS DIREITOS E OBRIGAÇÕES

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

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

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

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

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

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

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

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

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

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

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

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

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

CLÁUSULA SEXTA – DA VIGÊNCIA

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

CLÁUSULA SÉTIMA – DAS PENALIDADES

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

CLÁUSULA OITAVA – DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

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

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

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

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

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

CLÁUSULA NONA – DO FORO

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

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

De acordo

CONTRATANTE	CONTRATADA	TESTEMUNHA 1	TESTEMUNHA 2
_____ Fiscal do Contrato	_____ Preposto	_____ Nome/Qualificação	_____ Nome/Qualificação

Brasília, _____ de _____ de 20_____.

EDITAL DO PREGÃO ELETRÔNICO Nº 18/2023

ANEXO V - TERMO DE CIÊNCIA DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO

Visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos no projeto sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.

IDENTIFICAÇÃO

CONTRATO Nº			
OBJETO			
CONTRATANTE			
GESTOR DO CONTRATO		**MATRÍCULA**	
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 Manutenção de Sigilo e as normas de segurança vigentes no Contratante.

CIÊNCIA	
CONTRATADA - Funcionários	
_____ Nome/CPF	_____ Nome/CPF
_____ Nome/CPF	_____ Nome/CPF
_____ Nome/CPF	_____ Nome/CPF

Brasília, _____ de _____ de 20_____.

EDITAL DO PREGÃO ELETRÔNICO Nº 18/2023

ANEXO VI - TERMO DE RECEBIMENTO PROVISÓRIO (TRP)

IDENTIFICAÇÃO

Pregão Eletrônico nº XX/20XX.

Contrato nº: XXX/20XX.

Período da Vigência: O contrato terá vigência de XX (por extenso) meses, contados da data da assinatura do contrato pelo CONTRATANTE, podendo ser prorrogado nos moldes da legislação vigente, ou seja, de DIA/MÊS/ANO a DIA/MÊS/ANO.

Nota de Empenho: Nota de inscrição em restos a pagar nº XX (SEI nº XXXX), no valor de R$ XX (por extenso).

Contratante: Conselho Federal de Engenharia e Agronomia - Confea

Contratada:

CNPJ:

Endereço:

Endereço Eletrônico:

Ordem de Serviço nº: XX/20XX (SEI nº XXX)

Objeto:

Valor dos Bens/Serviços Recebidos: R$ XX (por extenso), com pagamentos anuais no valor de R$ XX (por extenso).

Data da Entrega: DIA/MÊS/ANO.

Data do Recebimento: DIA/MÊS/ANO.

Documentos Entregues

SEI nº XXX: nome do documento.

SEI nº XXX: nome do documento.

SEI nº XXX: nome do documento.

TERMOS

Por este instrumento, atesto, para fins de cumprimento do disposto no art. 33, inciso I, da Instrução Normativa nº 94, de 23 de dezembro de 2022, que os serviços e/ou bens integrantes da Ordem de Serviço acima identificada, ou conforme definido no Modelo de Execução do contrato supracitado, foram recebidos, **provisoriamente**,

nesta data e serão objetos de avaliação quanto à adequação da Solução de Tecnologia da Informação e à conformidade de qualidade de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato pelo contratante.

Ressaltamos que o recebimento definitivo destes serviços e/ou bens ocorrerá em até 10 (dez) dias úteis, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Contrato acima identificado.

EDITAL DO PREGÃO ELETRÔNICO Nº 18/2023

ANEXO VII - TERMO DE RECEBIMENTO DEFINITIVO (TRD)

IDENTIFICAÇÃO

Pregão Eletrônico nº: XX/20XX.

Contrato nº: XXX/20XX.

Período da Vigência: O contrato terá vigência de XX (por extenso) meses contados da data da assinatura do contrato pelo CONTRATANTE, podendo ser prorrogado nos moldes da legislação vigente, ou seja, de DIA/MÊS/ANO a DIA/MÊS/ANO.

Nota de Empenho: Nota de inscrição em restos a pagar nº XX (SEI nº XXXX), no valor de R$ XX (por extenso).

Contratante: Conselho Federal de Engenharia e Agronomia - Confea.

Contratada:

CNPJ:

Endereço:

Endereço Eletrônico:

Ordem de Serviço nº: XX/20XX (SEI nº XXX)

Objeto:

Valor dos Bens/Serviços Recebidos: R$ XX (por extenso), com pagamentos anuais no valor de R$ XX (por extenso).

Data da Entrega: DIA/MÊS/ANO.

Data do Recebimento: DIA/MÊS/ANO.

TERMOS

1. Por este instrumento, em **caráter definitivo**, atestamos que os serviços e/ou bens acima identificados foram devidamente executados/entregues e atendem às exigências especificadas no Contrato nº XX/20XX (SEI nº XXXX).

2. De forma a subsidiar este Termo de Recebimento Definitivo, foram considerados as seguintes análises e documentos:

2.1. Termo de Recebimento Provisório (SEI nº XXXX e documentos correlatos).

2.2. Análise Técnica do Fiscal do Contrato (SEI nº XXXX documento correlatos).

EDITAL DO PREGÃO ELETRÔNICO Nº 18/2023

ANEXO VIII - MINUTA DE CONTRATO

CONTRATO QUE ENTRE SI CELEBRAM O CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA (CONFEA) E A EMPRESA _____, CONFORME PROCESSO Nº 00.003325/2023-49**.**

O **Conselho Federal de Engenharia e Agronomia - Confea**, neste ato denominado **CONTRATANTE**, com sede no SEPN, Quadra 508, Bloco "A", Edifício Confea - Engenheiro Francisco Saturnino de Brito Filho, Asa Norte, CEP.: 70.740-541, Brasília - DF, inscrito no CNPJ (MF) sob o nº 33.665.647/0001-91, representado pelo seu Vice-Presidente no exercício da Presidência, **Eng. Eletr. Evânio Ramos Nicoleit** , CPF nº 575.599.100-68, RG nº 7034291951 SSP/RS, e, de outro lado, a empresa _____, inscrita no CNPJ (MF) sob o nº _____, estabelecida a _____, doravante denominada simplesmente **CONTRATADA**, neste ato representada pelo Sr. _____, portador da Cédula de Identidade nº _____, CPF (MF) nº _____, de acordo com a representação legal que lhe é outorgada, têm entre si justo e avençado e celebram o presente instrumento, de acordo com o **Edital do Pregão Eletrônico nº 18/2023** e a proposta apresentada pela **CONTRATADA**, constante do **Processo nº** 00.003325/2023-49, sujeitando-se **CONTRATANTE** e **CONTRATADA** às normas disciplinares da Lei nº 8.666, de 21 de junho de 1993, e da Lei nº 10.520, de 17 de julho de 2002, e do Decreto nº 10.024, de 20 de setembro de 2019, mediante as cláusulas que se seguem:

CLÁUSULA PRIMEIRA - DO OBJETO

Contratação de empresa especializada em serviços integrados de segurança cibernética de ponta, incluindo a provisão de um sistema de proteção de perímetro robusto e avançado, para atender as necessidades do Conselho Federal de Engenharia e Agronomia - Confea, conforme especificações e condições constantes neste instrumento e no Edital de Pregão Eletrônico nº 18/2023 e seus anexos.

CLÁUSULA SEGUNDA - DO REGIME DE EXECUÇÃO

A execução ocorrerá de forma indireta, sob o regime de empreitada por preço global, segundo o disposto nos artigos 6º e 10º da Lei nº 8.666/93.

CLÁUSULA TERCEIRA - DO VALOR DO CONTRATO

3.1. O valor global estimado deste contrato é de R$ xxxxxxx (xxxxxxxxx), para consecução da presente contratação pelo período de 36 (trinta e seis) meses, conforme tabela a seguir:

Item	CatSer	Descrição	Quant.	Métrica	Valor Unitário	Valor Total
01	393277	Appliance com capacidade para suportar um *throughput* mínimo de 12 Gb/s.	2	*Hardware*	R$	R$
02	27464	Licença de uso de *software* a ser utilizada no equipamento do Item 01, incluindo garantia, atualização de versões e suporte técnico por 36 meses.	2	*Software*	R$	R$

03	21172	Solução de Zero Trust Network Access (ZTNA) com capacidade para suportar 500 usuários.	2	Serviço	R$	R$
TOTAL						**R$**

CLÁUSULA QUARTA - DA DOTAÇÃO ORÇAMENTÁRIA

4.1. A despesa orçamentária para a contratação do objeto deste instrumento correrá a cargo das seguintes Contas Orçamentárias nº: 6.2.2.1.1.02.01.03.006 - Equipamentos de Processamento de Dados, 6.2.2.1.1.01.04.09.005 - Serviços de Informática e 6.2.2.1.1.01.04.09.011 - Serviços de Seleção e Treinamento de Pessoal, do Centro de Custo 3.3.02 - TI Atividades de Tecnologia da Informação.

4.2. Nos exercícios seguintes, as despesas correrão à conta de dotação orçamentária própria, consignada no respectivo Orçamento Anual, ficando o CONTRATANTE obrigado a apresentar, no início de cada exercício, a respectiva Nota de Empenho estimativa, e em havendo necessidade, emitir Nota de Empenho complementar, respeitada a mesma classificação orçamentária.

CLÁUSULA QUINTA - DO LOCAL DE EXECUÇÃO DO SERVIÇO

5.1. Os produtos/serviços deverão ser entregues/executados na sede do Confea, localizado no SEPN 508, Bloco A, Edifício Engenheiro Francisco Saturnino de Brito Filho, Asa Norte, Brasília – DF.

5.2. O deslocamento de prestador de serviço da CONTRATADA para o Confea não implicará, de nenhuma forma, o acréscimo ou majoração nos valores dos serviços, bem como nenhum tipo de pagamento correspondente a deslocamentos, diárias, horas-extras ou adicionais noturnos.

5.3. A definição do horário de trabalho para a execução das atividades nas instalações do Confea deve ser acordada entre o Confea e a Contratada.

5.4. Como padrão e quando não especificado em contrário, considerar-se-á como dia útil o período de 10 horas úteis, das 8h às 18h, de segunda a sexta-feira, nos dias em que houver expediente no Confea.

5.4.1. Considerar-se-á hora útil o intervalo de uma hora dentro de um dia útil.

5.5. Os serviços eventualmente realizados fora do horário de expediente, aos sábados, domingos e feriados, sejam no ambiente da CONTRATADA ou no ambiente do Confea, não implicarão nenhum acréscimo ou majoração nos valores pagos à CONTRATADA.

CLÁUSULA SEXTA - DO PRAZO DE VIGÊNCIA E DE EXECUÇÃO

6.1. O contrato terá vigência de **36 (trinta e seis) meses** contados da data da assinatura do contrato pelo CONTRATANTE, podendo ser prorrogado nos moldes da legislação vigente.

CLÁUSULA SÉTIMA - DO PAGAMENTO

7.1. Mediante a prestação dos serviços, após o aceite definitivo do documento Termo de Recebimento Definitivo, o pagamento será feito no prazo de **15 (quinze) dias úteis**, contado da data da atestação da nota fiscal/fatura.

7.1.1. O aceite dos serviços prestados por força desta contratação será feito mediante ateste das notas fiscais, correspondendo tão somente aos serviços efetivamente prestados.

7.1.2. O Confea não se responsabilizará pelo pagamento de quaisquer serviços realizados sem a solicitação ou autorização do fiscal do contrato.

7.2. O Confea efetivará a atestação da nota fiscal/fatura no prazo de **05 (cinco) dias úteis** contados do seu recebimento ou procederá à devolução quando aquela se encontrar em desacordo ao pactuado.

7.3. A nota fiscal/fatura, que será emitida sem rasura, legível, deverá ser acompanhada dos documentos que comprovem a sua regularidade fiscal, compreendendo FGTS, Receita Federal/ Estadual/ Municipal, Dívida Ativa da União, CNDT e demais documentos que se fizerem pertinentes às comprovações de regularidade.

7.4. A nota fiscal/fatura deverá ser emitida pela CONTRATADA e com o mesmo nº de CNPJ que originou a contratação, na qual constará o número do contrato e as informações para crédito em conta corrente.

7.5. No caso de incorreção nos documentos apresentados, 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, não respondendo o CONTRATANTE por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes.

7.5.1. Na hipótese de devolução, a documentação será considerada como não apresentada, para fins de atendimento das condições contratuais.

7.5.2. Na hipótese de que trata a cláusula anterior, o prazo para pagamento de que trata o **subitem 7.1.** se iniciará após a regularização ou reapresentação dos documentos.

7.6. O CONTRATANTE poderá deduzir do montante a pagar os valores correspondentes às multas ou indenizações devidas pela CONTRATADA, ou, ainda, glosar parte de serviços que não tenham sido executados, nos termos pactuados, garantido o contraditório e a ampla defesa.

7.7. Encontrando-se a CONTRATADA inadimplente na data da consulta, poderá ser concedido, a critério do CONTRATANTE, prazo de até 15 (quinze) dias para que a empresa regularize a sua situação, sob pena de, não o fazendo, ter o contrato rescindido com aplicação das sanções cabíveis.

7.8. O CONTRATANTE efetuará o pagamento somente para a empresa CONTRATADA, vedada a negociação dos documentos de cobrança com terceiros, ou a sua colocação em cobrança bancária.

7.9. Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido para tanto, fica convencionado que a taxa de compensação financeira devida pelo CONTRATANTE, entre a data acima referida e a correspondente ao efetivo adimplemento da parcela, serão calculados com a aplicação da seguinte fórmula:

EM = I x N x VP

Onde:

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 = 0,0001644, assim apurado:

$$I = \frac{(TX/100)}{365} \qquad I = \frac{(6/100)}{365} \qquad I = 0{,}0001644$$

TX = Percentual da taxa anual = 6%

7.10. A compensação financeira prevista nesta condição será incluída na fatura a ser apresentada posteriormente.

CLÁUSULA OITAVA - DAS OBRIGAÇÕES DO CONTRATANTE

8.1. O CONTRATANTE, além das obrigações estabelecidas nos anexos do edital do Pregão Eletrônico nº 18/2023, deve:

8.1.1. Fazer cumprir fielmente as cláusulas do contrato;

8.1.2. Proporcionar as facilidades indispensáveis à boa execução das obrigações contratuais;

8.1.3. Receber o objeto no prazo e condições estabelecidas no Edital e seus Anexos;

8.1.4. Designar fiscal para acompanhar e fiscalizar a execução do contrato;

8.1.5. Atestar a nota fiscal/fatura ou devolvê-la, em caso de desacordo ou por descumprimento ao pactuado, no prazo de **5 (cinco) dias úteis** após o seu recebimento e encaminhando para pagamento, desde que cumpridas todas as exigências pactuadas;

8.1.6. Efetuar o pagamento à CONTRATADA de acordo com as condições e prazos estabelecidos no instrumento contratual, desde que cumpridas todas às exigências pactuadas;

8.1.7. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

8.1.8. Notificar à CONTRATADA a ocorrência de serviços executados e/ou ausência destes que estiverem em desacordo com instrumento contratual;

8.1.9. Fiscalizar os documentos que comprovem a manutenção das condições de habilitação da CONTRATADA, solicitando os originais quando julgar necessário;

8.1.10. Permitir acesso dos empregados da CONTRATADA às suas dependências para a execução do serviço; e

8.1.11. Observar o cumprimento dos requisitos de qualificação profissional exigidos nas especificações técnicas e nas atribuições, solicitando à CONTRATADA as substituições e os treinamentos que se verificarem necessários**.**

CLÁUSULA NONA - DAS OBRIGAÇÕES DA CONTRATADA

9.1. A CONTRATADA além das obrigações estabelecidas nos anexos do edital do Pregão Eletrônico nº 18/2023, deve:

9.1.1. Cumprir e garantir o pleno cumprimento do instrumento de contrato, praticando as melhores técnicas administrativas e operacionais de mercado;

9.1.2. Observar as normas e regulamentos internos do CONTRATANTE, bem como fazer com que seus empregados os observem;

9.1.3. Selecionar e preparar rigorosamente os empregados que irão prestar os serviços, tendo funções profissionais legalmente registradas em suas carteiras de trabalho;

9.1.4. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato;

9.1.5. Responsabilizar-se por todas as obrigações trabalhistas de seus funcionários, tais como: salários; seguros; benefícios; encargos sociais e previdenciários; assistência médica e quaisquer outros, em decorrência de sua condição de empregadora, ficando o CONTRATANTE isento de qualquer vínculo empregatício;

9.1.6. Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho quando, em ocorrência da espécie, forem vítimas, os seus empregados ou prepostos alocados na execução dos serviços, ainda que verificados nas dependências do CONTRATANTE;

9.1.7. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

9.1.8. Indicar/designar preposto ou empregado para manter entendimento e/ou receber comunicações, solicitações ou transmiti-las ao CONTRATANTE;

9.1.9. Atender, por meio de preposto designado, as solicitações do contratante, prestando as informações referentes à prestação dos serviços, bem como as correções de eventuais irregularidades na execução do objeto contratado;

9.1.10. Providenciar a correção das deficiências apontadas pelo CONTRATANTE, no prazo de até **3 (três) dias úteis**, sob pena de aplicação de sanções;

9.1.11. Comunicar ao CONTRATANTE, por escrito, quando verificar condições inadequadas de execução dos serviços ou a iminência de fatos que possam prejudicar a sua execução;

9.1.12. Comunicar, por escrito, eventual atraso ou paralisação dos serviços, apresentando razões justificadoras que serão objeto de apreciação pelo CONTRATANTE;

9.1.13. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto e documento de interesse do CONTRATANTE, ou de terceiros, de que tomar conhecimento em razão da execução do objeto contratual, devendo orientar seus empregados a observar rigorosamente esta determinação;

9.1.14. Não reproduzir, divulgar ou utilizar em benefício próprio, ou de terceiros, quaisquer informações de que tenha tomado conhecimento em razão da execução dos serviços, sem consentimento, por escrito, do CONTRATANTE;

9.1.15. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato;

9.1.16. Prestar garantia em favor do CONTRATANTE no prazo de até **10 (dez) dias úteis**, contados da assinatura do instrumento contratual, correspondente a 5% (cinco por cento) do valor total do contrato, numa modalidades previstas na Lei nº 8.666, de 21 de junho de 1993;

9.1.16.1. A reposição do valor da garantia que vier a ser utilizado pelo CONTRATANTE deverá ocorrer no prazo máximo de **10 (dez) dias úteis**, contados da data da ciência à CONTRATADA;

CLÁUSULA DÉCIMA - DAS OBRIGAÇÕES GERAIS

10.1. A inadimplência da CONTRATADA não transferirá a responsabilidade pelo pagamento ao CONTRATANTE, tampouco onerará o objeto deste contrato, razão pela qual a CONTRATADA renuncia expressamente qualquer vínculo de solidariedade, ativa ou passiva, para com o CONTRATANTE.

10.2. Deverá a CONTRATADA observar que:

10.2.1. É expressamente proibida a veiculação de publicidade acerca do contrato, salvo se houver prévia autorização da Administração do Confea;

10.2.2. É expressamente proibida a contratação de colaborador pertencente ao quadro de pessoal do CONTRATANTE durante a vigência deste contrato; e

10.2.3. É expressamente proibida, sem a prévia anuência do CONTRATANTE, a transferência/subcontratação no todo ou em parte do objeto deste contrato.

CLÁUSULA DÉCIMA PRIMEIRA - DO REAJUSTE

11.1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data do orçamento a que a proposta se referir.

11.2. 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**, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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.

11.4. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

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.

11.5.1. 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.

11.6. Não será acatado pelo Confea o reajuste de preços no caso de atraso na execução decorrente de solicitação da CONTRATADA, mesmo que em decorrência de atraso de fornecimento de produtos pelo fabricante.

CLÁUSULA DÉCIMA SEGUNDA - DA GARANTIA DO CONTRATO

12.1. A CONTRATADA deverá apresentar à Administração do CONTRATANTE, no prazo máximo de 10 (dez) dias úteis, contado da data que a CONTRATADA recebeu a sua via do contrato assinada, comprovante de prestação de garantia de 5% (cinco por cento) sobre o valor anual do contrato, mediante a opção por uma das

seguintes modalidades:

12.1.1. caução em dinheiro ou títulos da dívida pública;

12.1.1.1. A garantia em apreço, quando em dinheiro, deverá ser efetuada na Caixa Econômica Federal, em conta específica, com correção monetária, em favor do Confea.

12.1.2. seguro-garantia; ou

12.1.3. fiança bancária.

12.2. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 5% (cinco por cento).

12.3. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover o bloqueio dos pagamentos devidos à CONTRATADA, até o limite de 5% (cinco por cento) do valor anual do contrato, a título de garantia.

12.4. O bloqueio efetuado com base no **subitem 12.3** desta cláusula não gera direito a nenhum tipo de compensação financeira à CONTRATADA.

12.5. A CONTRATADA, a qualquer tempo, poderá substituir o bloqueio efetuado com base no **subitem 12.3** desta cláusula por quaisquer das modalidades de garantia, caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

CLÁUSULA DÉCIMA TERCEIRA - DO CONTROLE E GESTÃO DA EXECUÇÃO DOS SERVIÇOS

13.1. A fiscalização do cumprimento das obrigações contratuais será exercida por empregados devidamente designados pelo CONTRATANTE, por meio de Portaria específica, nas funções de Gestor do Contrato, Fiscal Técnico, Fiscal Administrativo e Fiscal Requisitante, em conformidade com o art. 29 da Instrução Normativa nº 01/2019, da Secretaria de Governo Digital do Ministério da Economia.

13.2. A equipe de fiscalização do Contrato, atuando nos termos do artigo 31 a 38 da Instrução Normativa nº 01/2019, deverá acompanhar, fiscalizar, conferir e avaliar a execução do fornecimento/serviços, bem como dirimir e desembaraçar quaisquer dúvidas e pendências que surgirem, determinando medidas necessárias à regularização das faltas, falhas, problemas ou defeitos observados no curso do Contrato, e de tudo dará ciência diretamente à CONTRATADA, conforme artigo 67, parágrafos, da Lei n.º 8.666/1993 e suas alterações.

13.3. Para o caso de impedimento de qualquer dos empregados indicados para as funções de fiscalização, serão designados pelo CONTRATANTE servidores para atuar como substitutos.

13.4. Conforme previsto no artigo 31, inciso I, da Instrução Normativa nº 01/2019, cabe ao Gestor do Contrato a convocação para realização da reunião inicial, com a participação dos Fiscais Técnico, Requisitante e Administrativo do Contrato, da CONTRATADA e dos demais intervenientes por ele identificados, cuja pauta observará, pelo menos:

13.4.1. presença do representante legal da CONTRATADA, que apresentará o preposto;

13.4.2. entrega, por parte da CONTRATADA, do termo de compromisso e do termo de ciência, conforme art. 18, inciso V, da Instrução Normativa nº 01/2019; e

13.4.3. esclarecimentos relativos a questões operacionais, administrativas e de gestão do Contrato.

13.5. As faltas cometidas pela CONTRATADA deverão ser devidamente registradas no Processo de Execução pelo Gestor do Contrato, que deverá propor ao Ordenador de Despesas a aplicação das sanções que entender cabíveis para a regularização das faltas, nos termos do artigo 67, parágrafo 2.º e do artigo 87 da Lei n.º 8.666/1993.

13.6. Caberá à CONTRATADA o pronto atendimento às exigências inerentes ao objeto contratado, feitas pelo Gestor do Contrato ou por seu substituto.

13.7. A CONTRATADA é responsável pelos danos causados diretamente à Administração ou à terceiros, decorrentes de sua culpa ou dolo na execução do Contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento por parte do CONTRATANTE (art. 70 da Lei nº 8.666.1993 c/c art.9º da Lei nº 10.520/2002).

13.8. O CONTRATANTE se reserva o direito de rejeitar, no todo ou em parte, o serviço prestado em desacordo com o Contrato (art. 76 da Lei nº 8.666/93).

CLÁUSULA DÉCIMA QUARTA - DOS MECANISMOS FORMAIS DE COMUNICAÇÃO

14.1. Sempre que exigir-se, a comunicação entre o Gestor do Contrato e o Preposto da CONTRATADA deverá ser formal, considerando-se como documentos formais, além de documentos do tipo Ofício, as comunicações por correio eletrônico e/ou por *software* de gestão de contratos.

14.2. O Gestor do Contrato e o Preposto responderão sobre todas as questões sobre o Contrato a ser firmado, procurando solucionar todos os problemas que defrontarem, dentro dos limites legais e dentro da razoabilidade.

14.3. Caberá à CONTRATADA indicar formalmente o(s) e-mail(s) e telefone(s) de contato do(s) preposto(s) indicado(s), bem como o endereço de contato, quando da realização da reunião inicial.

14.3.1. Na mesma ocasião, o CONTRATANTE informará os contatos do Gestor e dos demais fiscais.

CLÁUSULA DÉCIMA QUINTA - DA PROTEÇÃO DE DADOS PESSOAIS

15.1. O CONTRATANTE e a CONTRATADA se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, garantindo que:

15.1.1. O tratamento de dados pessoais dar-se-á de acordo com as bases legais previstas nas hipóteses dos art. 7º e 11º da Lei 13.709/2018 às quais se submeterão os serviços, e para propósitos legítimos, específicos, explícitos e informados ao titular;

15.1.2. O tratamento seja limitado às atividades necessárias ao atingimento das finalidades de execução do contrato e do serviço contratado, utilizando-os, quando seja o caso, em cumprimento de obrigação legal ou regulatória, no exercício regular de direito, por determinação judicial ou por requisição da Autoridade Nacional de Proteção de Dados (ANPD);

15.1.3. Em caso de necessidade de coleta de dados pessoais indispensáveis à própria prestação do serviço, essa será realizada mediante prévia aprovação do CONTRATANTE, responsabilizando-se a CONTRATADA por obter o consentimento dos titulares (salvo nos casos em que opere outra hipótese legal de tratamento). Os dados assim coletados só poderão ser utilizados na execução dos serviços especificados neste Contrato e, em nenhuma hipótese, poderão ser compartilhados ou utilizados para outros fins;

15.1.4. Os sistemas operacionais que servirão de base para o armazenamento dos dados pessoais coletados deverão seguir um conjunto de premissas, políticas e especificações técnicas que regulamentam a utilização da tecnologia da informação e comunicação no Governo Federal;

15.1.5. Os dados obtidos em razão deste Contrato serão armazenados em um banco de dados seguro, com garantia de registro das transações realizadas na aplicação de acesso (log) e de adequado controle de acesso e com transparente identificação do perfil dos usuários, tudo estabelecido como forma de garantir a rastreabilidade de cada transação e a franca apuração, a qualquer momento, de desvios e falhas, vedado o compartilhamento desses dados com terceiros; e

15.1.6. Encerrada a vigência deste Contrato ou não havendo mais necessidade de utilização dos dados pessoais, sejam eles sensíveis ou não, a CONTRATADA interromperá o tratamento dos dados pessoais disponibilizados pelo CONTRATANTE e, em no máximo 30 (trinta) dias, sob instruções e na medida do determinado pelo CONTRATANTE, eliminará completamente os dados pessoais e todas as suas cópias porventura existentes (seja em formato digital ou físico), salvo se a CONTRATADA tiver que manter os dados para cumprimento de obrigação legal ou outra hipótese prevista na LGPD.

15.2. A CONTRATADA dará conhecimento formal aos seus empregados das obrigações e condições acordadas nesta subcláusula, inclusive no tocante à Política de Privacidade do CONTRATANTE, cujos princípios deverão ser aplicados à coleta e ao tratamento dos dados pessoais de que trata a presente cláusula.

15.3. O eventual acesso, pela CONTRATADA, às bases de dados que contenham ou possam conter dados pessoais ou segredos de negócio do CONTRATANTE implicará para a CONTRATADA e para os seus prepostos - devida e formalmente instruídos neste sentido - o mais absoluto dever de sigilo, no curso do presente Contrato e pelo prazo de até 10 (dez) anos contados de seu termo final.

15.4. A CONTRATADA cooperará com o CONTRATANTE no cumprimento das obrigações referentes ao exercício dos direitos dos titulares previstos na LGPD e nas leis e regulamentos de proteção de dados em vigor e no atendimento de requisições e determinações do Poder Judiciário, Ministério Público e Órgãos de Controle.

15.5. A CONTRATADA deverá informar imediatamente ao CONTRATANTE quando receber uma solicitação de um titular de dados a respeito de seus dados pessoais e abster-se de responder qualquer solicitação em relação aos dados pessoais do solicitante, exceto nas instruções documentadas do CONTRATANTE ou conforme exigido pela LGPD ou pelas leis e regulamentos de proteção de dados em vigor.

15.6. O Encarregado da CONTRATADA manterá contato formal com o Encarregado do CONTRATANTE no prazo de até 24 (vinte e quatro) horas da ocorrência de qualquer incidente que implique em violação ou risco de violação de dados pessoais, para que esse possa adotar as providências devidas.

15.7. A critério do Encarregado do CONTRATANTE, a CONTRATADA poderá ser provocada a colaborar na elaboração do Relatório de Impacto à Proteção de Dados (RIPD), conforme a sensibilidade e o risco inerente dos serviços objeto deste Contrato, no tocante a dados pessoais.

15.8. Eventuais responsabilidades das partes serão apuradas conforme estabelecido neste instrumento e de acordo com o que dispõe a Seção III, Capítulo VI da LGPD.

CLÁUSULA DÉCIMA SEXTA - DAS SANÇÕES ADMINISTRATIVAS

16.1. Com fundamento no artigo 7º da Lei nº 10.520, de 17 de julho de 2002, ficará impedida de licitar e contratar com o Confea e será descredenciada do Sicaf, pelo prazo de até 5 (cinco) anos, garantida a ampla defesa, sem prejuízo da rescisão unilateral do contrato e da aplicação de multa de até 30% (trinta por cento) sobre o valor total da contratação, a CONTRATADA que:

16.1.1. apresentar documentação falsa;

16.1.2. fraudar a execução do contrato;

16.1.3. comportar-se de modo inidôneo;

16.1.4. cometer fraude fiscal; ou

16.1.5. fizer declaração falsa.

16.2. Para os fins do **subitem 16.1.3**, reputar-se-ão inidôneos atos tais como os descritos nos artigos 92, parágrafo único, 96 e 97, parágrafo único, da Lei nº 8.666/1993.

16.3. Com fundamento nos artigos 86 e 87, incisos I a IV, da Lei nº 8.666/1993; e no art. 7º da Lei nº 10.520/2002, nos casos de retardamento ou de inexecução do objeto, garantida a ampla defesa, a CONTRATADA poderá ser apenada, isoladamente, ou juntamente com as multas definidas nos **subitens 16.4 e 16.5** abaixo, com as seguintes penalidades:

16.3.1. advertência;

16.3.2. suspensão temporária de participação em licitação e impedimento de contratar com a Administração do Confea, por prazo não superior a dois anos;

16.3.3. 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 Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior; ou

16.3.4. impedimento de licitar e contratar com a Administração Pública e descredenciamento no Sicaf, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/2002, pelo prazo de até cinco anos.

16.4. Em caso de inexecução parcial do objeto, a CONTRATADA fica sujeita à multa equivalente a 1% (um por cento) do valor unitário do bem em atraso, por dia, por unidade, até o limite de 20% (vinte por cento) do valor empenhado.

16.4.1.Considera-se inexecução parcial o atraso injustificado no prazo de entrega (para bens) ou no início da execução contratual (para serviços) até o limite de 20 (vinte) dias.

16.5. Em caso de inexecução total do objeto, a CONTRATADA fica sujeita à multa de, no máximo, 20% (vinte por cento) do valor do contrato.

16.5.1. Considera-se inexecução total o atraso injustificado no prazo de entrega (para bens) ou no início da execução contratual (para serviços) superior a 20 (vinte) dias.

16.6. O não-cumprimento de obrigação contratual acessória, a exemplo da garantia exigida na Cláusula 12ª (Garantia do contrato), sujeitará a CONTRATADA à multa de até 10% (dez por cento) do valor empenhado.

16.7. A falha na execução do contrato estará configurada quando a CONTRATADA se enquadrar em qualquer das situações previstas na tabela 2 do **subitem 16.8**, a seguir.

16.8. Pelo descumprimento das obrigações contratuais, a Administração aplicará multas conforme a graduação estabelecida nas tabelas seguintes:

Tabela nº 01	
GRAU	**CORRESPONDÊNCIA (%)**
01	10%
02	5%
03	3%

Tabela nº 02			
ITEM	**DETALHAMENTO DA INFRAÇÃO**	**GRAU**	**INCIDÊNCIA**
A	Não reparar, corrigir, remover, reconstruir ou substituir às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções, no prazo estipulado no Termo de Referência.	03	Por ocorrência
B	Fornecer produtos/serviços com especificação e qualidade diversa e/ou inferior a demandada.	03	Por produtos/serviços
C	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratados.	03	Por dia
D	Recusar a execução de serviço determinado pela fiscalização, sem motivo justificado.	02	Por ocorrência
E	Manter funcionário na execução dos serviços demandados sem a qualificação especificada no Termo de Referência e seus anexos	02	Por empregado e por dia

F	Destruir ou danificar documentos por culpa ou dolo de seus agentes.	02	Por ocorrência
G	Permitir situação que crie a possibilidade de causar ou que cause dano físico, lesão corporal ou consequências letais.	02	Por ocorrência
H	Não manter as condições de habilitação originárias da contratação.	02	Por ocorrência e por dia
I	Descumprir qualquer das obrigações contratuais previstas no Termo de Referência e seus anexos.	01	Por ocorrência
J	Não executar os serviços e/ou entregar os produtos conforme as especificações e as qualificações estabelecidas no Termo de Referência e seus anexos.	01	Por ocorrência e por dia
K	Não observar os prazos para execução dos serviços e/ou entrega de produtos.	01	Por ocorrência e por dia
L	Permitir a presença de empregado não uniformizado ou com uniforme manchado, sujo, mal apresentado e/ou sem crachá.	01	Por empregado e por ocorrência
M	Não fornecer os materiais e ferramentas necessários à completa execução do objeto.	01	Por item não fornecido
N	Não prestar as informações e os esclarecimentos que venham a ser solicitados.	01	Por ocorrência e por dia
O	Prestar serviços que não estejam em conformidade com as especificações técnicas previstas no Termo de Referência, no Contrato e/ou na proposta da Contratada	03	Por serviço

16.9. O valor da multa poderá ser descontado das faturas devidas à CONTRATADA.

16.9.1. Se o valor a ser pago à CONTRATADA não for suficiente para cobrir o valor da multa, a diferença será descontada da garantia contratual.

16.9.2. Se os valores das faturas e da garantia forem insuficientes, fica a contratada obrigada a recolher a importância devida no prazo de **15 (quinze) dias**, contado da comunicação oficial.

16.9.3. Esgotados os meios administrativos para cobrança do valor devido pela contratada ao contratante, aquela será encaminhada para inscrição em dívida ativa.

16.9.4. Caso o valor da garantia seja utilizado no todo ou em parte para o pagamento da multa, esta deve ser complementada no prazo de até **10 (dez) dias úteis**, contado da solicitação do CONTRATANTE.

16.10. O contrato, sem prejuízo das multas e demais cominações legais nele previstas, poderá ser rescindido unilateralmente, por ato formal da Administração, nos casos enumerados no art. 78, incisos I a XII e XVII, da Lei nº 8.666/1993.

16.11. Comprovado impedimento ou reconhecida força maior, devidamente justificado e aceito pela Administração do CONTRATANTE, em relação a(s) penalidade(s) aplicada(s) a CONTRATADA ficará isenta desta(s).

16.12. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa, observando-se o procedimento previsto na Lei nº 8.666/1993 e subsidiariamente na Lei nº 9.784, de 29 de janeiro de 1999.

16.13. Caberá ao Ordenador de Despesa, após o devido processo legal, garantido o contraditório e a ampla defesa, decidir pela aplicação da sanção administrativa cabível.

CLÁUSULA DÉCIMA SÉTIMA - DA RESCISÃO

17.1. A inexecução total ou parcial do contrato enseja a sua rescisão, conforme disposto nos arts. 77 a 80 da Lei nº 8.666, de 1993.

17.2. A rescisão do contrato poderá ser:

17.2.1. Determinada por ato unilateral e escrito da Administração do Confea, nos casos enumerados nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, notificando-se a CONTRATADA com a antecedência mínima de 30 (trinta) dias.

17.2.2. Amigável, por acordo entre as partes, reduzidas a termo no processo da licitação, desde que haja conveniência para a Administração do Confea.

17.2.3. Judicial, nos termos da legislação vigente sobre a matéria.

17.2.4. No caso de a CONTRATADA perder as condições de habilitação técnica e qualificação econômica exigidas para a celebração deste contrato.

17.2.5. No caso de as sanções contratuais previstas serem insuficientes para reparação do dano causado pela CONTRATADA ao erário.

17.3. A rescisão administrativa ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.

CLÁUSULA DÉCIMA OITAVA - DA VINCULAÇÃO AO EDITAL E À PROPOSTA DA CONTRATADA

É parte integrante deste Contrato, independente de sua transcrição, a integralidade do **Processo nº 00.003325/2023-49**, vinculado aos termos do **Pregão Eletrônico nº 18/2023**, cuja realização decorre da autorização da autoridade superior deste Conselho, e a proposta da CONTRATADA.

CLÁUSULA DÉCIMA NONA - DO AMPARO LEGAL

A lavratura do presente Contrato decorre da realização do **Pregão Eletrônico nº 18/2023** realizado com fundamento nas Leis nº 8.666, de 1993 e nº 10.520, de 2002.

CLÁUSULA VIGÉSIMA - DOS CASOS OMISSOS

Fica estabelecido que, caso venha a ocorrer algum fato não previsto neste contrato, no edital de **Pregão Eletrônico nº 18/2023** e seus anexos, os chamados casos omissos, estes serão resolvidos entre as partes, respeitado o objeto do contrato, a legislação e demais normas reguladoras da matéria, em especial a Lei nº 8.666, de 1993, aplicando-lhe, quando for o caso, supletivamente, os princípios da teoria geral dos contratos estabelecidos na legislação civil brasileira e às disposições do direito privado.

CLÁUSULA VIGÉSIM PRIMEIRA - DO FORO

As questões decorrentes da execução deste instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas na Seção Judiciária do Distrito Federal, com exclusão de qualquer outro por mais privilegiado que seja.

E, para firmeza e prova de assim haverem, entre si, ajustado e acordado, depois de lido, o presente Contrato é assinado eletronicamente pelas partes.