SERVIÇO PÚBLICO FEDERAL
CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA
SEPN 508, Bloco A Ed. Confea - Engenheiro Francisco Saturnino de Brito Filho - Bairro Asa Norte, Brasília/DF, CEP 70740-541
Telefone: 6121053700 - http://www.confea.org.br

EDITAL DE LICITAÇÃO

Processo nº 01407/2021

EDITAL DO PREGÃO ELETRÔNICO Nº 2/2022

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 388, de 06 de dezembro de 2021, 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 1/2019, 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: 18/02/2022

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 fornecimento de soluções de proteção avançada para *endpoints*, incorporando estações de trabalho e servidores, proteção para e-mail e rede corporativa, gerenciamento, orquestração e validação de segurança, mediante renovação dos produtos por *Part Number*, e fornecimento de soluções para segurança de acessos em nuvem e Microsoft 365, contando com implementação, configuração e transferência de conhecimento, para atender as necessidades Conselho Federal de Engenharia e Agronomia - Confea.

1.2. 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;

3.2.10. 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 **0,1% (zero vírgula um 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 IV - 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 ao Setor de Licitações e Contratos - Setac, 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.

9.11. Não serão aceitas propostas com valores unitários e globais superiores aos estimados pelo Confea.

9.12. Não serão aceitas propostas com preços manifestamente inexequíveis.

9.12.1. 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**.

9.12.2. 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:

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

9.12.2.2. Levantamento de informações junto aos órgãos públicos competentes;

9.12.2.3. Pesquisas em órgãos públicos ou empresas privadas;

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

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

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

9.12.2.7. Estudos setoriais;

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

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

9.12.2.10. Demais verificações que porventura se fizerem necessárias.

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

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

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

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

9.16. 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; e

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 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. Entender-se-á como compatível com o objeto pretendido o atestado que demonstre que a licitante executa ou executou contrato correspondente ao especificado no **Anexo I** deste edital;

10.12.1.2. Será admitido o somatório de atestados quando se referirem à execução de serviços similares e compatíveis, desde que prestados simultaneamente;

10.12.1.3. O(s) atestado(s) ou declaração(ões) de capacidade técnica deverá(ão) se referir a serviços prestados, no âmbito de sua atividade econômica principal e/ou secundária, especificada no contrato social, devidamente registrado na junta comercial competente, bem como no cadastro de pessoas jurídicas da Receita Federal do Brasil - RFB.

10.12.1.4. No caso de apresentação de atestado de empresas privadas, não serão considerados aqueles apresentados por empresas participantes do mesmo grupo empresarial da contratada. Serão consideradas como de mesmo grupo, empresas controladas pela contratada, ou que tenham pelo menos uma pessoa física ou jurídica que seja sócia da empresa emitente e da contratada.

10.12.2. Declaração, assinada pelo representante legal da licitante, de que possuirá, no momento da assinatura do contrato, profissional tecnicamente habilitado para responsabilizar-se pela execução de serviços de características semelhantes aos licitados.

10.12.3. 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 01, de 2019.**

10.12.4. Todos os atestados e declarações apresentados em língua estrangeira deverão ser autenticados pelos respectivos consulados e traduzidos por tradutor juramentado.

10.12.5. 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.

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

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

12.12.8. 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 ao Setor de Aquisições e Contratos - Setac, 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 14.1**, 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 Conta Orçamentária nº 6.2.2.1.1.01.04.09.005 **-** Serviços de Informática, do Centro de Custo 9.03.09.04 - SUINF 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 **12 (doze) 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 01407/2021** vinculado aos termos do **Pregão Eletrônico nº 2/2022,** 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 GTI nº 3/2022 (SEI nº 0557690)

Anexo II - Tabela Estimativa de Preços

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.

Documento assinado eletronicamente por **João de Carvalho Leite Neto**, **Chefe da Subprocuradoria Consultiva**, em 04/02/2022, às 16:25, 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 **Janaína Fonseca Araújo**, **Chefe do Setor de Aquisições e Contratos**, em 04/02/2022, às 16:48, 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 **0557684** e o código CRC **9E1B94F3**.

EDITAL DO PREGÃO ELETRÔNICO Nº 2/2022
ANEXO II - TABELA ESTIMATIVA DE PREÇOS

Para fins do que dispõe o Edital de Pregão Eletrônico nº 2/2022, serão considerados os seguintes **valores unitários e globais máximos:**

Item	*Part Number*	Descrição	Unid.	Quant.	Preço Unit.(R$)	Preço Total (R$)
1	EP-E-P-2W-PTM-499-1Y	Solução de proteção avançada para *endpoints*	Estações e servidores	335	371,24	124.365,40
2	EM-U-CA-2W-PTM-499-1Y	Solução para proteção avançada de e-mail corporativo	Usuários	385	123,37	47.497,45
3	NW-3500-HWSVR	Solução de segurança de rede avançada contra APTs	Dispositivos	1	270.111,00	270.111,00
4	HELIX-E-PTM-499-1Y	Solução de gerenciamento, orquestração e validação de segurança	Eventos por segundo (EPS)	350	732,00	256.200,00
5	N/A	Operação assistida	Meses	12	7.500,00	90.000,00
						788.173,85

EDITAL DO PREGÃO ELETRÔNICO Nº 2/2022
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 Contratação de empresa especializada na em fornecimento de soluções de proteção avançada para *endpoints*, incorporando estações de trabalho e servidores, proteção para e-mail e rede corporativa, gerenciamento, orquestração e validação de segurança, mediante renovação dos produtos por *Part Number*, e fornecimento de soluções para segurança de acessos em nuvem e

Microsoft 365, contando com implementação, configuração e transferência de conhecimento, 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.

ITEM	PART NUMBER	DESCRIÇÃO	UNIDADE	QUANT.	PREÇO UNIT.	PREÇO TOTAL
1	EP-E-P-2W-PTM-499-1Y	Solução de proteção avançada para *endpoints*	Estações e servidores	335	R$	R$
2	EM-U-CA-2W-PTM-499-1Y	Solução para proteção avançada de e-mail corporativo	Usuários	385		
3	NW-3500-HWSVR	Solução de segurança de rede avançada contra APTs	Dispositivos	1		
4	HELIX-E-PTM-499-1Y	Solução de gerenciamento, orquestração e validação de segurança	Eventos por segundo (EPS)	350		
5	N/A	Operação assistida	Meses	12		
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 2/2022

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/2021, 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 - DAS 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 2/2022

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 2/2022

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

1. Por este instrumento, atesto, para fins de cumprimento do disposto no art. 33, inciso I, da Instrução Normativa nº 1, de 4 de abril de 2019, emitida pelo Ministério da Economia/Secretaria Especial de

Desburocratização, Gestão e Governo Digital/Secretaria de Governo Digital, 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 pela Contratante.

2. Ressaltamos que o recebimento definitivo destes serviços e/ou bens ocorrerá em até 5 (cinco) dias úteis, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Contrato acima identificado.

EDITAL DO PREGÃO ELETRÔNICO Nº 2/2022

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 2/2022

ANEXO VIII - MINUTA DE CONTRATO

CONTRATO QUE ENTRE SI CELEBRAM O CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA (CONFEA) E A EMPRESA _____, CONFORME PROCESSO Nº 01407/2021.

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 Presidente, **Eng. Civ. Joel Krüger**, 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 2/2022** e a proposta apresentada pela **CONTRATADA**, constante do **Processo nº 01407/2021**, 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 fornecimento de soluções de proteção avançada para *endpoints*, incorporando estações de trabalho e servidores, proteção para e-mail e rede corporativa, gerenciamento, orquestração e validação de segurança, mediante renovação dos produtos por *Part Number*, e fornecimento de soluções para segurança de acessos em nuvem e Microsoft 365, contando com implementação, configuração e transferência de conhecimento, para atender as necessidades Conselho Federal de Engenharia e Agronomia - Confea, conforme especificações e condições constantes neste instrumento e no Edital de Pregão Eletrônico nº 2/2022 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

O valor global estimado deste contrato é de R$ xxxxxxx (xxxxxxxxx), para consecução da presente contratação pelo período de 12 (doze) meses, conforme tabela a seguir:

ITEM	PART NUMBER	DESCRIÇÃO	UNIDADE	QUANT.	PREÇO UNIT.	PREÇO TOTAL
1	EP-E-P-2W-PTM-499-1Y	Solução de proteção avançada para *endpoints*	Estações e servidores	335	R$	R$
2	EM-U-CA-2W-PTM-499-1Y	Solução para proteção avançada de e-mail corporativo	Usuários	385		
3	NW-3500-HWSVR	Solução de segurança de rede avançada contra APTs	Dispositivos	1		
4	HELIX-E-PTM-499-1Y	Solução de gerenciamento, orquestração e validação de segurança	Eventos por segundo (EPS)	350		

5	N/A	Operação assistida	Meses	12		
TOTAL						**R$**

CLÁUSULA QUARTA - DO REAJUSTE

4.1. Os preços dos serviços objeto deste contrato, desde que observado o interregno mínimo de 12 (doze) meses, contado da data limite para apresentação da proposta de preços pela licitante ou, nos reajustes subsequentes ao primeiro, da data de início dos efeitos financeiros do último reajuste ocorrido, poderão ser reajustados utilizando-se a variação do **ICTI - Índice de Custo da Tecnologia da Informação**, calculado pelo Ipea (Instituto de Pesquisa Econômica Aplicada) ou, em sua ausência ou inaplicabilidade, do IPCA - Índice Nacional de Preços ao Consumidor Amplo, mantido pelo IBGE (Instituto Brasileiro de Geografia e Estatística), acumulado em 12 (doze) meses, adotando-se a seguinte fórmula:

Fórmula de cálculo:

Pr = P + (P x V)

Onde:

Pr = preço reajustado, ou preço novo;

P = preço atual (antes do reajuste);

V = variação percentual obtida na forma do **item 11.1** desta cláusula, de modo que (P x V) significa o acréscimo ou decréscimo de preço decorrente do reajuste.

4.2. Os reajustes deverão ser precedidos de solicitação da CONTRATADA.

4.2.1. Caso a CONTRATADA não solicite tempestivamente o reajuste e prorrogue o contrato sem pleiteá-lo, ocorrerá a preclusão do direito.

4.2.2. Também ocorrerá a preclusão do direito ao reajuste se o pedido for formulado depois de extinto o contrato.

4.3. O reajuste terá seus efeitos financeiros iniciados a partir da data de aquisição do direito da CONTRATADA, nos termos do **item 4.1** desta cláusula.

4.4. O percentual final do reajuste não poderá ultrapassar o percentual limite de crescimento da despesa pública para o exercício, fixado nos termos do novo regime fiscal instituído pela Emenda Constitucional nº 95, de15/12/2016.

CLÁUSULA QUINTA - DA DOTAÇÃO ORÇAMENTÁRIA

5.1. A despesa orçamentária para a contratação do objeto deste instrumento correrá às Conta Orçamentária nº 6.2.2.1.1.01.04.09.005 - Serviços de Informática, do Centro de Custo 9.03.09.04 - SUINF Atividades de Tecnologia da Informação.

5.2. 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 SEXTA - DO LOCAL DE EXECUÇÃO DO SERVIÇO

6.1. Os produtos/serviços deverão ser entregues/executados com a previsão de 02 (dois) dias úteis após a assinatura do contrato para iniciar os serviços de configuração e 45 (quarenta e cinco) dias, após o início, para conclusão da implementação, na sede do Confea, localizado no SEPN 508, Bloco A, Edifício Engenheiro Francisco Saturnino de Brito Filho, Asa Norte, Brasília - DF.

6.2. 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.

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

6.4. Como padrão e quando não especificado em contrário, considerar-se-á como dia útil o período de 10 horas úteis, das 8h00 às 18h00, de segunda a sexta-feira, nos dias em que houver expediente no Confea.

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

6.5. 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 SÉTIMA - DO PRAZO DE VIGÊNCIA E DE EXECUÇÃO

O contrato terá vigência de **12 (doze) meses** contados da data da assinatura do contrato pelo CONTRATANTE, podendo ser prorrogado nos moldes da legislação vigente.

CLÁUSULA OITAVA - DO PAGAMENTO

8.1. Mediante a entrega dos produtos descritos nos **itens de 1 a 4,** o pagamento será feito em uma única vez, no prazo de **15 (quinze) dias úteis**, contado da data da atestação da nota fiscal/fatura.

8.2. Mediante a prestação dos serviços descritos no **item 5**, o pagamento será mensal para, no prazo de **15 (quinze) dias úteis**, contado da data da atestação da nota fiscal/fatura.

8.3. Serão adotados os documentos "Ordem de Serviço", "Termo de Recebimento Provisório" e "Termo de Recebimento Definitivo" para fins de pagamento.

8.4. 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.

8.5. A nota fiscal/fatura, que será emitida sem rasura, legível, deverá ser acompanhada dos documentos que comprovem a sua regularidade fiscal, compreendendo INSS, FGTS, Receita Federal/ Municipal, Dívida Ativa da União, CNDT e demais documentos que se fizerem pertinentes às comprovações de regularidade.

8.6. 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.

8.7. 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.

8.7.1. Na hipótese de devolução, a documentação será considerada como não apresentada, para fins de atendimento das condições contratuais.

8.7.2. Na hipótese de que trata a cláusula anterior, o prazo para pagamento de que trata a **subitem 8.1.** se iniciará após a regularização ou reapresentação dos documentos.

8.8. 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.

8.9. 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.

8.10. 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.

8.11. 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%

8.12. A compensação financeira prevista nesta condição será incluída na fatura a ser apresentada posteriormente.

CLÁUSULA NONA - DAS OBRIGAÇÕES DO CONTRATANTE

9.1. O CONTRATANTE, além das obrigações estabelecidas nos anexos do edital do Pregão Eletrônico nº 2/2022, deve:

9.1.1. Fazer cumprir fielmente as cláusulas do contrato;

9.1.2. Proporcionar as facilidades indispensáveis à boa execução das obrigações contratuais;

9.1.3. Receber o objeto no prazo e condições estabelecidas no Edital e seus Anexos;

9.1.4. Verificar minuciosamente, no prazo fixado, a conformidade dos serviços realizados provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimentos;

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

9.1.6. 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;

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

9.1.8. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

9.1.9. 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;

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

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

9.1.12. Permitir acesso dos empregados da CONTRATADA às suas dependências para a execução do serviço;

9.1.13. 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;

9.1.14. Anotar em registro próprio e notificar à CONTRATADA, por escrito, a ocorrência de eventuais imperfeições no curso de execução do serviço, fixando prazo para a sua correção.

CLÁUSULA DÉCIMA - DAS OBRIGAÇÕES DA CONTRATADA

9.1. A CONTRATADA além das obrigações estabelecidas nos anexos do edital do Pregão Eletrônico nº 2/2022, deve:

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

9.1.2. Observar as normas e regulamentos internos do CONTRATANTE, bem como fazer com que seus empregados os observem;

9.1.3. 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 modalidades previstas na Lei nº 8.666, de 21 de junho de 1993;

9.1.3.1. 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;

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

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

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. 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;

9.1.8. Manter seus empregados devidamente identificados por crachás, desde o primeiro dia de trabalho nas dependências do CONTRATANTE (será de inteira responsabilidade da CONTRATADA o cuidado na apresentação pessoal de seus empregados, inclusive as despesas com o fornecimento e troca periódica de uniformes);

9.1.9. Exercer controle sobre a assiduidade e a pontualidade de seus empregados, substituindo qualquer empregado no caso de falta, ausência legal ou férias, de maneira que não prejudique o andamento e a boa execução dos serviços;

9.1.10. A contratada deverá fornecer escala nominal de férias, licenças, ausências justificadas dos prestadores de serviço e os respectivos substitutos, bem como substituição de profissional;

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

9.1.12. 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;

9.1.13. Providenciar a correção das deficiências apontadas pelo contratante, no prazo de até **3 (três) dias úteis**, sob pena de aplicação de sanções;

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

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

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

9.1.17. 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;

9.1.18. 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

9.1.19. 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.

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 - DA GARANTIA DO CONTRATO

11.1. 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:

11.1.1. caução em dinheiro ou títulos da dívida pública;

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

11.1.2. seguro-garantia; ou

11.1.3. fiança bancária.

11.2. 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).

11.3. 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.

11.4. O bloqueio efetuado com base no **subitem 11.1.1.1.** desta cláusula não gera direito a nenhum tipo de compensação financeira à CONTRATADA.

11.5. A CONTRATADA, a qualquer tempo, poderá substituir o bloqueio efetuado com base no **subitem 11.1.1.1.** desta cláusula por quaisquer das modalidades de garantia, caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

11.6. O prazo de apresentação da garantia poderá ser prorrogado por igual período a critério do Confea.

CLÁUSULA DÉCIMA SEGUNDA - DO CONTROLE E GESTÃO DA EXECUÇÃO DOS SERVIÇOS

12.1. 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.

12.2. 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.

12.3. Para o caso de impedimento de qualquer dos empregados indicados para as funções de fiscalização, serão designados pelo CONTRATANTE servidores para atuar como substitutos.

12.4. 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:

12.4.1. presença do representante legal da CONTRATADA, que apresentará o preposto;

12.4.2. 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

12.4.3. esclarecimentos relativos a questões operacionais, administrativas e de gestão do Contrato.

12.5. 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.

12.6. Caberá à CONTRATADA o pronto atendimento às exigências inerentes ao objeto contratado, feitas pelo Gestor do Contrato ou por seu substituto.

12.7. 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).

12.8. 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 TERCEIRA - DOS MECANISMOS FORMAIS DE COMUNICAÇÃO

13.1. 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.

13.2. 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.

13.3. Caberá à CONTRATADA indicar formalmente o(s) email(s) e telefone(s) de contato do(s) preposto(s) indicado(s), bem como o endereço de contato, quando da realização da reunião inicial.

13.3.1. Na mesma ocasião, o CONTRATANTE informará os contatos do Gestor e dos demais fiscais.

13.4. A Ordem de Serviço é o instrumento formal pelo qual o Confea encaminha a demanda de serviço para a CONTRATADA.

13.5. 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.

13.6. As Ordens de Serviço serão emitidas, acompanhadas, revisadas e recebidas (aceitas) pelo Confea.

13.7. 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.

13.8. 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.

13.9. As Ordens de Serviço serão recebidas pelo Confea tanto em caráter provisório como em definitivo.

13.10. Do Termo de Recebimento Provisório do objeto e da avaliação de qualidade e conformidade.

13.10.1. 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 nº 01/2019: "**Termo de Recebimento Provisório** - declaração formal de que os serviços foram prestados ou os bens foram entregues, para posterior análise das conformidades e qualidades baseadas nos requisitos e nos critérios de aceitação, 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";

13.11. Após a execução dos serviços previstos para a Ordem de Serviço, será emitido o Termo de Recebimento Provisório no prazo de até **05 (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.

13.12. O recebimento provisório será realizado pelo fiscal técnico do contrato quando da entrega do objeto resultante de cada etapa de serviço. Após o aceite, consistirá na emissão do termo de recebimento provisório.

13.13. Os serviços entregues serão objeto de avaliação e aprovação pela equipe do Confea.

13.14. Será comunicada formalmente à CONTRATADA a não conformidade dos produtos.

13.15. Os bens 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.

13.16. 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.

13.17. Do Termo de Recebimento Definitivo.

13.17.1. 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 nº 01/2019: "**Termo de Recebimento Definitivo** - declaração formal de que os serviços prestados ou bens fornecidos atendem aos requisitos estabelecidos e aos critérios de aceitação, 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".

13.17.2. Concluída a avaliação da qualidade e da conformidade dos serviços/produtos e de sua entrega, o gestor do contrato efetuará o recebimento definitivo dos serviços por meio do termo de recebimento definitivo, com base nas informações da etapa de avaliação da qualidade, contendo a autorização para emissão de nota(s) fiscal(is), a ser encaminhado ao preposto da CONTRATADA.

13.17.3. No prazo de até **10 (dez) dias úteis**, contados do recebimento provisório, após a verificação da qualidade e quantidade do(s) bens constantes neste instrumento, o objeto será recebido definitivamente, a respectiva Nota Fiscal atestada e o processo encaminhado para pagamento.

13.17.4. 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.

13.17.5. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

13.18. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

13.19. 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.

13.20. A Ordem de Serviço poderá ser replanejada a qualquer momento a critério do Confea, sendo registrada formalmente tal ação.

13.21. 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.

CLÁUSULA DÉCIMA QUARTA - DA PROTEÇÃO DE DADOS PESSOAIS

14.1. 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:

14.1.1. 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;

14.1.2. 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);

14.1.3. 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 no CONTRATO ORIGINAL e, em nenhuma hipótese, poderão ser compartilhados ou utilizados para outros fins;

14.1.4. 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;

14.1.5. Os dados obtidos em razão do CONTRATO ORIGINAL 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

14.1.6. Encerrada a vigência do CONTRATO ORGINAL 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.

14.2. 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.

14.3. 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.

14.4. 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.

14.5. 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.

14.6. 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.

14.7. 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 do CONTRATO ORIGINAL, no tocante a dados pessoais.

14.8. 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 QUINTA - DAS SANÇÕES ADMINISTRATIVAS

15.1. 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:

15.1.1. apresentar documentação falsa;

15.1.2. fraudar a execução do contrato;

15.1.3. comportar-se de modo inidôneo;

15.1.4. cometer fraude fiscal; ou

15.1.5. fizer declaração falsa.

15.2. Para os fins do **subitem 15.1.3**, 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.

15.3. 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 15.4 e 15.5** abaixo, com as seguintes penalidades:

15.3.1. advertência;

15.3.2. suspensão temporária de participação em licitação e impedimento de contratar com a Administração do Confea, por prazo não superior a dois anos;

15.3.3. 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

15.3.4. 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.

15.4. 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.

15.4.1.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.

15.5. Em caso de inexecução total do objeto, a CONTRATADA fica sujeita à multa de, no máximo, 20% (vinte por cento) do valor do contrato.

15.5.1. 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.

15.6. A falha na execução do contrato estará configurada quando a CONTRATADA se enquadrar em qualquer das situações previstas na tabela 2 do **subitem 15.7**, a seguir.

15.7. 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 Edital e seus Anexos.	03	Por ocorrência

B	Fornecer produtos com especificação e qualidade diversa e/ou inferior a demandada.	03	Por produto
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	Destruir ou danificar documentos por culpa ou dolo de seus agentes.	02	Por ocorrência
F	Não manter as condições de habilitação originárias da contratação.	02	Por ocorrência
G	Descumprir qualquer das obrigações contratuais previstas no Edital e seus Anexos.	01	Por ocorrência
H	Não executar os serviços e/ou entregar os produtos conforme as especificações e as qualificações estabelecidas no Edital e seus Anexos.	01	Por ocorrência
I	Não observar os prazos para execução dos serviços e/ou entrega de produtos.	01	Por dia
J	Não fornecer os materiais e equipamentos, ferramentas e produtos necessários à completa execução do objeto.	01	Por ocorrência
K	Não prestar as informações e os esclarecimentos que venham a ser solicitados.	01	Por ocorrência
L	Não apresentar, quando solicitado, documentação fiscal, trabalhista, previdenciária e outros documentos necessários à habilitação.	01	Por ocorrência

15.8. O valor da multa poderá ser descontado das faturas devidas à CONTRATADA.

15.9. Se o valor a ser pago à contratada não for suficiente para cobrir o valor da multa, a diferença será descontada da garantia contratual.

15.9.1. Se os valores das faturas forem insuficientes, fica a CONTRATADA obrigada a recolher a importância devida no prazo de 15 (quinze) dias, contado da comunicação oficial.

15.9.2. Esgotados os meios administrativos para cobrança do valor devido pela CONTRATADA ao CONTRATANTE, aquela será encaminhada para inscrição em dívida ativa.

15.9.3. 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.

15.10. O contrato, sem prejuízo das multas e demais cominações legais 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.

15.11. 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).

15.12. 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.

15.13. 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 SEXTA - DA RESCISÃO

16.1. 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.

16.2. A rescisão do contrato poderá ser:

16.2.1. 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.

16.2.2. Amigável, por acordo entre as partes, reduzidas a termo no processo da licitação, desde que haja conveniência para a Administração do Confea.

16.2.3. Judicial, nos termos da legislação vigente sobre a matéria.

16.2.4. No caso de a CONTRATADA perder as condições de habilitação técnica e qualificação econômica exigidas para a celebração deste contrato.

16.2.5. No caso de as sanções contratuais previstas serem insuficientes para reparação do dano causado pela CONTRATADA ao erário.

16.3. A rescisão administrativa ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.

CLÁUSULA DÉCIMA SÉTIMA - DA VINCULAÇÃO AO EDITAL E À PROPOSTA DA CONTRATADA

É parte integrante deste Contrato, independente de sua transcrição, a integralidade do **Processo nº 01407/2021**, vinculado aos termos do **Pregão Eletrônico nº 2/2022**, cuja realização decorre da autorização da autoridade superior deste Conselho, e a proposta da CONTRATADA.

CLÁUSULA DÉCIMA OITAVA - DO AMPARO LEGAL

A lavratura do presente Contrato decorre da realização do **Pregão Eletrônico nº 2/2022** realizado com fundamento nas Leis nº 8.666, de 1993 e nº 10.520, de 2002.

CLÁUSULA DECIMA NONA - DOS CASOS OMISSOS

Fica estabelecido que, caso venha a ocorrer algum fato não previsto neste contrato, no edital de **Pregão Eletrônico nº 2/2022** 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 VIGÉSIMA - 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.

SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA – Confea

TERMO DE REFERÊNCIA/PROJETO BÁSICO GTI Nº 3/2022

Processo: CF-01407/2021

Tipo de Processo: Gestão de TI: Planos e Projetos

Assunto: Aquisição de Licenciamento para Solução de Segurança Corporativa

Interessado: Gerência de Tecnologia da Informação

1. **DEFINIÇÃO DO OBJETO**

1.1. Contratação de empresa especializada em fornecimento de soluções de proteção avançada para endpoints, incorporando estações de trabalho e servidores, proteção para e-mail e rede corporativa, gerenciamento, orquestração e validação de segurança, mediante renovação dos produtos por Part Number, em concordância com todas as especificações técnicas contidas neste Termo de Referência e anexos relacionados, para atender as necessidades Conselho Federal de Engenharia e Agronomia – Confea, sediado em Brasília – DF.

2. **CATMAT OU CATSER**

2.1. Consoante artigo 12 da Instrução Normativa nº 1, de 4 de abril de 2019, "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. O código mais aproximado é o CatMat de nº 350949 ("software", aplicação: informática, tipo: client server suite, características adicionais: antivírus corporativo, atualização contínua e su-).

3. **DESCRIÇÃO DA SOLUÇÃO**

3.1. Os objetos alvos desta possível contratação contam com subscrição para utilização de softwares de segurança da informação, atendendo todas as especificações técnicas que ainda serão listadas. Segue abaixo o descritivo de cada item esperado:

3.1.1. **Solução de proteção avançada para endpoints**, renovação da solução de proteção para endpoints da FireEye, em uso atualmente, de forma a manter as estações de trabalho e servidores protegidos contra os mais diversos tipos de ameaças, através das tecnologias de antivírus, anti-malware, anti-spyware e EDR.

3.1.2. **Solução para proteção avançada de e-mail corporativo**, renovação da solução de proteção para e-mail corporativo, em uso atualmente, de forma a manter o ambiente protegido contra spams e ameaças avançadas enviadas por e-mail, através das tecnologias de antispam, antimalware, análise avançada de links maliciosos, análise avançada de domínios que se comunicam com o CONFEA via e-mail e sandbox para análise de anexos maliciosos.

3.1.3. **Solução de segurança de rede avançada contra APTs**, tem como objetivo criar meios de proteção contra ameaças simples e avançadas para todos os ativos e usuários do CONFEA, sem precisar de um agente instalado, por meio de conexão direta à rede corporativa, através da tecnologia NX da FireEye.

3.1.4. **Solução de gerenciamento, orquestração e validação de segurança**, tem como objetivo renovar a solução FireEye Helix, em uso atualmente, trabalhando a solução como um ponto central de convergência entre todas a plataformas de segurança e infraestrutura, através da coleta e correlacionamento de logs e/ou eventos de segurança, redes ou infraestrutura e também automação de tarefas de resposta e validação de segurança. Tal solução deverá disponibilizar um framework para resposta de todos os incidentes de segurança direcionados ao CONFEA.

3.1.5. **Solução de gerenciamento de usuário remoto**, tem como objetivo prover meios para facilitar, controlar e proteger de forma eficaz todos os acessos remotos direcionados a rede do CONFEA. Tal solução deverá proteger tantos os acessos de teletrabalho quanto os acessos administrativos voltados para manutenções ou acompanhamentos tecnológicos.

3.1.6. **Solução para acesso remoto seguro**, deve permitir meios seguros para que usuários de teletrabalho acessem componentes internos necessários para realização de suas atividades, sem a necessidade de VPN, reduzindo a exposição de serviços a redes e dispositivos sem os mesmos critérios de proteção utilizados internamente.

3.1.7. **Solução de acesso a aplicações em nuvem**, deve estabelecer controles efetivos para controle na utilização de aplicativos de nuvem, como o Microsoft 365, Microsoft One drive, Microsoft Teams, etc. Tal solução irá trabalhar para gerar a visibilidade necessária para todo o tráfego e utilização de aplicações em nuvem, permitindo também controlar e proteger esses meios que são cada vez mais utilizados pelos usuários.

3.1.8. **Solução de gerenciamento, acesso e prevenção contra vazamento de dados em nuvem**, deve ampliar a camada de proteção de dados atual do CONFEA, permitindo o controle de vazamento de informações sensíveis sejam de usuários de dentro da empresa ou em teletrabalho.

3.2. Bens e Serviços que compõem a solução

ITEM	Part Number	DESCRIÇÃO	UNIDADE	QTD
1	EP-E-P-2W-PTM-499-1Y	Solução de proteção avançada para endpoints	Estações e servidores	335
2	EM-U-CA-2W-PTM-499-1Y	Solução para proteção avançada de e-mail corporativo	Usuários	385

ITEM	Part Number	DESCRIÇÃO	UNIDADE	QTD
3	NW-3500-HWSVR	Solução de segurança de rede avançada contra APTs	Dispositivos	1
4	HELIX-E-PTM-499-1Y	Solução de gerenciamento, orquestração e validação de segurança	Eventos por segundo (EPS)	350
5	N/A	Operação assistida	Meses	12

4. **JUSTIFICATIVA PARA A CONTRATAÇÃO/AQUISIÇÃO**

4.1. Para alcançar a sua missão, o CONFEA conta com mais de 200 empregados públicos e funcionários terceirizados. As atividades de todas as áreas do CONFEA dependem diretamente do uso das facilidades proporcionadas por recursos tecnológicos cada vez mais essenciais ao desenvolvimento de suas funções. Sendo assim, torna-se imprescindível a existência de serviços continuados com o quantitativo de pessoal suficiente e capacitado para garantir a continuidade e o adequado funcionamento dos serviços de atendimento e suporte às demandas de TI dos usuários.

4.2. De acordo com orientações do governo, o cenário atual de guerra cibernética em que o mundo se encontra e também necessidades específicas de proteção de informações desencadeadas pelos mais diversos serviços tecnológicos ofertados pelo CONFEA, a contratação em questão visa contar com serviços/soluções de eficiência comprovada, com integração eficiente entre os demais itens tecnológicos já contratados (Estendendo também para contratações futuras) e continuidade no gerenciamento de alertas e mitigação de eventos de segurança.

4.3. A contratação em questão envolve itens ligados a ampliação do nível de maturidade do CONFEA, mantendo e estabelecendo itens que são considerados a base e a linha de frente da organização para combate as mais diversas atividades maliciosas que dia após dia serão monitoradas e devidamente combatidas.

4.4. Os itens descritos na contratação também colocam o CONFEA no caminho em direção ao atendimento da estratégia nacional de segurança cibernética (Decreto 10.222, de 5 de fevereiro de 2020) e a possibilidade de não podermos contar com as soluções, afastam o CONFEA de objetivos e necessidades internas, também alinhadas ao governo federal. Segue abaixo apenas um trecho introdutório do decreto citado, que está sendo utilizado como base para planejamento de algumas atividades relacionadas à segurança cibernética:

4.5. DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020 que introduz a estratégia nacional de segurança cibernética:

> *"A revolução digital está transformando profundamente nossa sociedade. Nas últimas duas décadas, bilhões de pessoas se beneficiaram do crescimento exponencial do acesso à internet, da rápida adoção dos recursos de tecnologia da informação e comunicação, e das oportunidades econômicas e sociais oriundas do ambiente digital.*
>
> *Os rápidos avanços na área de tecnologia da informação e comunicação resultaram no uso intenso do espaço cibernético para as mais variadas atividades, inclusive a oferta de serviços por parte do Governo federal, em coerência com as tendências globais. Entretanto, novas e crescentes ameaças cibernéticas surgem na mesma proporção, e colocam em risco a administração pública e a sociedade.*
>
> *Desse modo, proteger o espaço cibernético requer visão atenta e liderança para gerenciar mudanças contínuas, políticas, tecnológicas, educacionais, legais e internacionais. Nesse sentido, o Governo, a indústria, a academia e a sociedade em geral devem incentivar a inovação tecnológica e a adoção de tecnologias de ponta, e manter constante atenção à segurança nacional, à economia e à livre expressão.*
>
> *Em nível superior aos debates sobre a segurança no espaço cibernético está a Segurança da Informação, área sistêmica, e diretamente relacionada à proteção de um conjunto de informações e ao valor que estas possuem para um indivíduo ou para uma organização. Desse modo, segundo o art. 2º do Decreto nº 9.637, de 2018, a Segurança da Informação abrange a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais, e tem como princípios fundamentais a confidencialidade, a integridade, a disponibilidade e a autenticidade.*
>
> *Entende-se que os recursos tecnológicos empregados na segurança sistêmica devem apoiar políticas que garantam os princípios fundamentais da autenticidade e da integridade dos dados, e prover mecanismos para proteção da legitimidade contra sua alteração ou eliminação não autorizada. Do mesmo modo, as informações coletadas, processadas e armazenadas na infraestrutura de tecnologia da informação e comunicação devem ser acessíveis apenas a pessoas, a processos ou a entidades autorizadas, a fim de garantir a confidencialidade das informações. Adicionalmente, os recursos de tecnologia da informação e comunicação devem prover disponibilidade permanente e apoiar de forma contínua todos os acessos autorizados.*
>
> *A E-Ciber, além de preencher importante lacuna no arcabouço normativo nacional sobre segurança cibernética, estabelece ações com vistas a modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento de instituições e de indivíduos sobre o assunto. Em primeiro lugar, verifica-se que há boas iniciativas gerenciais nessa área, entretanto, mostram-se fragmentadas e pontuais, o que dificulta a convergência de esforços no setor. Em segundo, nota-se a falta de um alinhamento normativo, estratégico e operacional, o que frequentemente gera retrabalho ou resulta na constituição de forças-tarefas para ações pontuais, que prejudicam a absorção de lições aprendidas e colocam em risco a eficácia prolongada dessas ações. Em terceiro, vê-se a existência de diferentes níveis de maturidade da sociedade em segurança cibernética, o que resulta em percepções variadas sobre a real importância do tema.*
>
> *Após a presente parte introdutória, discorre-se sobre a metodologia adotada nas linhas de análise, que tiveram por base o estudo de dois conjuntos de eixos temáticos: os de proteção e segurança, e os denominados transformadores. Aborda-se, ainda, como os subgrupos de trabalho se estruturaram, de acordo com os temas propostos.*
>
> *Na Parte I, apresenta-se um diagnóstico da segurança cibernética, baseado no cenário internacional e o no cenário nacional, com especial atenção às ameaças, aos ataques e às vulnerabilidades cibernéticas, e ao modo como esses elementos impactam a sociedade e as instituições.*
>
> *Os eixos temáticos são apresentados separadamente na Parte II. Primeiro, abordam-se os relativos à proteção e à segurança: governança da Segurança cibernética nacional, o universo conectado e seguro e a proteção estratégica. Depois, analisam-se aqueles que, por sua natureza, são chamados de Transformadores: a dimensão normativa; a pesquisa, desenvolvimento e inovação; a dimensão internacional e parcerias estratégicas; e a educação.*
>
> *Em virtude da análise diagnóstica e do estudo dos eixos temáticos, apresentam-se os objetivos estratégicos e, em seguida, as ações estratégicas, elaboradas com o fim de atingir os objetivos especificados. Por meio dessas ações, para cuja realização recomenda-se a elaboração de planos, apontam-se valiosas direções, capazes de conduzir a sociedade e as instituições a um ambiente próspero, resiliente e seguro, como condição ideal para o crescimento econômico e para o desenvolvimento social.*
>
> *Por fim, é importante ressaltar que no decorrer da apresentação da Estratégia são mencionados diversos termos relacionados não apenas à segurança cibernética, mas também ao grande campo de estudos da segurança da informação. Com o propósito de esclarecê-los, caso necessário, recomenda-se a consulta ao Glossário de Segurança da Informação, publicado pela Portaria nº 93, de 26 de setembro de 2019, do Gabinete de Segurança Institucional da Presidência da República.*
>
> *Em decorrência da presente Estratégia, recomenda-se que cada órgão do setor público e do setor privado, planeje e realize gestões no sentido de colocar em prática os aspectos que lhe cabem e que estão estabelecidos nas ações estratégicas, em um esforço conjunto e dedicado, em prol do pleno alcance dos objetivos estratégicos do País, no crítico e atual tema da segurança cibernética nacional."*

4.6. Como é de conhecimento de todos, o governo vem sofrendo muitos ataques cibernéticos nos últimos anos, como:

4.6.1. STJ – Superior Tribunal de Justiça (https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04112020-Em-razao-de-ataque-cibernetico--STJ-funcionara-em-regime-de-plantao-ate-o-dia-9.aspx);

4.6.2. CNJ – Conselho Nacional de Justiça (https://www.conjur.com.br/2019-abr-01/cnj-sofre-ataque-hacker-dados-milhares-pessoas-vazam),

4.6.3. Ministério da saúde (https://www.poder360.com.br/governo/ministerio-da-saude-identifica-virus-na-rede-do-datasus/),

4.6.4. GDF (https://g1.globo.com/df/distrito-federal/noticia/2020/11/05/governo-do-df-tira-sistemas-online-do-ar-apos-ataque-hacker.ghtml) e ;

4.6.5. TJ-RS (https://g1.globo.com/rs/rio-grande-do-sul/noticia/2021/05/06/nove-dias-apos-ataque-cibernetico-tj-rs-ainda-enfrenta-dificuldades-para-acessar-processos.ghtml).

4.7. Alguns dos ataques supracitados, também conhecidos como ataques de “ransomware”, tem como característica explorar vulnerabilidades na estrutura computacional do datacenter, infiltrar softwares maliciosos nas estações de trabalho e servidores de rede com objetivo de “sequestrar” os dados dos sistemas de armazenamento (local ou compartilhado).

4.8. Tais evidências reforçam a afirmação da eficiência das plataformas em uso atualmente no CONFEA, uma vez que a casa não foi atingida.

4.9. Portanto, o processo visa além de renovar as soluções atuais, ampliar o nível de proteções voltadas para nuvem, uma vez que o CONFEA já trabalha atualmente com serviços de nuvem da Microsoft.

5. ESPECIFICAÇÕES DOS REQUISITOS DA CONTRATAÇÃO

5.1. Aquisição/renovação de solução de segurança integrada para ambiente corporativo, em compliance com o DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020 (E-Ciber), baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento.

5.2. Com o fornecimento da solução suportada por fabricantes distintos, a integração com os módulos de segurança já adquiridos pelo CONFEA deverá ser documentada, homologada e implementada, sem custo adicional.

5.3. Fazem parte da contratação, para a qual se destina este edital, visando a efetiva operacionalização e funcionamento da solução por completo os seguintes itens:

5.3.1. Implantação da solução;

5.3.2. Configuração;

5.3.3. Garantia e suporte;

5.3.4. Transferência de conhecimento.

5.4. **Item 1 - Solução de proteção avançada para endpoints**

5.5. **Requerimentos Gerais da Solução**

5.5.1. A solução oferecida deve ser independente de qualquer outra solução de segurança implementada ou a ser implementada. Todos os recursos necessários devem ser fornecidos na contratação.

5.5.2. A solução deve permitir realização de backup local e externo não limitando-se a Mídias externas como USB, SCP, FTP ou qualquer outro armazenamento disponível que não esteja diretamente ligado a solução. A solução deve ainda permitir restauração das configurações independentemente do tipo de backup realizado.

5.5.3. Deve possuir capacidade de ser fornecido em modelo appliance.

5.5.4. Deve possuir capacidade de ser fornecido em modelo virtual-appliance, compatível com VMWARE ou Hyper-V.

5.5.5. Sistema operacional da solução deve ser disponibilizado como “pre-hardened”, com limitação dos serviços em uso, ampliando a segurança da plataforma, facilitando a implementação dos componentes necessários e permitindo apenas a execução dos componentes estritamente necessários para funcionamento da plataforma.

5.5.6. O banco de dados da plataforma deve ser entregue junto ao appliance/virtual-appliance ou caso não seja possível, a contratada deve fornecer a licença do mesmo para funcionamento.

5.5.7. A solução deve atender aos requisitos para instalação On-premises e, no caso de utilização do hardware do próprio fabricante (Appliance), os componentes da solução devem fornecer redundância em suas fontes, ventiladores e discos.

5.5.8. No caso de utilização de hardware, o mesmo deve possuir a capacidade de ser gerenciado através de uma interface do tipo serial, de onde os parâmetros básicos do equipamento podem ser configurados, evitando o uso de um console de gerenciamento externo para sua configuração inicial.

5.5.9. A solução deve permitir controle de acesso a plataforma de forma granular, restringindo o acesso apenas para quem está autorizado. Oferecendo também como opção a utilização de algum protocolo de autenticação para administração do produto, não se limitando apenas a RADIUS, TACACS+ ou LDAP. Assim como também, deve suportar a utilização de usuários locais.

5.5.10. Todos os dispositivos (Incluindo os demais itens do tópico 3.2) devem suportar o gerenciamento através de uma console centralizada onde deve-se configurar as políticas e outras configurações para melhor utilização do produto. Está console de gerência unificada deve suportar minimamente os seguintes itens:

5.5.10.1. Permitir o download dos indicadores de comprometimento em alguns dos seguintes formatos CSV, STIX, JSON ou XML;

5.5.10.2. Deve permitir gerar alertas das soluções integradas;

5.5.10.3. Permitir a exportação dos alertas através da própria console;

5.5.10.4. Permitir o agendamento de novos relatórios diariamente, semanalmente, mensalmente ou em período customizado;

5.5.10.5. Deve permitir e possuir APIs para facilitar a integração de outras soluções;

5.5.10.6. Receber os índices de comprometimento de todas as soluções integradas (Endpoint, antiAPT de rede e AntiSpam) e realizar trocas transparentes entre as mesmas, permitindo que uma detecção em um dos vetores, automaticamente seja implementada nas demais soluções, sem a necessidade de download de uma vacina ou novo pacote de inteligência;

5.5.10.7. Permitir bloqueio de artefatos com apenas uma única ação para todas as soluções do tópico 3.2;

5.5.10.8. Configurar regras YARA e\ou SNORT.

5.5.11. Todos os dispositivos devem suportar o uso de certificados assinados ou não para comunicação dos agentes. Assim como, se faz necessário a utilização de certificados para acesso a console WEB através de protocolos seguros como HTTPS.

5.5.12. Deve implementar a tecnologia de EDR (Endpoint Detection and Response) nos endpoints sem a necessidade de nenhum agente adicional.

5.5.13. A solução completa deve utilizar um único agente, incluindo todas as funcionalidades (Antivírus, Anti-Malware, EDR, etc.).

5.5.14. A implementação das funcionalidades de EDR não devem requerer a utilização de nenhuma console adicional.

5.5.15. Todos os agentes devem suportar a visualização de dados como:

5.5.15.1. Nome do usuário logado;

5.5.15.2. Nome do host;

5.5.15.3. Informações de sistema operacional (Build, Plataforma etc.);

5.5.15.4. Estado do equipamento (Online ou Offline);

5.5.15.5. Última data comunicação com a console de gerenciamento;

5.5.15.6. Informações relacionadas à rede (IP, DNS, DHCP etc.);

5.5.15.7. Timezone;

5.5.15.8. Versão do agente e todos os componentes;

5.5.15.9. Versão das definições de detecção;

5.5.15.10. Quantidade de armazenamento livre.

5.5.16. Os usuários locais da plataforma devem ter uma política de senha que permita, no mínimo as seguintes configurações:

5.5.16.1. Alteração de senha após primeiro login;

5.5.16.2. Definição do período de expiração da senha;

5.5.16.3. Número mínimo e máximo de caracteres aos quais devem incluir letras maiúsculas, minúsculas e números;

5.5.16.4. Evitar repetição de senha em curto período.

5.5.17. A solução deve permitir ainda além do acesso a console Web o acesso direto através do servidor, para execução de comandos e tarefas administrativas.

5.5.18. A solução deve permitir a criação de usuários com perfis para, no mínimo:

5.5.18.1. Administrador (sysadmin);

5.5.18.2. Administrador limitado;

5.5.18.3. Usuários de monitoramento;

5.5.18.4. Usuários de API.

5.5.19. A solução deve possuir de forma bem documentada suas APIs públicas, as quais podem ser utilizadas para futuras integrações.

5.5.20. A solução deve possuir tecnologias de proteção contra ameaças avançadas e gerar alertas quando elas forem detectadas no ambiente.

5.5.21. A solução deve possuir capacidade para responder de forma efetiva durante as investigações realizadas pelo time de operações ou de resposta a incidente, provendo através de sua console centralizada capacidades para coleta de artefatos, análise de processos, isolamento de equipamentos, recursos para forense e etc.

5.5.22. A solução deve fornecer visibilidade abrangente que permitirá às equipes de segurança procurar, identificar e discernir rapidamente o nível de ameaças detectadas, além de possuir recursos de detecção e resposta para identificar, investigar e conter equipamentos de forma rápida e agilizar a resposta.

5.5.23. A solução deve possuir um console de gerenciamento centralizado para todos os agentes implantados.

5.5.24. O console de gerenciamento centralizado de terminais deve ter pelo menos as seguintes funcionalidades:

5.5.24.1. Permitir definir e gerenciar grupos de dispositivos, que devem ser definidos de forma estática ou por meio de um filtro lógico, com base nas características dos dispositivos que suportam a criação de combinações lógicas;

5.5.24.2. Deve permitir a atualização automática de versão de todos os agentes, sem exigir a intervenção do operador ou usuário do dispositivo;

5.5.24.3. A solução deve ser capaz de detectar agentes duplicados ou inativos;

5.5.24.4. Deve fornecer acesso seguro ao console por meio de uma interface web HTTPS;

5.5.24.5. Deve gerenciar alertas antigos, permitindo a exclusão automática e\ou envio de alertas aos administradores;

5.5.24.6. Deve gerenciar o espaço em disco disponível para capturas de dados para análise forense, definindo limites de uso;

5.5.24.7. O painel de controle da solução (dashboard) deve exibir pelo menos as seguintes métricas de detecção e contenção: Número de terminais com alertas, número total de alertas, número de indicadores separados por fonte de inteligência, número de coletas classificadas por estado e número de terminais em status de contenção / isolamento;

5.5.24.8. Todas as informações forenses geradas pelo equipamento devem poder ser analisadas no mesmo console, sem ter que acessar outro software adicional;

5.5.24.9. A solução deve poder enviar alertas por e-mail e HTTP/HTTPS para, no mínimo, os seguintes eventos:

5.5.24.10. Indicador de presença de malware;

5.5.24.11. Indicações de execução de malware;

5.5.24.12. Bloqueio de exploração;

5.5.24.13. Detecção de exploração.

5.5.24.14. O dashboard deve exibir pelo menos o número total de equipamentos monitorados e o número de equipamentos ativos por período. O período para a detecção de terminais ativos deve ser personalizável;

5.5.24.15. O console deve oferecer todas as versões de agentes disponíveis;

5.5.24.16. Todas as atualizações do agente devem ser feitas exclusivamente no console central;

5.5.24.17. A frequência de atualização dos agentes no console central deve ser de pelo menos 5 minutos;

5.5.24.18. A frequência de atualização dos indicadores de comprometimento dos agentes no console central devem ser pelo menos a cada 60 segundos.

5.5.25. Caso existam agentes duplicados, a solução deverá criar um alerta e permitir a resolução do problema através de ações executadas no console de gerenciamento.

5.6. **Requerimentos gerais do agente**

5.6.1. A solução deve possuir capacidade de ser instalada sem requerer nenhuma licença adicional de sistema operacional ou qualquer outra não fornecida pela contratada.

5.6.2. Uma solução baseada em agente deve ser fornecida para a proteção de ameaças de dia zero em ameaças que não utilizam assinaturas ou padrões como a principal forma de detecção e bloqueio de ameaças.

5.6.3. A solução deve operar em tempo real, monitorando e bloqueando as ameaças.

5.6.4. A solução deve detectar e bloquear tentativas de exploração por malware conhecido ou desconhecido, usando técnicas de análise de comportamento na interação entre componentes.

5.6.5. A solução deve fornecer a capacidade de executar análises forenses de estações de trabalho/servidores sem a necessidade de interagir com o usuário. Essa capacidade deve ser centralizada e transparente para o usuário.

5.6.6. A solução deve fornecer a opção de análise investigativa e\ou forense em sua própria console de gerenciamento.

5.6.7. A solução deve fornecer suporte para estações de trabalho que não estão conectadas à rede interna, como computadores na Internet, sem perder a capacidade de proteger, atualizar e ainda realizar análises forenses.

5.6.8. Para gerenciamento de equipamentos fora da rede, a solução on-premise deve possuir um equipamento ou software específico para estes casos, sem utilizar-se do mesmo hardware ou software implementado para proteção de equipamentos na rede interna. Como por exemplo, um recurso criado para trabalhar especificamente em DMZ.

5.6.9. Deve incluir recursos para detecção de malware conhecido, incluindo a capacidade de operar em conjunto com outras ferramentas de proteção a estações de trabalho.

5.6.10. A solução deve ter a capacidade de detectar metodologias e padrões de ataques, mesmo sem a presença de arquivos de malware (malware operando apenas na memória\fileless).

5.6.11. No caso de detecção um incidente, a solução deve permitir a execução de rotinas automatizadas para rapidamente responder aos eventos gerados pelos dispositivos.

5.6.12. A solução deve poder integrar-se automaticamente com outros equipamentos de proteção anti-malware, a fim de criar indicadores de comprometimento com base nas detecções feitas na navegação (rede) e no correio (email) analisado. Expandindo assim suas capacidades de Endpoint Protection e EDR para uma plataforma completa de análise contra APTs também na rede, email e\ou nuvem.

5.6.13. A solução deve poder quarentenar máquinas infectadas, isolando-as logicamente da rede sem afetar a capacidade de análise forense.

5.6.14. A solução deve implementar adicionalmente, as seguintes funcionalidades:

5.6.14.1. Rastreio de logons para detecção de possíveis movimentações laterais, criando um mapa visual das ocorrências.

5.6.14.2. Rastreio de processos suspeitos, aos quais podem receber classificações através dos indicadores de comprometimentos mapeados pela rede de inteligência do fabricante.

5.6.14.3. Rastreio de tentativas de roubo de credenciais e\ou tentativa de acessos indevidos a recursos chave do sistema operacional.

5.6.14.4. Integração com sandbox para envio de artefatos suspeitos para análise.

5.6.14.5. Permitir que os administradores da solução se conectem remotamente aos dispositivos gerenciados, disponibilizando um terminal para execução de comandos do sistema operacional. Também deve ser possível o upload de scripts para execução.

5.6.14.6. Permitir a visualização automática de contexto adicional sobre alertas, fornecendo um fluxo de trabalho automatizado que coleta e analisa artefatos, destacando rapidamente índices de comprometimento já conhecidos.

5.6.14.7. Permitir encaminhamento de log de eventos do Windows (Event Viewer) via syslog para soluções SIEM. Deve permitir, pelo menos, o envio dos seguintes tipos de logs do Windows: System, Application Experience, Security, AppLocker, PowerShell, Application, Windows Defender, Task Scheduler, Print Service, and Terminal Services.

5.6.14.8. Permitir a criação de alertas e, opcionalmente, bloqueios de ataques que visam bypass do controle de conta de usuário (UAC), identificando rapidamente atividades potencialmente maliciosas, gerando alertas para os hosts envolvidos. A funcionalidade deve detectar, minimamente, as seguintes técnicas de ataque: Token manipulation, Process masquerading, Environmental variable hijacking, Shell command hijacking, COM handler hijacking, Program output abuse.

5.6.15. A solução deve permitir a criação de exceção em caso de falso positivo ou até mesmo em casos pontuais para atendimento de possíveis regras do negócio.

5.6.16. A solução deve possuir módulos de detecção avançados, tais como mecanismos de machine learning e proteção contra exploração de vulnerabilidades em aplicações, também permitindo que exceções ou customizações de regras sejam realizadas para impedir falsos positivos ou até mesmo para atender regras do negócio.

5.6.17. A solução deve permitir a configuração de autoproteção como, configurar uma senha para impedir sua remoção por usuários não autorizados.

5.6.18. A solução deve prover formas de segregar os equipamentos por grupo facilitando assim a aplicação de políticas granulares e outras configurações.

5.6.19. A solução deve permitir a criação de grupos de hosts de forma estática, ou seja, adicionando manualmente todos os ativos pertinentes;

5.6.20. A solução deve permitir a criação de grupos de hosts dinâmicos, movimentando os ativos automaticamente, baseado minimamente nos seguintes critérios:

5.6.20.1. Versão do agente;

5.6.20.2. Domínio na qual a máquina está inserida ou grupo de trabalho;

5.6.20.3. Sistema operacional;

5.6.20.4. Arquitetura;

5.6.20.5. Timezone;

5.6.20.6. Subnet;

5.6.20.7. Hostname.

5.6.21. A solução deve permitir o cadastramento de hosts de alto valor, como Active Directory, Exchange, Banco de dados, etc, não permitindo que certas ações de resposta se apliquem aos mesmos.

5.6.22. A solução deve possuir capacidade de realizar ações tais como:

5.6.22.1. Coleta de arquivos;

5.6.22.2. Realizar dump de memória parcial ou completo;

5.6.22.3. Isolamento de hosts;

5.6.22.4. Obter listagem de arquivos da máquina;

5.6.22.5. Obter pacotes de diagnóstico para análise de saúde do agente;

5.6.22.6. Deletar alertas do host;

5.6.22.7. Coleta de comandos digitados em:

5.6.22.8. PowerShell;

5.6.22.9. CMD;

5.6.22.10. Bash.

5.6.23. A solução deve permitir a customização de ações, facilitando assim o tipo de coleta durante uma investigação.

5.6.24. A solução deve permitir a realização de análise das coletas através da console centralizada, sem necessidade de extrair estes dados durante a análise inicial.

5.6.25. Deve haver a possibilidade de importar indicadores ou mesmo criar indicadores customizados dentro da plataforma para que estes sejam utilizados para detecção e contenção de ameaças.

5.6.26. A solução deve permitir realizar buscas específicas sobre os eventos coletados e catalogados na console centralizada, assim como permitir a realização de buscas em tempo real de indicadores de comprometimento.

5.6.27. A solução deve permitir o controle de utilização de recursos na estação ou servidor, estabelecendo o percentual de CPU máximo a ser utilizado pelo agente e também a quantidade de espaço em disco destinada aos eventos gerados.

5.6.28. A plataforma deve submeter a rede de inteligência do fabricante todos os hashs de arquivos verificados pelos agentes, obtendo respostas rápidas sobre o nível de risco do artefato.

5.6.29. A solução deve realizar rastreamento de logons, permitindo a pesquisa por meio da interface gráfica da solução, possibilitando o rastreamento de máquinas acessadas por um determinado usuário.

5.6.30. O rastreamento de logons deve possuir inteligência para detecção de movimentação lateral e utilização indevida de credenciais.

5.7. **Requerimentos técnicos do agente**

5.7.1. A solução deve suportar no mínimo 335 agentes conectados em uma única console de gerenciamento.

5.7.2. Suportar a instalação em ambientes Windows, suportando minimamente:

5.7.2.1. Windows 7;

5.7.2.2. Windows 8;

5.7.2.3. Windows 10;

5.7.2.4. Windows Server 2008 R2;

5.7.2.5. Windows Server 2012;

5.7.2.6. Windows Server 2016;

5.7.2.7. Windows Server 2019.

5.7.3. Deve suportar o ambiente Mac OS X 10.9 ou posterior.

5.7.4. Deve suportar distribuições Linux para no mínimo, as seguintes versões:

5.7.4.1. Red Hat Enterprise Linux (RHEL) 6.8 a 6.10;

5.7.4.2. Red Hat Enterprise Linux (RHEL) 7.1 a 7.7;

5.7.4.3. Red Hat Enterprise Linux (RHEL) 8;

5.7.4.4. CentOS 6.8 a 6.10;

5.7.4.5. CentOS 7.1 a 7.7;

5.7.4.6. CentOS 8;

5.7.4.7. Ubuntu 14.04, 16.04, 18.04, 19.04;

5.7.4.8. SUSE 11.3, 11.4, 12.2, 12.3, 15;

5.7.4.9. Oracle Linux 6.10, 7.6.

5.7.5. 1.3.5. Deve suportar sistemas de 32 e 64 bits.

5.7.6. 1.3.6. Agente único com mecanismos de detecção para minimizar a configuração e maximizar a detecção e o bloqueio.

5.7.7. 1.3.7. A solução deve poder operar independentemente da localização da estação de trabalho, desde que esteja conectada à Internet.

5.7.8. 1.3.8. Todos os dispositivos que operam fora da rede da organização devem ser acessados por um equipamento/software intermediário, fornecido e suportado diretamente pela mesma contratada. Recursos baseados em um proxy de uso geral ou NAT realizado em um dispositivo de rede não serão aceitos.

5.8. **Capacidades técnicas mínimas necessárias:**

5.8.1. Capacidade de detectar malware conhecido, incluindo vírus, cavalos de tróia, worms, spyware, adware, key loggers, rootkits e outros programas indesejados.

5.8.2. Detectar, possíveis incursões.

5.8.3. Responder, de forma a fazer a contenção e correção dos problemas.

5.8.4. A solução deve oferecer suporte ao uso de indicadores de comprometimento para detecção de presença e execução de malware. Os indicadores de compromisso devem ser fornecidos pelo fabricante e atualizados automaticamente e regularmente.

5.8.5. Os indicadores de comprometimento devem permitir identificar pelo menos as seguintes atividades de ameaças e/ou evidências:

5.8.5.1. Uso não autorizado de contas de usuário válidas;

5.8.5.2. Atividade de comando e controle;

5.8.5.3. Malware conhecido e desconhecido;

5.8.5.4. Tráfego de rede suspeito;

5.8.5.5. Uso de programas válidos para fins maliciosos;

5.8.5.6. Acesso não autorizado a arquivos do sistema.

5.8.6. A solução deve permitir a criação de indicadores de comprometimento manual e\ou automaticamente por meio de API ou manualmente no console de gerenciamento.

5.8.7. Os indicadores de compromisso devem permitir a avaliação de pelo menos as seguintes condições:

5.8.7.1. Gravação de arquivo, avaliando minimamente: Caminho completo, nome do arquivo, tamanho do arquivo, Hash md5, processo que o gravou, caminho para o processo executado e usuário que o escreveu.

5.8.7.2. Gravação no registro, avaliando minimamente: processo que o gravou, caminho para o processo executado, caminho para a chave, nome e valor do atributo e tipo de evento de gravação.

5.8.7.3. Nova conexão de rede, avaliando minimamente: IP remoto e local, porta remota e local, protocolo, processo que iniciou a conexão, processo que a escreveu, rota para o processo executado e usuário associado ao processo.

5.8.7.4. Carregamento de imagem binária para execução, avaliando minimamente: processo executado, nome e caminho do executável, processo que o carregou (pai) e caminho do executável que o carregou.

5.8.7.5. Resolução de DNS por meio da API do sistema operacional, avaliando minimamente: nome do host resolvido, processo associado à resolução, caminho para o executável do processo e usuário associado ao processo.

5.8.7.6. Eventos relacionados a processos, avaliando minimamente: tipo de evento, processo executado, nome e caminho do executável, processo que o iniciou (pai), caminho para o executável do processo que o iniciou, hora de início, linha de comando usada e hash md5 do binário.

5.8.7.7. URL acessada em navegadores suportados, avaliando minimamente: nome do host, URL, método HTTP, User Agent, cabeçalho HTTP, IP remoto, porta local e remota, processo associado a requisição e caminho para o executável do processo associado.

5.8.8. A solução deve permitir definir uma lista branca de dispositivos com os quais a comunicação não será interrompida no caso de isolamento de máquinas comprometidas.

5.8.9. Toda vez que um host for contido (isolado), a solução deve permitir a customização da tela de bloqueio que o usuário irá receber ao tentar realizar suas atividades.

5.8.10. Para isolar um host, a solução deve estabelecer um fluxo de aprovação, permitindo que a ação seja validada por outro analista, se necessário.

5.8.11. Para desbloquear hosts isolados, a solução deve permitir a utilização de códigos específicos, a serem obtidos na console de gerenciamento, a fim de validar a ação de resposta.

5.8.12. A solução deve suportar a capacidade de executar pesquisas em massa em toda ou parte da base instalada usando uma sequência de condições lógicas e operadores "e" / "ou". Os resultados dessas pesquisas devem retornar a lista de dispositivos pesquisados, se a pesquisa foi efetiva ou falhou e se ocorreu um erro durante a pesquisa. As condições mínimas nas pesquisas em massa deve ser:

5.8.12.1. Nome das aplicações;

5.8.12.2. Nome do navegador da Web;

5.8.12.3. Versão do navegador da Web;

5.8.12.4. Atributos do cookie (metadados);

5.8.12.5. Nome do cookie;

5.8.12.6. Valor do cookie;

5.8.12.7. Nome DNS;

5.8.12.8. Nome do driver de dispositivo;

5.8.12.9. Nome da DLL exportada no executável;

5.8.12.10. Nome da função exportada no executável;

5.8.12.11. Nome da função importada no executável;

5.8.12.12. Nome do módulo importado no executável;

5.8.12.13. Nome do executável injetado;

5.8.12.14. Atributo de arquivo;

5.8.12.15. Nome do emissor do certificado digital do arquivo executável;

5.8.12.16. Tipo MIME dos arquivos baixados;

5.8.12.17. Registro de arquivos baixados;

5.8.12.18. Tipo de arquivos baixados;

5.8.12.19. Caminho e nome dos arquivos no disco;

5.8.12.20. MD5, SHA1 e SHA256 dos arquivos em disco;

5.8.12.21. Nome do fluxo de arquivos;

5.8.12.22. Conteúdo no cabeçalho dos arquivos;

5.8.12.23. Nome do dispositivo;

5.8.12.24. Cabeçalho HTTP das requisições realizadas;

5.8.12.25. IP local do dispositivo;

5.8.12.26. IP remoto em que o dispositivo estava conectado;

5.8.12.27. Portas UDP e TCP, locais e remotas de conexões feitas pelo dispositivo;

5.8.12.28. Nome dos processos em execução no dispositivo;

5.8.12.29. Argumentos dos processos em execução no dispositivo;

5.8.12.30. Caminho dos elementos, chaves e valores no registro;

5.8.12.31. Serviços registrados, por nome, status do tipo e DDL associado;

5.8.12.32. Entradas nos logs de eventos (syslog e EventLog);

5.8.12.33. Tarefas de execução registradas, por nome, referência, status e atributos;

5.8.12.34. Registro de tempo de acesso, criação e alteração de arquivos;

5.8.12.35. Registro de tempo no último login;

5.8.12.36. Registro de URLs acessadas;

5.8.12.37. Usuário logado.

5.8.13. A solução deve suportar a detecção e o bloqueio de explorações no mínimo dos seguintes aplicativos:

5.8.13.1. Acrobar Reader;

5.8.13.2. Adobe Flash;

5.8.13.3. Internet Explorer;

5.8.13.4. Mozilla Firefox;

5.8.13.5. Google Chrome;

5.8.13.6. Java;

5.8.13.7. Microsoft Word;

5.8.13.8. Microsoft Excel;

5.8.13.9. Microsoft PowerPoint.

5.8.14. A detecção de uma exploração deve acionar automaticamente a coleta de evidências das atividades realizadas anteriormente pelo aplicativo afetado. As evidências devem ser armazenadas no servidor de gerenciamento e acessadas na console para análise profunda do alerta.

5.8.15. A solução deve suportar a criação de grupos de estações nas quais a execução da detecção de exploração é excluída.

5.8.16. No caso de um alerta, a solução deve executar uma captura automática de recursos para análise forense. No mínimo, deve fornecer as seguintes informações:

5.8.16.1. Usuário conectado na estação de trabalho;

5.8.16.2. Conteúdo em cache;

5.8.16.3. Serviços em execução e portas abertas;

5.8.16.4. Contas de usuário e tarefas agendadas;

5.8.16.5. Processos em execução.;

5.8.16.6. Subconjuntos de registros de dados relacionados à atividade recente;

5.8.16.7. Dados do sistema;

5.8.16.8. Lista de discos;

5.8.16.9. Lista de volumes lógicos;

5.8.16.10. Histórico e downloads do navegador;

5.8.16.11. Entradas DNS e ARP.

5.8.17. A solução deve fornecer uma API que permita a integração com outros produtos. A API deve ser adequadamente documentada para conhecer todas as operações possíveis e os valores e parâmetros necessários para utilização.

5.8.18. A API deve fornecer autenticação baseada em certificados digitais e deve ser acessada através de um protocolo SSL seguro.

5.8.19. A API deve oferecer suporte mínimo às seguintes opções: Criação, consulta, modificação e exclusão de todos os indicadores de comprometimento suportados pela solução. Consulta, listagem e exclusão de alertas gerados pela solução. Consulta de todas as estações de trabalho configuradas, consulta de detalhes de um host específico, criar aquisições de evidências, consultar as aquisições feitas e /ou exclui-las, manipular os processos de contenção de um host, criar um requisito de contenção, aprovar e restaurar um equipamento da contenção. Criar pesquisas para indicadores de consolidação em todas as estações de trabalho registradas.

5.8.20. A solução deve permitir que você configure a frequência com a qual os agentes se conectam ao console central.

5.8.21. A solução deve permitir que os agentes indiquem os IPs e os domínios que devem ser usados para a conexão ao console central e a ordem de prioridade em que devem tentar se conectar.

5.8.22. A solução deve permitir que os agentes usem uma configuração de proxy para se conectar ao console.

5.8.23. A solução deve incluir recursos de proteção baseados em malware conhecido e sua interação com os arquivos no sistema de arquivos. Qualquer arquivo malicioso deve ser isolado e armazenado em uma área de quarentena.

5.8.24. A solução deve incluir scans de todos os arquivos no disco do dispositivo. Esses processos devem ser programáveis.

5.8.25. Os usuários devem ter a capacidade de interromper ou pausar os scans, mas esse recurso deve poder ser desativado pelo administrador.

5.8.26. Os processos de contenção de equipamentos infectados devem permitir definir uma série de IPs excluídos da contenção, para que a contenção não afete os processos de análise forense. A exclusão deve ser definida por IP ou nome de domínio.

5.8.27. Todos os requisitos de investigação devem ser listados juntamente com o status de execução, indicando se estão pendentes, em execução ou executados, bem como se algum erro foi detectado no processo.

5.8.28. As evidências coletadas devem poder ser analisadas no console de gerenciamento ou por meio de software fornecido pela contratada.

5.8.29. Para evitar congestionamentos, o número máximo simultâneo de coleções deve ser definido.

5.8.30. A configuração da coleção deve permitir a inclusão de um ou mais dos seguintes componentes:

5.8.30.1. Gravação de arquivo, para no mínimo: caminho completo, nome do arquivo, tamanho do arquivo, hash md5, processo que o gravou, caminho para o processo executável, usuário que o escreveu;

5.8.30.2. Gravação no registro, para no mínimo: processo que o escreveu, caminho para o executável do processo, caminho para a chave, nome e valor do atributo e tipo de evento de gravação;

5.8.30.3. Conexão de rede, registrando-se minimamente: IP remoto e local, porta remota e local, protocolo, processo que iniciou a conexão, processo que a escreveu, rota utilizada pelo processo executado e usuário associado ao processo;

5.8.30.4. Carregamento de imagem binária para execução, para no mínimo: processo executado, nome e caminho do executável, processo que o carregou (pai) e caminho para o executável que o carregou;

5.8.30.5. Resolução de DNS por meio da API do sistema operacional, registrando minimamente: nome do host resolvido, processo associado à resolução, caminho para o executável do processo e usuário associado ao processo;

5.8.30.6. Eventos relacionados ao processo, para no mínimo: tipo de evento, processo executado, nome e caminho do executável, processo que o iniciou (pai), caminho para o executável do processo que o iniciou, hora de início, linha de comando usada e hash md5 do binário;

5.8.30.7. URL acessada em navegadores suportados, registrando minimamente: nome do host, URL, método HTTP, User Agent, cabeçalho HTTP, IP remoto, porta local e remota, processo associado e caminho para o executável do processo associado.

5.8.31. A solução ainda deve poder realizar coletas e obter informações minimamente sobre:

5.8.31.1. Descrição sobre o navegador da web;

5.8.31.2. Lista de drivers carregados na memória;

5.8.31.3. Eventos do sistema (EventLog ou syslog), incluindo eventos de aplicativo, sistema e segurança, além de qualquer outro disponível.

5.8.31.4. Coleta de arquivo, diretório ou árvore de diretórios de um disco;

5.8.31.5. Captura das tabelas e amarrações do kernel, como:

5.8.31.6. Tabela de descritores de interrupção (IDT);

5.8.31.7. Tabela de descritor de serviço do sistema (SSDT);

5.8.31.8. Requisições de entrada\saída (IRP).

5.8.31.9. Captura de tabelas de conexão de rede estabelecidas;

5.8.31.10. Captura dos processos em execução, com detalhes sobre eles.

5.8.31.11. Captura de parte ou todo o registro, permitindo a filtragem das chaves ou valores de interesse por meio de expressões regulares.

5.8.31.12. Captura da lista de Serviços, seu status de execução e os detalhes dos processos binários associados.

5.8.31.13. Captura da linha de comando e histórico de execução do PowerShell.

5.8.31.14. Captura de informações do sistema operacional e host.

5.9. **Item 2 - Solução para proteção avançada de e-mail corporativo**

5.10. **Características Gerais**

5.10.1. A solução deve permitir fácil integração com tecnologias em nuvem e otimizar os investimentos realizados sem necessidade de novas contratações em uma futura migração para serviços como Office 365.

5.10.2. A solução deve possuir ao menos 2 diferentes métodos de implementação, sendo um deles menos evasivo, ou seja, não requerendo alterações de registros DNS como MX, possibilitando assim, o recebimento de uma cópia do tráfego para análise.

5.10.3. A solução deve operar em tempo real, analisando e retendo e-mails até que seja determinado se ele deve ser excluído, colocado em quarentena e\ou enviado para o servidor de correio eletrônico.

5.10.4. A solução deve implementar minimamente as seguintes funcionalidades de MTA:

5.10.4.1. Capacidade de filtrar as conexões recebidas pelo IP de origem, para limitar quem pode enviar e-mail para a solução;

5.10.4.2. A solução deve suportar o uso do Transport Layer Security (TLS) suportando pelo menos TLS 1.2. Além disso, você deve poder forçar o uso do TLS nos e-mails de entrada ou saída, bloqueando as sessões que não são criptografadas;

5.10.4.3. A solução deve poder verificar a identidade do MTA do próximo salto usando TLS e certificados digitais.

5.10.5. A solução deve oferecer suporte ao gerenciamento de congestionamentos para evitar o colapso das sessões de entrada. Suportando minimamente os seguintes modos:

5.10.5.1. Rejeitar conexões, para não receber mais e-mails;

5.10.5.2. Não analisar o tráfego e enviar diretamente;

5.10.5.3. Descartar o email.

5.10.6. Depois que o e-mail for analisado e liberado, ele poderá ser enviado para o próximo salto utilizando, pelo menos uma das seguintes opções:

5.10.6.1. Reenviar para um único IP;

5.10.6.2. Envio para vários IPs, usando um sistema de prioridade para poder distribuir tráfego com diferentes taxas de carga;

5.10.6.3. Enviar usando os resultados de uma consulta DNS para o registro MX do domínio de cada destinatário.

5.10.7. A solução deve permitir visualização de estatísticas relacionadas ao número de correspondências vistas com os itens que constam nas listas negra ou branca.

5.10.8. A solução deve ser capaz de criar um e-mail de notificação para o administrador e, opcionalmente, para os destinatários das mensagens bloqueadas. O e-mail deve poder ser configurado para conter o texto definido pelo administrador.

5.10.9. A solução deve permitir a criação alertas de notificações a serem enviados por e-mail.

5.10.10. A solução deve oferecer suporte ao rastreio de mensagens através de no mínimo as opções abaixo:

5.10.10.1. Atributos da mensagem;

5.10.10.2. ID da fila;

5.10.10.3. ID original da mensagem.

5.10.10.4. Remetente;

5.10.10.5. Destinatário;

5.10.10.6. Assunto;

5.10.10.7. Status da mensagem;

5.10.10.8. Resultado de análise de ameaças avançadas;

5.10.10.9. Resultado de análise de malware;

5.10.10.10. Ações de políticas de conteúdo;

5.10.10.11. Tamanho da mensagem;

5.10.10.12. IP do remetente;

5.10.10.13. Mensagens que contenham anexo;

5.10.10.14. Domínios cadastrados na plataforma.

5.10.11. Durante a realização de filtros para rastreamento de mensagens, a solução deve permitir a utilização de expressões condicionais, permitindo negar atributos da mensagem na busca como:

5.10.11.1. Remetente;

5.10.11.2. Destinatário;

5.10.11.3. Assunto;

5.10.11.4. Status da mensagem;

5.10.11.5. Resultado de análise de ameaças avançadas;

5.10.11.6. Resultado de análise de malware;

5.10.11.7. Ações de políticas de conteúdo;

5.10.11.8. IP do remetente.

5.10.12. A solução deve permitir relatórios estatísticos baseados em:

5.10.12.1. Estatísticas de recebimento e entrega de mensagens;

5.10.12.2. Estatísticas de mensagens retidas pelos filtros da solução;

5.10.12.3. Número de mensagens retidas por conterem ameaças avançadas;

5.10.12.4. Número de mensagens retidas por tentativa de representação;

5.10.12.5. Número de mensagens retidas por conterem malwares;

5.10.12.6. Estatísticas de motivo de rejeição de mensagens;

5.10.12.7. Estatísticas contendo médias do tamanho das mensagens;

5.10.12.8. Estatísticas dos principais tipos de anexos recebidos/enviados;

5.10.12.9. Estatísticas de acionamento de regras de listas negras e brancas;

5.10.12.10. Estatísticas de acionamento de regras de conteúdo;

5.10.12.11. Estatísticas contendo os remetentes que mais enviaram mensagens para organização;

5.10.12.12. Estatísticas contendo o IP dos remetentes que mais enviaram mensagens para organização;

5.10.12.13. Estatísticas contendo os usuários internos que mais recebem/enviam e-mails.

5.10.13. A solução deve exibir um mapa de ameaças, organizando as detecções de ameaças avançadas recebidas por seus devidos países de origem.

5.10.14. A solução deve permitir integração com qualquer provedor de email.

5.10.15. A solução precisa possuir no mínimo as seguintes certificações:

5.10.15.1. ISO 27001;

5.10.15.2. SOC 2 Type 2;

5.10.15.3. FedRAMP.

5.10.16. A plataforma deve possuir auditoria de ações executadas no console administrativo para consulta.

5.10.17. A solução não deve limitar o número de domínios a serem cadastrados na plataforma.

5.10.18. A solução deve permitir a criação de grupos de domínio a serem cadastrados para organização dos mesmos.

5.10.19. Para mensagens de saída da organização, a solução deve implementar uma chave de autenticação a ser verificada em todas as mensagens pelas plataformas. Qualquer mensagem que não contenha a chave indicada, deverá ser rejeitada.

5.10.20. As regras customizadas devem permitir a utilização de, pelo menos, os seguintes atributos para condições de acionamento:

5.10.20.1. Envelope From;

5.10.20.2. Envelope From Domain;

5.10.20.3. Assunto;

5.10.20.4. Palavras chave;

5.10.20.5. HELO/EHLO Name;

5.10.20.6. Body;

5.10.20.7. Body Size;

5.10.20.8. Header exists;

5.10.20.9. Header value;

5.10.20.10. Recipient;

5.10.20.11. DMARC verdict;

5.10.20.12. DKIM result;

5.10.20.13. SPF result;

5.10.20.14. Reverse Domain;

5.10.20.15. Message size;

5.10.20.16. Sender IP;

5.10.20.17. Country;

5.10.20.18. Anexos.

5.10.21. As condições de acionamento de regras customizadas, devem permitir, pelo menos, os seguintes operadores lógicos:

5.10.21.1. Igual;

5.10.21.2. Contém;

5.10.21.3. Validação de expressão regular;

5.10.21.4. Campo vazio?

5.10.22. As regras customizadas devem permitir a utilização de, pelo menos, as seguintes ações:

5.10.22.1. Inserir Header;

5.10.22.2. Modificar o assunto;

5.10.22.3. Bypassar verificações de segurança;

5.10.22.4. Roteamento da mensagem;

5.10.22.5. Entrega normal;

5.10.22.6. Rejeição da conexão;

5.10.22.7. Movimentar mensagem para quarentena.

5.10.23. As regras customizadas devem permitir que os anexos sejam manipulados utilizando, pelo menos, os seguintes atributos:

5.10.23.1. Extensão do arquivo;

5.10.23.2. Nome do arquivo;

5.10.23.3. Hash do arquivo;

5.10.23.4. Tipo real do arquivo;

5.10.23.5. Tamanho do arquivo.

5.10.24. As regras customizadas devem permitir criação de exceções utilizando, pelo menos, os seguintes atributos:

5.10.24.1. Envelope From;

5.10.24.2. Envelope From Domain;

5.10.24.3. Assunto;

5.10.24.4. Palavras chave;

5.10.24.5. HELO/EHLO Name;

5.10.24.6. Body;

5.10.24.7. Body Size;

5.10.24.8. Header exists;

5.10.24.9. Header value;

5.10.24.10. Recipient;

5.10.24.11. DMARC verdict;

5.10.24.12. DKIM result;

5.10.24.13. SPF result;

5.10.24.14. Reverse Domain;

5.10.24.15. Message size;

5.10.24.16. Sender IP;

5.10.24.17. Country;

5.10.24.18. Anexos.

5.10.25. A solução deve permitir a configuração de, pelo menos, os seguintes limites de parâmetros de mensagens:

5.10.25.1. Número de mensagens por domínio de destinatário;

5.10.25.2. Número de mensagens por IP do remetente;

5.10.25.3. Número de Mensagens por Endereço do Remetente;

5.10.25.4. Volume de mensagens por domínio de destinatário (em KB);

5.10.25.5. Volume de mensagens por IP do remetente (em KB);

5.10.25.6. Volume de mensagens por endereço do remetente (em KB).

5.11. **Antivírus**

5.11.1. A solução para proteção de e-mails deve fornecer no mínimo capacidade para lidar com ameaças conhecidas e possuir recursos para detectar e bloquear ameaças modernas e desconhecidas.

5.11.2. A solução deve suportar a análise de URLs "reduzidos", como Tiny URL, bit.ly ou outros.

5.11.3. Os URLs detectados como maliciosos devem incluir uma captura de tela do site malicioso.

5.11.4. A solução deve poder adicionar um cabeçalho de e-mail indicando o resultado da análise realizada, para que o MTA a seguir possa definir regras de processamento condicional para esse cabeçalho, identificando minimamente os seguintes resultados:

5.11.4.1. E-mail limpo;

5.11.4.2. Anexo malicioso;

5.11.4.3. URL maliciosa;

5.11.4.4. Estrutura de email suspeita;

5.11.4.5. Email não analisado;

5.11.4.6. Erro na análise.

5.11.5. O texto do cabeçalho deve ser modificável pelo administrador.

5.11.6. A solução deve analisar arquivos compactados.

5.11.7. A solução deve analisar os arquivos que estão ofuscados.

5.11.8. A solução deve poder analisar os URIs protegidos com base64.

5.11.9. A solução deve detectar, analisar e bloquear ataques de rootkit.

5.11.10. A solução deve detectar, analisar e bloquear ataques de injeção de DLL que tentam modificar aplicativos instalados no sistema operacional, como as ferramentas do MS Office.

5.11.11. A solução deve permitir remediação automática para Office 365 em e-mails que se tornaram maliciosos depois da entrega.

5.11.12. O processo de remediação para o Microsoft 365 deve permitir a execução de pelo menos, as seguintes ações na caixa do usuário:

5.11.12.1. Remediação automática, para e-mails que se tornaram maliciosos depois da entrega;

5.11.12.2. Movimentação de mensagens da caixa de entrada do usuário para qualquer outra pasta definida;

5.11.12.3. Remover a mensagem da caixa de entrada do usuário e armazenar a mesma na quarentena da solução;

5.11.12.4. Deletar a mensagem permanentemente, mesmo que a mensagem já tenha sido recebida pelo usuário.

5.11.13. Deve fornecer detecção e proteção em tempo real contra ataques de coleta de credenciais, representação e spear-phishing.

5.11.14. Deve possuir ferramentas avançadas contra táticas de representação que se tornam cada vez mais comuns em ataques virtuais.

5.11.15. A ferramenta contra ataques de representação deve considerar em suas análises no mínimo:

5.11.15.1. Frequência que um usuário recebe e-mails de um remetente específico (Consultando também bases globais de inteligência pra correlacionamento);

5.11.15.2. Indicadores de domínios e endereços IP que normalmente se comunicam com cada cliente e o serviço de email como um todo;

5.11.15.3. Idade do domínio em questão;

5.11.15.4. Domínios conectados pela primeira vez com a plataforma.

5.11.16. Deve possuir ferramentas para detectar a idade de domínios e tratar automaticamente domínios registrados recentemente como suspeitos.

5.11.17. A solução deve suportar a definição de um tamanho máximo de e-mail, para evitar riscos de ataques de saturação.

5.11.18. A solução deve permitir a criação de listas brancas para poder enviar diretamente os e-mails recebidos sem serem analisados. Essas listas devem poder ser definidas de acordo com:

5.11.18.1. Endereço de email do remetente;

5.11.18.2. Domínio remetente;

5.11.18.3. IP de origem;

5.11.18.4. País de origem da qual a mensagem é recebida.

5.11.19. A solução deve permitir a criação de listas negras para bloquear diretamente os e-mails recebidos sem serem verificados. Essas listas devem poder ser definidas de acordo com:

5.11.19.1. Endereço de email do remetente;

5.11.19.2. Domínio remetente;

5.11.19.3. IP de origem;

5.11.19.4. País de origem da qual a mensagem é recebida.

5.11.20. A solução deve permitir a instalação de soluções de antivírus, para consulta de inteligência de detecção de outros fabricantes. A solução deve permitir a utilização das bases de pelo menos, os seguintes fabricantes:

5.11.20.1. Ad-Aware;

5.11.20.2. AegisLab;

5.11.20.3. Agnitum;

5.11.20.4. Avast;

5.11.20.5. AVG;

5.11.20.6. Bitdefender;

5.11.20.7. ClamAV;

5.11.20.8. Comodo;

5.11.20.9. eSafe;

5.11.20.10. ESET-NOD32;

5.11.20.11. F-secure;

5.11.20.12. Fortinet;

5.11.20.13. Karpersky;

5.11.20.14. MalwareBytes;

5.11.20.15. McAfee;

5.11.20.16. Microsoft;

5.11.20.17. Panda;

5.11.20.18. Sophos;

5.11.20.19. Symantec;

5.11.20.20. TrendMicro.

5.12. **Proteção de ameaças avançadas (ATP)**

5.12.1. A solução deve ser capaz de analisar os URLs incluídos no e-mail para acessar os objetos de risco para os quais eles apontam, permitindo que eles sejam analisados em Sandbox.

5.12.2. A solução deve poder analisar URLs de FTP que não possuem o protocolo especificado (http:// ou https://).

5.12.3. A solução deve ser capaz de extrair senhas do corpo do e-mail para tentar desbloquear arquivos criptografados ou protegidos por senha.

5.12.4. A solução deve incluir uma lista de domínios a serem bloqueados associados aos ataques de Typosquatting, nos quais o usuário é redirecionado para um site mal-intencionado por ter cometido um erro de digitação ao escrever o domínio.

5.12.5. A solução deve ser capaz de detectar alertas retroativos, ou seja, alertas sobre URLs ou anexos que não foram detectados como maliciosos antes, mas que após uma atualização são listados como maliciosos.

5.12.6. Os alertas retroativos devem ser claramente identificados como tal entre os outros alertas.

5.12.7. A solução deve detectar código malicioso em documentos e arquivos como:

5.12.7.1. Microsoft Office em todas versões com suporte atualizado;

5.12.7.2. Documentos PDF;

5.12.7.3. Arquivos compactados.

5.12.8. A solução deve ser capaz de detectar e analisar URLs incorporados em arquivos PDF.

5.12.9. A solução deve ser capaz de detectar URLs ocultas em que a URL exibida não corresponde a URL que está realmente incorporada na mensagem. A diferença deve ser detectada no texto ou no protocolo.

5.12.10. A solução deve suportar a criação de regras no formato YARA, versão 3.4 ou superior.

5.12.11. Deve ser capaz de detectar, interromper e conter ataques de dia zero, ameaças persistentes (APT) e Spear Phishing.

5.12.12. No caso de e-mails, se um administrador confirmar que o e-mail analisado não é potencialmente malicioso, ele poderá ser liberado.

5.12.13. Se um ato malicioso for detectado em um e-mail, deve ser possível enviar um aviso ao administrador e ao destinatário. Essa detecção deve poder ser feita em ataques desconhecidos de dia zero e / ou ameaças persistentes.

5.12.14. A solução deve apresentar o risco associado a cada uma das ameaças, indicando se é baixo, médio ou alto risco.

5.12.15. A solução deve registrar toda a atividade que um objeto malicioso tenta executar, registrando as modificações do sistema operacional/aplicativo que ele consegue modificar, como:

5.12.15.1. Registro do Windows;

5.12.15.2. Registro da aplicação;

5.12.15.3. Registro de processos;

5.12.15.4. Registro de arquivos;

5.12.15.5. Registro de comportamento;

5.12.15.6. Registro de comunicações.

5.12.16. A solução deve analisar os anexos de e-mail, compactados, ofuscados e /ou criptografados.

5.12.17. Deve fornecer conhecimento profundo sobre ataques e agressores de investigações da linha de frente e observações de adversários.

5.12.18. A busca de ameaças avançadas deve percorrer minimamente as extensões abaixo:

5.12.18.1. EXE;

5.12.18.2. DLL;

5.12.18.3. PDF;

5.12.18.4. SWF;

5.12.18.5. DOC/DOCX;

5.12.18.6. XLS/XLSX;

5.12.18.7. PPT/PPTX;

5.12.18.8. JPG;

5.12.18.9. PNG;

5.12.18.10. MP3;

5.12.18.11. MP4;

5.12.18.12. ZIP/RAR/TNEF.

5.12.19. A proteção para e-mail deve permitir a possibilidade de atuação em caso de ameaças de ransonware iniciados por e-mail antes que a comunicação com o centro de comando seja efetivada.

5.12.20. Deve possuir dados analíticos e machine learning para detecção de ameaças que tentam evadir as tradicionais detecções por assinatura.

5.12.21. Todos os alertas gerados em detecções de ameaças avançadas, devem ter a possibilidade de serem enviados para soluções de SIEM.

5.12.22. A solução deve permitir que URLs suspeitas sejam reescritas para links seguros, evitando que usuários tenham acesso direto a links suspeitos, gerando um alerta (Que pode ser customizado) avisando que a URL é suspeita ou até mesmo impedindo o acesso se a mesma for considerada maliciosa.

5.13. **Item 3 - Solução de segurança de rede avançada contra APTs**

5.14. **Características Gerais**

5.14.1. Deve ser fornecido e modelo Virtual Appliance, compatível com Vmware.

5.14.2. A solução deve ser capaz de realizar proteções no sentido “Norte-Sul”, para tráfego de entrada e saída da organização, e “Leste-Oeste”, para tráfico interno da organização.

5.14.3. Para o cenário de análise de tráfego E-W (Leste-Oeste), a solução deve fornecer detecção de atividades do invasor na fase de pós-exploração e roubo de dados/informações ocorrendo em redes internas ou privadas. Deve suportar a funcionalidade NTA.

5.14.4. Deve ser capaz de detectar os ataques do tipo “Pass the Hash”, Fileless, enumeração de redes, hosts e serviços fornecendo assim capacidades para hunting de ameaças.

5.14.5. A solução deve possuir, de forma padrão, uma variedade de regras de detecção para o nível de análise do tráfego Leste-Oeste.

5.14.6. A solução deve ter um motor de correlação avançado, um motor analítico e utilizar técnicas de "Machine Learning" para detecção de movimentos laterais furtivos. Além disso, deve fornecer um registro de dados capturados nas camadas L4 e L7 para uma rápida investigação e análise forense.

5.14.7. solução deve gerar metadados para uma análise completa, incluindo protocolos como: FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB/2, SMTP, SSH e TLS.

5.14.8. A solução deve ser dimensionada de modo a suportar 500 Mbps de throughput.

5.14.9. Deverá ter a capacidade de analisar a navegação via espelhamento de portas para monitoramento ou ser implementada em modo inline para interceptação (bloqueio) de ameaças.

5.14.10. Deve ser capaz de integrar sensores de diferentes finalidades, como de análise web, e-mail, endpoints e outros, com a capacidade de correlacionar eventos através de um console única do mesmo fabricante.

5.14.11. Deve ser capaz de detectar o padrão de uma nova ameaça avançada e sincronizá-lo com os outros sensores implementados local ou remotamente. Tudo através uma única console de gerenciamento.

5.14.12. Deverá fornecer uma tecnologia sandbox local com virtualização proprietária que suporta o sistema Windows x86 e x64, além de MacOS e Linux integrando-se à rede de dados existente de forma autônoma. O mecanismo de Sandbox também deverá poder ser externalizado através de hardwares dedicados ou nuvem.

5.14.13. No tráfego interceptado, a solução deve fornecer as seguintes funcionalidades:

5.14.13.1. Bypass fail-open e fail-close configurável;

5.14.13.2. Capacidade de filtrar qual tráfego será analisado e qual será ignorado. O tráfego ignorado não deve passar pelos componentes da solução de análise de navegação;

5.14.13.3. Capacidade de agregar o tráfego de diferentes fibras, para garantir que os fluxos TCP atinjam cada um dos diferentes dispositivos que compõem a solução de análise de navegação;

5.14.13.4. Capacidade de balancear as sessões TCP analisadas entre os diferentes dispositivos que compõem a solução de análise de navegação. Após a queda de um dos componentes, a solução deve ser capaz de reatribuir sessões tcp para os dispositivos restantes;

5.14.13.5. Capacidade de detectar o status operacional dos dispositivos da solução de análise de navegação. Para o modo OOB (Out-of-band), deve ser capaz de identificar o estado da interface, enquanto, para o modo de operação em linha (inline), deve usar um pacote de monitoramento que deve circular por cada um dos componentes para verificar se os componentes estão processando o tráfego corretamente

5.14.14. A solução deve fornecer todos os SFPs/SFP+ necessários para a interconexão dos componentes, bem como a fiação correspondente.

5.14.15. A ferramenta deve ter mecanismos de bloqueio de tráfego mesmo que sua configuração e implantação de rede correspondam ao modo de monitoramento (TAP/SPAN) permitindo o uso de TCP Reset e Out-of-Band Blocking.

5.14.16. A solução deve permitir a criação de listas brancas para exclusão de análise de tráfego para, no mínimo:

5.14.16.1. Generic Routing Encapsulation (GRE);

5.14.16.2. Portas específicas;

5.14.16.3. Por Rede específicas;

5.14.16.4. VLAN específicas.

5.14.17. A solução deve incluir regras e Inteligência de Ameaças.

5.14.18. A solução deve incluir um pacote de regras padrões. Estas devem ser alimentados automaticamente diretamente pelo fabricante sem afetar a solução ou incluir a intervenção de analistas. Por sua vez, deve permitir a criação de regras personalizadas pela organização com padrão SNORT.

5.14.19. A solução deve incluir a descrição das famílias de malware.

5.14.20. A solução deve fornecer atribuição automática de alerta a grupos APT.

5.14.21. O fabricante da solução deve ter especialistas em segurança que estão monitorando as ameaças atuais e gerar pacotes de regras para ajudar a solução oferecida com detecção

5.14.22. Deve possuir capacidade de envio de logs para a equipe de suporte diretamente da solução, sem necessidade de envios externos, facilitando assim o tempo de resposta e resolução em caso de problemas.

5.14.23. Todos os dispositivos incluídos devem suportar o gerenciamento através de uma console centralizada onde deve-se configurar as políticas e outras configurações para melhor utilização do produto. Está console de gerência unificada deve suportar minimamente os seguintes itens:

5.14.23.1. Permitir o download dos indicadores de comprometimento em alguns dos seguintes formatos CSV, STIX, JSON ou XML;

5.14.23.2. Deve permitir gerar alertas dos dispositivos integrados;

5.14.23.3. Permitir a exportação dos alertas através da própria console;

5.14.23.4. Permitir o agendamento de novos relatórios diariamente, semanalmente, mensalmente ou em período customizado;

5.14.23.5. Deve permitir e possuir APIs para facilitar a integração de outras soluções;

5.14.23.6. Permitir bloqueio de artefatos com apenas uma única ação para todas os dispositivos;

5.14.23.7. Configurar regras YARA e\ou SNORT.

5.15. **Requisitos gerais de detecção e prevenção**

5.15.1. A solução deve fornecer um sistema avançado de proteção contra ameaças, proteção contra ataques cibernéticos gerados por grupos de "Hacktivismo", Crime Organizado, Espionagem e Ciber terrorismo.

5.15.2. A solução deve possuir camadas para: Detectar, Conter e Analisar, Malware, Botnets, APTs, Malware Polimórfico e ZeroDays sem fazer uso de reputação, conhecimento prévio ou assinaturas. Baseada em um modelo de detecção e bloqueio no ponto de monitoramento, garantindo a contenção de infecções recebidas e, assim, mantendo a integridade dos equipamentos que integram a rede computacional.

5.15.3. A solução deve ter a capacidade de bloquear as comunicações de comando e controle (C2C), evitando a perda de informações e outros danos a rede da empresa.

5.15.4. Possuir assinaturas de detecção baseadas em vulnerabilidades e, também, detecção de ataques desconhecidos através da análise de anomalias no tráfego da rede, sem a necessidade de assinaturas específicas.

5.15.5. Possuir a capacidade de operar em modo invisível (stealth), sem nenhum endereço IP associado as portas de detecção.

5.15.6. Possuir capacidade de remontagem de pacotes para identificação de ataques.

5.15.7. Deve possuir capacidade de criar assinaturas definidas pelo usuário com uso de expressões regulares.

5.15.8. Permitir a atualização das assinaturas e respectivos tratamentos de forma manual e automática.

5.15.9. Permitir identificação de ataques em protocolos que utilizam portas aleatórias.

5.15.10. Permitir o desenvolvimento de assinaturas de ataques descobertos de forma a prevenir a reincidência dos mesmos.

5.15.11. Possibilitar a atualização das assinaturas de ataques e defesa, via Internet, em intervalos regulares e de forma automática.

5.15.12. Possuir suporte a fragmentação e desfragmentação IP, além de TCP stream reassembly.

5.15.13. Possuir a capacidade de configurar ações e respostas, com a finalidade de evitar ataques.

5.15.14. Envio de eventos SNMP relativos ao desempenho e funcionamento do equipamento.

5.15.15. Deve ser possível colocar o equipamento em um modo passivo, onde todo o trafego é permitido, mas o sistema deve enviar os registros de alerta de acordo com as políticas aplicadas.

5.15.16. Deve atuar de forma que o bloqueio de uma determinada tentativa de invasão não interfira no restante do tráfego da rede.

5.15.17. Capacidade de enviar alarmes para a console de administração.

5.15.18. Permitir a captura de pacotes (PCAP) de um ataque detectado por uma assinatura.

5.15.19. O equipamento deve dispor de mecanismos tipo whitelist e blacklist que permitam o controle de exceções e listas de detecções customizadas para bloqueios em tempo real.

5.15.20. Deve permitir realizar as seguintes ações em resposta à inspeção de tráfego:

5.15.20.1. Bloquear;

5.15.20.2. Permitir;

5.15.20.3. Bloquear + Notificar;

5.15.20.4. Bloquear + Notificar + Capturar pacotes do ataque;

5.15.20.5. Permitir + Notificar;

5.15.20.6. Permitir + Notificar + Captura pacotes do ataque.

5.15.21. Deve possuir filtros de “PortScan”, protegendo a rede contra ataques do tipo “scan”.

5.15.22. Deve possuir mecanismos para detecção de WebShells em PHP, WAR, JSP, ASP e ASPX.

5.15.23. Deve possuir capacidade de fornecer uma pré-visualização de URLs envolvidas em alertas, além de conseguir identificar o alvo no caso de tentativas de roubo de credenciais.

5.15.24. Deve ser capaz de detectar novos tipos de ataques cibernéticos, como malware de dia zero, APT, polimorfismo; que superam os sistemas convencionais de segurança de computadores já instalados na rede.

5.15.25. O sistema de proteção contra malware deve detectar malware de dia zero, malware polimórfico, Botnets e outros APT (ameaças persistentes avançadas) na rede interna e nas comunicações para a Internet (tráfego de entrada e tráfego de saída). A plataforma também deve ter a capacidade de detectar software malicioso que aproveita as vulnerabilidades conhecidas.

5.15.26. O ambiente de inspeção virtual deve poder emular o sistema operacional e o navegador como se fosse o computador host, comunicando-se aos servidores da Web que tentam infectar o computador. Para fazer isso, não é necessário conectar-se a nenhum outro dispositivo cuja função seja fornecer assinaturas de malware ou qualquer outra dependência externa.

5.15.27. O sistema de proteção contra malware deve ter a capacidade de bloquear chamadas para servidores remotos (callbacks). No caso de ataques de dia zero, o Malware Protection System deve bloquear a capacidade do Malware de fazer chamadas de C&C (comando e controle), deixando-o inerte e evitando a perda de informações. Isso significa que o mesmo deve detectar e impedir malware avançado, ataques Zero Day e ameaças persistentes avançadas direcionadas sem ter sido previamente reconhecido por uma base de assinaturas.

5.15.28. A solução deve fornecer proteção contra ataques baseados na Web, como, por exemplo, downloads de arquivos maliciosos, callbacks de malware, etc.

5.15.29. Deve agir em tempo real, para relatar a presença de malware moderno na rede interna. A solução deve informar pelo menos: nome da ameaça, gravidade, IP, nome do host, número de infecções relacionadas. A solução também deve relatar a capacidade prejudicial da ameaça, detalhando se é um possível roubo de informações, comportamento malicioso ou alterações feitas no sistema operacional.

5.15.30. Para cada uma das infecções por malware detectadas, deve mostrar pelo menos os seguintes campos:

5.15.30.1. Detalhes da ameaça, PCAP, IP de origem, Cabeçalhos (origem);

5.15.30.2. Detalhe das alterações feitas no sistema operacional, indicando os alertas maliciosos detectados durante a análise do comportamento da ameaça, o tipo e a versão do sistema operacional.

5.15.31. A solução poderá fornecer informações sobre quantas vezes o computador foi infectado e a comunicação foi bloqueada. Também deve detalhar o malware que o infectou e seu nível de risco.

5.15.32. A ferramenta deve ser capaz de executar todo o código suspeito, URLs e vários tipos de arquivos em um ambiente de inspeção virtual no mesmo dispositivo. Para fazer isso, ele executará análises estáticas e dinâmicas no sistema.

5.15.33. Deve suportar a execução e a inspeção de pelo menos, os seguintes tipos de arquivos: 3gp, asf, avi, bat, chm, cmd, com, csv, dll, doc, docx, exe, flv, gif, hop, hml, htm, hwp, ico jar, jpg, js, lnk, midi, mov, mp3, mp4, mpg, pdf, ppsx, ppt, pptx, qt, rm, rmi, rtf, swf, tiff, url, vbs, vcf, vcs, wav , wma, wsf, xls, xlsx, xml.

5.15.34. Para analisar os diferentes tipos de arquivos maliciosos, as máquinas virtuais devem suportar por padrão:

5.15.34.1. Arquivos Microsoft Office (doc/docx, xls/xlsx, ppt/pptx) e PDF;

5.15.34.2. Objetos Flash;

5.15.34.3. Objetos Shockwave;

5.15.34.4. Conteúdo Java JDK & JRE;

5.15.34.5. Objetos Quicktime;

5.15.34.6. Objetos Realplayer;

5.15.34.7. Objetos Windows Media Player;

5.15.34.8. Conteúdos Microsoft.NET framework;

5.15.34.9. Conteúdos Microsoft Visual C++ Redistributable;

5.15.34.10. Conteúdos Microsoft Silverlight;

5.15.34.11. Formatos de Imagens (jpg, jpeg, gif, tiff, ico, png);

5.15.34.12. Conteúdos Microsoft DirectX.

5.15.35. A solução deve registrar e armazenar evidências de execução de malware no ambiente de inspeção, armazenando pelo menos: endereços IP, portas e protocolos usados por malware e todo o processo de execução e comunicação do ciclo de vida do malware detectado.

5.15.36. A solução deve registrar toda a atividade que um objeto malicioso tenta executar, registrando as modificações do sistema operacional/aplicativo que ele consegue modificar, como:

5.15.36.1. Registro do Windows;

5.15.36.2. Registro da aplicação;

5.15.36.3. Registro de processos;

5.15.36.4. Registro de arquivos;

5.15.36.5. Registro de comportamento;

5.15.36.6. Registro de comunicações.

5.15.37. No processo de detecção de malware, a solução deve ser capaz de:

5.15.37.1. Suportar Zero Day Browser Exploit Protection;

5.15.37.2. Suportar Zero Day Application Exploit Protection;

5.15.37.3. Suportar Zero Day Web Object Exploit Protection;

5.15.37.4. Suportar Zero Day C&C Callback Protection;

5.15.37.5. Suportar Local Virtual Machine/Sandbox Analysis.

5.15.38. Deverá detectar tráfego malicioso da rede, tais como consultas DNS, Botnet e WebShell detection.

5.15.39. Deverá identificar riskware, como no mínimo: PUPs, PUAs, adware e ferramentas de hacking.

5.15.40. Deverá detectar, analisar e bloquear ataques que envolvem rootkits.

5.15.41. A solução deve detectar, analisar e bloquear ataques de injeções de DLL que tentam modificar aplicativos instalados no sistema operacional da Microsoft, ou em suas ferramentas de escritório.

5.15.42. A solução deve suportar a criação de regras no formato YARA, versão 3.8.1 ou superior.

5.15.43. A solução deve suportar alertas retroativos em URLs que inicialmente não foram considerados maliciosos, com um prazo de até 24 horas depois da primeira análise. Os alertas retroativos devem ser claramente identificados como tal entre os outros alertas.

5.15.44. A solução deve analisar tráfegos como: SMB1, SMB2, DCERPC, WinRM, MS-SQL, VXLAN e outros protocolos baseados em TCP, comumente usados para movimentos horizontais. Além de poder detectar protocolos SCADA como ModBus.

5.15.45. A solução deve ser capaz de detectar os seguintes tipos de atividades maliciosas:

5.15.45.1. Reconhecimento interno;

5.15.45.2. Execução;

5.15.45.3. Persistência;

5.15.45.4. Escalação de privilégios;

5.15.45.5. Acesso às credenciais;

5.15.45.6. Movimentos laterais;

5.15.45.7. Exfiltração de informações.

5.15.46. A solução deve detectar outras técnicas de ameaça, como:

5.15.46.1. Acesso ao registro remoto (AppInit_DLLs, RunOnce, WinLogon etc);

5.15.46.2. Agendamento remoto de tarefas via ATSVC;

5.15.46.3. Execução remota de serviços como:

5.15.46.4. MSRPC Bind para serviço SRVSVC;

5.15.46.5. Chamada NetShareEnum para serviço SRVSVC;

5.15.46.6. Conexão SMB TreeConnect para ADMIN$;

5.15.46.7. Criação de requisição SMB por arquivos executáveis e MSRPC Bind para o serviço SCMR;

5.15.46.8. Operação de inicialização de serviços para SCMR;

5.15.46.9. Criação de requisição SMB para named pipe usando psexec;

5.15.46.10. Execução remota de diversos outros serviços;

5.15.46.11. MSRPC Bind para Service Control Manager;

5.15.46.12. Operação de chamada para abertura de serviço (qualquer um);

5.15.46.13. Operação de inicialização de serviços;

5.15.46.14. Ativação do serviço de registro remoto.

5.15.47. A solução deve ser capaz de detectar a exfiltração de informações da rede.

5.15.48. As informações devem ser armazenadas em um formato PCAP padrão, o que permitirá fácil manipulação com ferramentas de distribuição gratuitas, como wireshark.

5.16. **Requisitos gerais para análise de tráfego SSL/TLS**

5.16.1. Suportar, no mínimo TLS versões 1.0, 1.1 e 1.2.

5.16.2. Deve implementar a funcionalidade de inspeção SSL para análise de tráfego criptografado.

5.16.3. Deve permitir espelhamento de tráfego descriptografado para análise de soluções de outros fabricantes.

5.16.4. Realizar a análise de tráfego para comunicações destinadas para servidores internos, utilizando certificados e chaves assinados por Autoridades Certificadoras publicamente reconhecidas.

5.16.5. Realizar a análise de tráfego destinados para servidores externos, localizados em quaisquer outras redes, utilizando certificados auto assinados e certificados assinados por Autoridades Certificadoras de propriedade da CONTRATANTE.

5.16.6. Permitir criar regras para determinar quais tráfegos devem ser descriptografados, incluindo IP de origem e destino, porta destino, aplicação, zona, usuário e qualquer combinação destes.

5.16.7. Permitir criar regras de exceção para análise de tráfego por categoria de URLs de destino.

5.16.8. Suportar algoritmos de chaves simétricas incluindo, no mínimo DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard) e AES (Advanced Encryption Standard).

5.16.9. Possuir listas de cifras compatíveis com FIPS 140-2 e CC-NDPP

5.17. **Requisitos gerais do sistema de gerenciamento**

5.17.1. Em casos de múltiplos dispositivos a console de gerenciamento deve poder ser implementada em hardware dedicado, em solução virtualizada ou em nuvem, dimensionada para atender todas as necessidades técnicas especificadas.

5.17.2. No caso de oferta de solução virtualizada, ser compatível com Vmware.

5.17.3. A Solução deverá ter mecanismos de busca em sua console de gerenciamento, de modo que seja facilitada a busca por detecções.

5.17.4. Permitir a instalação, configuração e atualização de todos os componentes.

5.17.5. Deverá ter a capacidade de gerar gráficos em tempo real.

5.17.6. Deverá possuir interface WEB segura (HTTPS).

5.17.7. Deve possuir recurso de geolocalização (localização geográfica da máquina do atacante).

5.17.8. Emitir relatórios gráficos e em texto, permitindo a execução periódica de forma automática. A solução deverá permitir também o envio automático dos relatórios ou de um link de acesso para um e-mail escolhido pelo administrador.

5.17.9. Exportar relatórios para, no mínimo, os seguintes formatos: PDF e CSV. Os relatórios devem poder ser gerados de forma manual ou automática.

5.17.10. Toda alteração de política e definições na console de gerenciamento deve ser registrada e passível de auditoria.

5.17.11. 3Deve categorizar os eventos de acordo com a severidade.

5.17.12. Suportar a aplicação de diversos perfis de inspeção de tráfego, trabalhando de maneira simultânea em diferentes segmentos físicos ou lógicos.

5.17.13. Deve possuir atualizações de assinaturas de forma dinâmica e automática quando estas estiverem disponíveis pelo fabricante, sem a necessidade de pesquisa de conteúdo de segurança para a atualização do produto.

5.17.14. Deve manter os logs de ataques e de alarmes provenientes de detecções.

5.17.15. Deve suportar envio de logs para tecnologias de SIEM.

5.17.16. Deve permitir envio de eventos SNMP relativos ao desempenho e funcionamento do equipamento.

5.17.17. A solução deve possuir alternativas para autenticação, fornecendo opções locais e remotas utilizando servidores externos como LDAP e RADIUS. Também deve oferecer a opção de integração via SAML.

5.17.18. A solução a oferecer deve ser capaz de sincronizar sua data e hora via NTP.

5.17.19. A solução deve oferecer o envio de resultados das análises de ameaças através de e-mail, trap, syslog e/ou snmp para notificação.

5.17.20. A notificação de eventos de saúde do sistema deve poder ser enviada por e-mail.

5.17.21. Deve ter a capacidade de gerenciar diferentes níveis de usuário (administradores, usuários de monitoração e usuários de API em pelo menos 2 níveis)

5.17.22. O ambiente de análise virtual deve poder fornecer todas as descobertas de malware em um arquivo compactado como evidência para possível análise forense subsequente.

5.17.23. Deve ter um módulo de relatório que emita pelo menos relatórios sobre os principais alertas (atividade atual ou histórica) por intervalo de datas/ endereços IP e etc.

5.17.24. A solução deverá apresentar filtros de pesquisa em eventos que geram logs ou alertas com, no mínimo, os seguintes critérios:

5.17.24.1. Data (hora, dia, mês e ano);

5.17.24.2. Nome ou identificação do filtro;

5.17.24.3. Protocolo(serviço);

5.17.24.4. Endereço IP ou porta origem ou destino.

5.17.25. A solução deverá ser capaz de suportar a retenção de logs por no mínimo 90 dias.

5.17.26. Os relatórios e logs deverão ser exportados, pelo menos, para os formatos PDF e CSV.

5.18. **Item 4 - Solução de gerenciamento, orquestração e validação de segurança**

5.19. **Arquitetura**

5.19.1. A solução de SIEM deve ser on-premise ou baseada em nuvem (Cloud), para o caso de orquestração (SOAR) o mesmo deve ser implementado de forma On-premises para fácil comunicação com recursos que ainda estejam neste modelo.

5.19.2. No caso de utilização de hardware para a plataforma, o mesmo não deve constar em listas de EOF (End-of-Life) e deve suportar todos os requerimentos listados sem necessidade de contratação de licenças adicionais.

5.19.3. A solução deve fornecer componentes já licenciados para coleta e envio de logs/tráfego até a plataforma central.

5.19.4. O componente para coleta de logs/tráfego deve fornecer a possibilidade de instalação em servidores Windows, Linux ou imagens prontas já fornecidas junto a plataforma principal.

5.19.5. A solução deve suportar processamento de logs/eventos para, no mínimo os itens especificados previamente nos quantitativos indicados.

5.19.6. A solução deverá estar licenciada de forma a manter o processamento em tempo real ou realizar o buffer dos eventos, mesmo que o tráfego de eventos ultrapasse o volume licenciado nas horas de pico.

5.19.7. Suportar um tráfego de logs de, no mínimo, 350 eventos por segundo (EPS).

5.19.8. Deve possuir capacidade de recebimento e armazenamento, mínimo, de todos os logs de ativos de segurança, alertas de segurança, tráfego de pacotes, dentre outras informações relacionadas, em formado bruto (raw) e/ou metadados, necessárias para fins de correlacionamento e forense, conforme especificação abaixo:

	Tráfego de Pacotes	**Logs, Eventos, Alertas, dentre outras informações**
Metadados	Armazenar por no mínimo 365 dias	Armazenar por no mínimo 365 dias

	Tráfego de Pacotes	Logs, Eventos, Alertas, dentre outras informações
Dados brutos (raw)	Armazenar por no mínimo 365 dias	Armazenar por no mínimo 365 dias

5.19.9. A solução deve ter a capacidade de manter os itens coletados indexados para buscas rápidas por pelo menos 7 dias. Itens a serem buscados em datas superiores ao período de indexação devem respeitar o período de retenção do tópico anterior.

5.20. **Requerimentos Gerais da plataforma**

5.20.1. A solução deverá ser capaz de gerenciar de forma eficiente incidentes de segurança. O software de gerenciamento de incidentes de segurança deve permitir a definição de um processo abrangente desde o registro e triagem inicial de um incidente até sua resolução e prevenção.

5.20.2. A solução deve permitir a automação de fluxos de forma gráfica, incluindo estágios, tarefas paralelas ou sequenciais, regras de decisão e aprovação, sem a necessidade de programação ou alteração de código fonte para as integrações já existentes.

5.20.3. A solução deve permitir automatização e orquestração de fluxos relacionados a resposta de incidentes de segurança, integrando e simplificando as operações.

5.20.4. A solução deve fornecer visibilidade, rastreabilidade e indexação dos eventos detectados, integrando as várias ferramentas de segurança que a entidade possui, aumentando a capacidade de detecção e maturidade da segurança cibernética.

5.20.5. A solução deve permitir acelerar a resposta às lacunas de segurança cibernética por meio de análise contextual, automação de processos e capacidade de articulação para investigação, utilizando fluxos de análise e inteligência associada às metodologias de ataque de grupos de cibercrime.

5.20.6. A solução deve identificar, registrar e indexar incidentes de segurança rapidamente, registrando os eventos relatados pelas soluções que a entidade atualmente possui ou derivando diretamente da ferramenta SIEM.

5.20.7. A solução deve permitir integração e interoperabilidade com o ecossistema de segurança da entidade, independentemente da marca dos produtos de segurança utilizados.

5.20.8. Ela deve permitir a integração baseada em fluxos de trabalho através do cruzamento de dados das soluções de segurança como SIEMs, Firewalls, IPSs e sistemas de chamados.

5.20.9. A solução deve possuir controle granular de níveis de acesso a plataforma.

5.20.10. A solução deve funcionar com autenticação de dois fatores, sendo eles: OTP, SMS ou voz.

5.20.11. A solução deve permitir que você configure políticas restritas de senha como período de redefinição, bloqueio por tentativas sem sucesso, histórico de senha e desativação de usuários por tempo de inatividade.

5.20.12. A solução deve registrar e listar todos os alertas ativos, permitindo filtros e pesquisas sob demanda em uma linguagem de queries bem documentada.

5.20.13. A solução deve permitir a criação de listas a serem utilizadas durantes as pesquisas, com objetivo de poder facilmente utiliza-las para inclusão ou remoção de recursos na busca, evitando a repetição de comandos, tornando as ações de caça a ameaças (hunting) mais ágeis.

5.20.14. A solução deve possuir alertas indicando a gravidade do incidente, permitindo a detecção, validação e investigação, a fim de reconstruir toda a cadeia do ataque.

5.20.15. A solução deve suportar uma linha do tempo visual em relação aos eventos registrados.

5.20.16. Quando as soluções de proteção de email, rede e endpoint forem de mesmo fabricante, a mesma deve permitir a gestão destes equipamentos, isto incluí a realização de monitoramento de saúde dos equipamentos, modificação de políticas, realização de coletas e disponibilização de artefatos na console de forma unificada, mantendo o objetivo de fornecer uma plataforma de operações de segurança integrada.

5.20.17. A solução deve oferecer suporte à integração com soluções de segurança de terceiros. A integração deve ser baseada em syslog, ingestão/absorção de alertas e/ou análise de tráfego de rede.

5.20.18. A solução deve permitir a criação de painéis e dashboards com gráficos de gestão, de forma ágil e intuitiva, sem a necessidade de programação e alteração do código-fonte.

5.20.19. A solução deve permitir aos atendentes e solucionadores de incidentes a possibilidade de criação de seus próprios painéis e gráficos dentro da solução, compartilhando sempre que necessário com grupos ou usuários específicos, permitindo gerenciamento das permissões de compartilhamento de acordo com os perfis de cada usuário.

5.20.20. A solução deve permitir a criação de gráficos, utilizando como origem de dados, as informações de diferentes soluções de segurança da organização.

5.20.21. A solução deve permitir configurar o envio automático e agendado de relatórios e gráficos gerenciais para grupos de usuários ou usuários específicos.

5.20.22. A solução deve incluir painéis unificados, buscas e relatórios, para facilitar a transição da detecção para a investigação e a resposta subsequente ao incidente relatado.

5.20.23. O coletor da solução deverá ser capaz de coletar, aplicar parsing, normalizar e categorizar os eventos dos dispositivos monitorados em tempo próximo ao real.

5.20.24. O fabricante deve prover de mecanismos de apoio na realização de parsing de logs não interpretados pela solução, de maneira a qual a realização deste parsing possa ser feito através de um chamado de suporte.

5.20.25. Caso um utilitário seja fornecido para apoio no parsing, o mesmo deve ser compatível com uma linguagem de fácil intepretação e deve poder identificar tipos de dados, realizar validações no log identificando possíveis campos para o parsing, fornecer a quantidade de campos identificados e também uma opção para testar a quantidade de matches do parsing realizado.

5.20.26. A solução deve possuir parsing, para interpretação automática de logs, para pelo menos as seguintes marcas/soluções:

5.20.26.1. Aerohive;

5.20.26.2. Akamai;

5.20.26.3. AWS;

5.20.26.4. Apache;

5.20.26.5. Arbor;

5.20.26.6. ArcSight;

5.20.26.7. Aruba;

5.20.26.8. Barracuda;

5.20.26.9. BeyondTrust;

5.20.26.10. BlueCoat;

5.20.26.11. Broadcom;

5.20.26.12. Brocade;

5.20.26.13. Carbom Black;

5.20.26.14. CheckPoint;

5.20.26.15. Cisco;

5.20.26.16. Citrix;

5.20.26.17. Crowdstrike;

5.20.26.18. CyberArk.

5.20.26.19. Cylance;

5.20.26.20. Docker;

5.20.26.21. Eset;

5.20.26.22. F5;

5.20.26.23. FireEye;

5.20.26.24. Forcepoint;

5.20.26.25. Forescout;

5.20.26.26. Fortinet;

5.20.26.27. Graylog;

5.20.26.28. HP;

5.20.26.29. IBM;

5.20.26.30. Imperva;

5.20.26.31. Juniper;

5.20.26.32. Mandiant;

5.20.26.33. McAfee;

5.20.26.34. Microsoft;

5.20.26.35. Nagios;

5.20.26.36. Nginx;

5.20.26.37. Oracle;

5.20.26.38. Palo Alto;

5.20.26.39. Proofpoint;

5.20.26.40. Pulse Secure;

5.20.26.41. Riverbad;

5.20.26.42. RSA;

5.20.26.43. SonicWall;

5.20.26.44. Sophos;

5.20.26.45. Splunk;

5.20.26.46. Symantec;

5.20.26.47. Tenable;

5.20.26.48. Trend Micro;

5.20.26.49. Varonis;

5.20.26.50. Digital Guardian;

5.20.26.51. Vmware;

5.20.26.52. WatchGuard;

5.20.26.53. Zscaler.

5.20.27. A solução deve fornecer um guia de compliance que possa ser utilizado para facilitar o atendimento de algumas normativas tais como PCI e HIPAA.

5.20.28. A solução deve fornecer um módulo de UEBA ao qual possa ser utilizado para análise avançada do comportamento de entidades (computadores e usuários) aos quais podem estar envolvidos em atividades maliciosas. O módulo de UEBA deve utilizar técnicas avançadas para análise de comportamento sendo possível correlacionar eventos e extrair informações relevantes as quais devem ser utilizadas para definir o perfil de risco das entidades.

5.20.29. A análise comportamental baseada em entidades deve permitir a consulta também em ambientes que utilizam Azure AD, através de integração nativa com a nuvem da Microsoft.

5.20.30. A visualização de uma entidade/ativo na análise comportamental deve permitir, minimamente:

5.20.30.1. Realizar exportação do ativo/lista para CSV ou JSON;

5.20.30.2. Promover os alertas da entidade para um caso novo ou existente;

5.20.30.3. Suprimir todos os alertas relacionados a entidade;

5.20.30.4. Fechar todos os alertas relacionados a entidade;

5.20.30.5. Abrir novamente todos os alertas relacionados a entidade.

5.20.31. A plataforma SIEM deve analisar os tipos de log enviados e realizar sugestões de envio de importantes fontes de detecção de malware na qual ele não está recebendo logs. Exemplo: a organização não está enviando logs de firewall e DHCP, tais logs ampliam o poder de detecção da plataforma. Este recurso deve estar em execução automaticamente.

5.20.32. A solução deve possuir dashboards e relatórios que classifiquem os logs que foram devidamente classificados, permitindo também a rápida visualização dos que não foram, para que as ações de "parsing" possam ser planejadas.

5.20.33. A solução deve possuir dashboards prontos que são alimentados a partir da ingestão de logs para pelo menos, os seguintes fabricantes:

5.20.33.1. AWS;

5.20.33.2. Carbon Black;

5.20.33.3. Checkpoint;

5.20.33.4. Cisco;

5.20.33.5. Crowdstrike;

5.20.33.6. Druva;

5.20.33.7. FireEye;

5.20.33.8. Google Cloud Plataform;

5.20.33.9. iBoss;

5.20.33.10. Imperva;

5.20.33.11. McAfee;

5.20.33.12. Microsoft;

5.20.33.13. Microsoft Azure;

5.20.33.14. Okta;

5.20.33.15. Palo Alto;

5.20.33.16. Proofpoint;

5.20.33.17. Sophos;

5.20.33.18. Symantec;

5.20.33.19. Virtru.

5.20.34. A plataforma deve possuir meios de monitoramento de saúde de todos os sensores que enviam logs para a console central.

5.20.35. Caso alguma fonte para de enviar logs, a plataforma deve informar automaticamente os administradores para verificação.

5.21. **Inteligência de Ameaças**

5.21.1. A solução deve incluir regras de correlação e inteligência de ameaças.

5.21.2. A solução deve incluir um pacote de regras para detecção. Elas devem ser alimentadas automaticamente, sem gerar impacto na solução ou solicitar intervenção de um analista. Por sua vez, ela deve permitir a criação de regras personalizadas pela empresa, incluído a entrada manual de novos indicadores de comprometimento.

5.21.3. A solução deve fornecer uma boa variedade de regras de inteligência já criadas e disponíveis para detecção de ameaças e também permitir customização de novas para atender necessidades específicas.

5.21.4. A solução deve incluir inteligência de ameaças que revise, valide e compare as fontes que estão sendo utilizadas para detecção de ameaças.

5.21.5. A solução deve incluir a descrição das famílias de malware.

5.21.6. A solução deve fornecer atribuição automática de alertas a grupos de APTs.

5.21.7. O fabricante da solução deve possuir especialistas em segurança que estejam monitorando as ameaças atuais ao redor do mundo, gerando a partir disso, novos pacotes de regras para aprimorar a solução em seu nível de detecção. Tal serviço não deve ocasionar custo adicional para a CONTRATANTE.

5.21.8. O fabricante da solução deve rastrear grupos de crimes cibernéticos, a fim de aprimorar regras de detecção a partir de incidentes globais.

5.21.9. A solução deve utilizar uma rede de inteligência que processa diversas amostras de malware exclusivas por dia.

5.21.10. A solução deve injetar inteligência nos dados de log registrados.

5.21.11. A solução deve oferecer análises sobre "beaconing", permitindo no mínimo, a detecção de malwares que tentam estabelecer contato com “Command and Control”.

5.21.12. A solução deve incluir como fonte de inteligência as ameaças, plataformas de segurança contratadas e permitir identificar a telemetria e o perfil de proliferação de um ataque, além de ter informações sobre vítimas e táticas, técnicas e procedimentos geralmente utilizados pelo invasor.

5.21.13. A solução deve possibilitar consultas de segurança específicas (Buscando referências a malwares ou ataques conhecidos), incluindo análise, para no mínimo:

5.21.13.1. URLs;

5.21.13.2. Domínios;

5.21.13.3. Hashes MD5;

5.21.13.4. Endereços IP.

5.21.14. Deve permitir a criação de listas a serem utilizadas com escopo de inteligência, facilitando assim o uso das mesmas em regras ou mesmo para customizar detecções especificas do negócio.

5.21.15. Deve fornecer a possibilidade de análise de malwares, executando o mesmo de maneira controlada (sandbox), a fim de receber um relatório sobre os comportamentos encontrados com a execução.

5.21.16. Depois que a solução detectar uma ameaça, ela deve relacionar as informações registradas na plataforma central e as vincular fornecendo detalhes de inteligência.

5.21.17. A solução deve oferecer análises mínimas em:

5.21.17.1. Beaconing;

5.21.17.2. Beaconing Diferencial;

5.21.17.3. Geo-feasibility;

5.21.17.4. Uso indevido de credenciais;

5.21.17.5. Detecção de conexão não reconhecida;

5.21.17.6. Detecção de Fast-Flux DNS;

5.21.17.7. Entropia DNS;

5.21.17.8. Detecção de ataques via PowerShell;

5.21.17.9. Detecção de Exfiltração de Dados;

5.21.17.10. Detecção de conexões de entrada SSH, Telnet, SMB e RDP que sejam anômalas;

5.21.17.11. Detecção de contas comprometidas com VPN;

5.21.17.12. Detecção de movimento lateral.

5.21.18. A solução deve permitir que sejam realizadas pesquisas em seu ambiente para atividades de "caça" a malwares e atividades maliciosas.

5.21.19. O fabricante deve possuir capacidade de fornecer um serviço capaz de auxiliar com investigações e até mesmo quando necessário permitir que por dentro da própria solução haja interação via chat com seus especialistas.

5.21.20. A plataforma deve possuir capacidade analítica de eventos/tráfego, independente das regras, para detecção de no mínimo os seguintes comportamentos:

5.21.20.1. Uso suspeito de chave da API Amazon Web Services (AWS);

5.21.20.2. Login de autenticação multifator anormal do Duo com base no histórico de login anterior deste usuário;

5.21.20.3. Atividade anormal do Google Cloud Platform (GCP) por um usuário;

5.21.20.4. Logon anormal no Microsoft Office 365 com base no histórico de logon anterior deste usuário;

5.21.20.5. Login anormal do Okta com base no histórico de login anterior deste usuário;

5.21.20.6. Login anormal do protocolo RDP (Remote Desktop Protocol) com base no histórico de login anterior deste usuário;

5.21.20.7. Download ou upload anormal de arquivo do SharePoint com base no histórico anterior deste usuário;

5.21.20.8. Detecção de força bruta do Citrix NetScaler, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.

5.21.20.9. Detecção de força bruta no Druva, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.

5.21.20.10. Tráfego de rede para domínios semelhantes a (permutações) do domínio da organização descoberto. Isso pode indicar um ataque de phishing ou alguma outra atividade suspeita.

5.21.20.11. Detecção de força bruta no Linux, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.

5.21.20.12. Detecção de força bruta do Office 365, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.

5.21.20.13. Okta detecção de força bruta. Isso realiza verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.

5.21.20.14. Vários logins de RDP pelo mesmo usuário.

5.21.20.15. Vários logins de RDP no mesmo host.

5.21.20.16. Login de VPN anormal com base no histórico de login de VPN anterior do usuário.

5.21.20.17. Uma conta de usuário foi excluída dentro de 24 horas após sua criação.

5.21.20.18. Detecção de força bruta do Windows NT LAN Manager (NTLM), realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.

5.21.20.19. Vários erros de "usuários únicos não encontrados" de uma fonte. Isso pode indicar uma tentativa de enumeração do usuário.

5.21.20.20. Vários processos exclusivos de um usuário ou host dentro de um curto período de tempo. Isso pode indicar atividade de reconhecimento.

5.22. **Capacidades de Investigação**

5.23. A solução deve incluir recursos de workflow para resposta a incidentes de segurança.

5.23.1. A solução deve ser capaz de coordenar os processos de segurança atuais no nível de alertas de rede e alertas de outras soluções de segurança.

5.23.2. A solução deve fornecer recursos de busca e pesquisa nas estações de trabalho, de acordo com os seguintes exemplos:

5.23.2.1. Ampla pesquisa por comportamentos maliciosos conhecidos;

5.23.2.2. Caça proativa de atividades suspeitas;

5.23.2.3. Investigação completa nos endpoints comprometidos;

5.23.2.4. Procurar evidências de intrusões avançadas como ameaças sem arquivo (fileless).

5.23.3. A solução deve fornecer recursos de resposta em tempo real, para no mínimo:

5.23.3.1. Investigar todos as atividades em terminais suspeitos;

5.23.3.2. Reproduzir a linha do tempo completa de um ataque avançado;

5.23.3.3. Capturar detalhes da atividade que ocorreu durante intrusões;

5.23.3.4. Executar uma análise aprofundada no nível de: Acesso ao disco, análise de memória e detecção de rootkit.

5.23.4. Depois que a solução detectar um alerta, a mesma deve fornecer pelo menos as seguintes informações:

5.23.4.1. A inteligência em torno do alerta detectado;

5.23.4.2. Métodos de detecção da ameaça em questão;

5.23.4.3. Mostrar graficamente uma linha do tempo de eventos relacionados ao alerta detectado;

5.23.4.4. Dicas de pesquisa para orientar os analistas em todo o processo de resposta a incidentes. Essas dicas devem estar associadas à experiência que o fabricante tem em responder a incidentes críticos de segurança em empresas em todo o mundo;

5.23.4.5. Mostrar os eventos brutos (raw data) que geraram o alerta;

5.23.4.6. Histórico de eventos associados.

5.23.5. A solução deve incluir dicas intuitivas de investigação, trazendo automaticamente no mínimo, os seguintes dados para consulta no alerta:

5.23.5.1. Existem outras regras alertadas para esse IP de origem?

5.23.5.2. Existem regras acionadas que foram baseadas em sensores de inteligência, relacionadas a algum desses índices de comprometimento?

5.23.5.3. Quais logs estão disponíveis para este dispositivo?

5.23.5.4. Quais logs estão disponíveis para este IP?

5.23.5.5. Em quais outros hosts esse malware foi encontrado?

5.23.5.6. Existem outros logs com esse hash?

5.23.5.7. Existem alertas relacionados usando o IP do agente?

5.23.5.8. Existem alertas relacionados usando o este dispositivo?

5.23.5.9. Existem alertas relacionados usando o hash envolvido no incidente?

5.23.6. A visualização de um caso deve permitir pelo menos, as seguintes ações:

5.23.6.1. Controle do Nome, Status, Prioridade, Classificação e Descrição do caso;

5.23.6.2. Permitir que o caso seja assinado para algum usuário;

5.23.6.3. Permitir que qualquer log/evento relacionado possa ser adicionado e visualizado no mesmo;

5.23.6.4. Permitir a visualização de todos os alertas/incidentes envolvidos no caso;

5.23.6.5. Permitir que o caso seja exportado em formatos CSV e JSON;

5.23.6.6. Permitir a adição e visualização de comentários no caso.

5.23.7. Durante o processo de resposta a incidentes, quando um caso for fechado, todos alertas relacionados também devem ser fechados. No caso de alertas que pertencem a mais de um caso, os mesmos devem permanecer abertos.

5.23.8. No nível analista/operador, a solução deve fornecer:

5.23.8.1. Um painel de pesquisa, onde são registrados alertas e casos atribuídos aos analistas;

5.23.8.2. Detalhe de alertas como: nível de risco, nome do alerta, tipo de alerta, origem, data da primeira ocorrência, data da última ocorrência, número de eventos, resumo, fontes e destino, status do alerta e opções de: exportação do alerta nos formatos CSV e JSON para excluir e\ou fechá-lo;

5.23.8.3. Cada alerta deve poder ser atribuído a um analista específico, para iniciar o processo de investigação, contenção, caça, etc.;

5.23.8.4. Deve haver um painel de casos, que permita a criação, gerenciamento e alocação de casos, a fim de rastrear as atividades e o tempo de resposta de cada analista;

5.23.8.5. Cada caso pode conter vários alertas, várias anotações, para validar o estado evolutivo na resposta a um incidente;

5.23.8.6. A ferramenta deve poder atribuir a cada caso níveis de: prioridade, gravidade e, como opção, outro tipo de classificação;

5.23.8.7. Cada caso deve ter: Descrição, Eventos, Alertas, Revisões e Notas, bem como o registro do qual o analista foi designado ou modificou o caso.

5.23.9. A solução deve ter a capacidade de realizar pesquisas para o processo de busca proativa e reativa nos eventos e metadados coletados de maneira automática.

5.23.10. A solução deve ter um módulo de pesquisa avançada ou indexação de pesquisa que contenha:

5.23.10.1. Um módulo de ajuda de sintaxe;

5.23.10.2. Um módulo de histórico de pesquisas;

5.23.10.3. Um módulo de pesquisa salva como favorita;

5.23.10.4. Capacidade de salvar a pesquisa.

5.23.11. As pesquisas devem ter uma sintaxe completa baseada em Query Language contemplando documentação completa e atualizada.

5.23.12. Deve incluir opções de pesquisa, com base em cada um dos campos de metadados, como: Domínio, porta de destino, método HTTP, metaclasses, porta de origem, useragent, IP de Origem, IP de destino e etc.

5.23.13. A solução deve possuir um módulo de UEBA ao qual poderá ser utilizado para melhor compreensão dos eventos, identificando possíveis entidades (equipamentos ou usuários) envolvidos anteriormente em outros eventos maliciosos ou suspeitos.

5.23.14. A visualização de um alerta/incidente deve permitir pelo menos, as seguintes ações:

5.23.14.1. Assinar o incidente para um analista;

5.23.14.2. Marcar como falso positivo;

5.23.14.3. Adicionar o alerta em um caso para um trabalho aprofundado envolvendo mais pessoas e artefatos de investigação;

5.23.14.4. Fechar ou suprimir o alerta;

5.23.14.5. Exportar o alerta para CSV ou JSON;

5.23.14.6. Fazer pesquisas de Índices de comprometimento diretamente em bases externas como VirusTotal e DomainTools;

5.23.14.7. Adicionar através de um clique, artefatos em listas para facilitar o trabalho de investigação e melhorar a assertividade das regras de detecção;

5.23.14.8. Visualizar a correlação de índices de comprometimento em outros incidentes abertos ou fechados;

5.23.14.9. Consultar análises realizadas automaticamente em bases de inteligência cibernética;

5.23.14.10. Analisar o histórico de modificações no incidente;

5.23.14.11. Adicionar comentários no incidente;

5.23.14.12. Quando realiza análise em sandbox para artefatos envolvidos em incidentes, permitir a visualização das modificações que o binário realizou.

5.23.15. Ao visualizar um tipo de evento, a plataforma deve permitir, a partir de cliques com o mouse (Sem necessidade de escrita de query), incrementar as buscas, para pelo menos as seguintes ações:

5.23.15.1. Realizar uma busca por qualquer campo daquela classe. Exemplo: Ip de origem/destino, hash md5, destinatário/remetente, ações aplicadas, etc;

5.23.15.2. No caso de uma busca já estar sendo realizada, deve ser possível adicionar qualquer campo listado na busca atual para seguimento das atividades de hunting;

5.23.15.3. Deve ser possível também realizar exclusões na busca a partir do valor de qualquer campo listado;

5.23.15.4. Dever ser possível realizar um agrupamento de qualquer valor listado, formando automaticamente um dashboard, estabelecendo as contagens e classificações de acordo com os valores dos campos;

5.23.15.5. Quando visualizado algum índice de comprometimento, deve ser possível realizar pesquisas em bases externas como VirusTotal e DomainTools;

5.23.15.6. Deve ser possível adicionar índices de comprometimento em listas para facilitar as buscas e criação de regras.

5.23.16. A solução deve permitir que as buscas mais realizadas sejam salvas para execução rápida sempre que necessário.

5.23.17. oda busca realizada deve ter a possibilidade de ser transformada em uma regra para detecção de comportamentos desejados.

5.24. **Orquestração e Automatização**

5.24.1. A arquitetura da plataforma de orquestração deve ser moderna e granular ao ponto de ao menos possuir as seguintes segmentações de seus serviços:

5.24.1.1. Serviço para orquestração;

5.24.1.2. Serviço Web para acesso à interface de gerência;

5.24.1.3. Ambiente virtual para execução de playbooks (Python);

5.24.1.4. Ambiente isolado para interpretações python do OS;

5.24.1.5. Serviço de banco de dados para gestão e armazenamento de dados o orquestrador;

5.24.1.6. Serviço de filas (RabbitMQ);

5.24.1.7. Database para armazenamento de informações do serviço de filas;

5.24.1.8. Serviço para tratativas de I/O do sistema web (Erlang);

5.24.1.9. Serviço para tratativas de execução do serviço de fila (Erlang Runtime);

5.24.1.10. Suporte a Node.js para interpretação de scripts customizados (JavaScript e Mustache);

5.24.1.11. Serviço de agendamento de comandos.

5.24.2. Deve possuir uma interface gráfica que contemple ao menos os itens abaixo para melhor organização, gerencia e ação durante possíveis investigações ou automatizações de atividades internas.

5.24.2.1. Dashboard;

5.24.2.2. Guia de chamados;

5.24.2.3. Playbooks;

5.24.2.4. Dispositivos;

5.24.2.5. Adaptadores;

5.24.2.6. Tabelas;

5.24.2.7. Tags;

5.24.2.8. Formulários;

5.24.2.9. Scripts;

5.24.2.10. Tipos;

5.24.2.11. Biblioteca.

5.24.3. Deve possuir plugins predefinidos e compatíveis com as diferentes tecnologias que a entidade possui no nível de segurança cibernética.

5.24.4. Deve fornecer uma biblioteca de plug-ins que permita integrar fluxos de trabalho e automação com vários tipos de tecnologias, para no mínimo:

5.24.4.1. TIPs - plataformas de inteligência;

5.24.4.2. Ferramentas de análise de malware;

5.24.4.3. EDR - Detecção e resposta do terminal;

5.24.4.4. SIEM;

5.24.4.5. Armazenamento - baseado em nuvem;

5.24.4.6. Sistemas de chamados;

5.24.4.7. Soluções de endpoint;

5.24.4.8. Firewalls;

5.24.4.9. Switches;

5.24.4.10. Ferramentas de sandbox;

5.24.4.11. Servidores de email;

5.24.4.12. Ferramentas de chat;

5.24.4.13. Dispositivos móveis etc.

5.24.5. A solução deve ter um ambiente gráfico que permita a criação dos fluxos para interação com as diferentes tecnologias.

5.24.6. A solução deve permitir a automação das atividades de resposta a incidentes com base nas necessidades e processos da entidade.

5.24.7. A solução deve poder registrar as métricas de desempenho e tempo economizado nas tarefas usando a orquestração.

5.24.8. Deve permitir etapas para escalação e aprovação em fluxos de trabalho.

5.24.9. Deve suportar a definição de tarefas ou ações assíncronas.

5.24.10. A solução deve suportar SMTP para envio de e-mails.

5.24.11. Deve permitir nível de acesso a console e componentes de forma granular.

5.24.12. No nível de gerenciamento de caso/ticket a solução deve ser capaz de alterar dinamicamente a prioridade dos casos, alterar a atribuição e o status de acordo com o fluxo definido.

5.24.13. Deve permitir a criação de novos plugins em Python, além de fornecer a habilidade de customização de playbooks através de linguagens de programação tais como JavaScript ou Mustache para criação de templates.

5.24.14. Deve fornecer um serviço HTTP server para receber informações através de um método POST e então converter o conteúdo recebido para JSON a fim de obter melhores integrações e expandir as capacidades com integrações web.

5.24.15. Deve suportar operações básicas no processamento de fluxo, como:

5.24.15.1. Realizar operações matemáticas básicas (+, -, *, /,%, **), suportando retornar o resultado com decimais ou números exatos (arredondados);

5.24.15.2. Suporte à pesquisa de arquivos, tipo de documento de conteúdo que corresponda a uma expressão regular. Deve suportar documentos do tipo: csv, doc, docx, eml, epub, gif, jpg, json, html, msg, odt, ogg, pdf, png, pptx, ps, rtf, tiff, txt, wav, xlsx, zip;

5.24.15.3. Programar a ocorrência de eventos no futuro semelhante para Windows ou Unix;

5.24.15.4. Conectar-se a um servidor IMAP e\ou POP3;

5.24.15.5. Executar localmente os seguintes comandos: Ping, Telnet para uma porta, traceroute, whois e\ou aguardar alguns segundos;

5.24.15.6. Exibir hora local;

5.24.15.7. Operar arquivos locais através das seguintes operações: criar arquivos, adicionar a um arquivo (anexar), excluir arquivos, mover arquivos, ler arquivos, listar diretórios etc.;

5.24.15.8. Ler um feed RSS;

5.24.15.9. Realizar uma captura de tela de uma página do site. Deve suportar o uso de proxy e permitir armazenar a imagem em um arquivo;

5.24.15.10. Enviar dados através de uma porta TCP;

5.24.15.11. Oferecer suporte ao SFTP, através das seguintes operações: Listar diretório, ver se existe um arquivo, ver se existe um diretório, buscar um arquivo, buscar um diretório e seu conteúdo recursivamente, fazer upload de um arquivo;

5.24.15.12. Enviar uma mensagem via SMTP;

5.24.15.13. Executar comandos remotamente via SSH e coletar a saída de execução assim como seus erros de execução;

5.24.15.14. Criar um elemento STIX a partir de um indicador de consolidação do índice de comprometimento (Hash, IP, URL, HostName, Domínio);

5.24.15.15. Gerar uma solicitação HTTP para uma API Web generic;

5.24.15.16. Oferecer suporte ao uso de cabeçalhos HTTP personalizados;

5.24.15.17. Importar arquivos a serem utilizados em ações do playbook;

5.24.15.18. Adicionar tags para fácil identificação de ativos envolvidos em um playbook;

5.24.15.19. Possuir a capacidade de executar sequências condicionais que mudem a direção ou fluxo de um playbook em execução.

5.24.16. Deve suportar a interpretação de dados como:

5.24.16.1. Extrair o domínio de uma URL;

5.24.16.2. Extrair o domínio de um email;

5.24.16.3. Extrair um ou mais URLs de um texto;

5.24.16.4. Codifique um texto em base64;

5.24.16.5. Decodifique base64 em texto;

5.24.16.6. Decodifique um texto JSON usando uma expressão jsonpath;

5.24.16.7. Extrair um subtexto do XML usando um filtro xpath;

5.24.16.8. Codifique uma string usando urlEncode;

5.24.16.9. Decodifique um URL usando urlDecode;

5.24.16.10. Resolver do IP para o domínio;

5.24.16.11. Resolver do domínio para o IP;

5.24.16.12. Converter de texto em campo Hash MD5;

5.24.16.13. Filtrar de uma lista de textos aqueles que contêm um determinado subtexto;

5.24.16.14. Aplicar uma substituição em expressão regular;

5.24.16.15. Verificar se um texto corresponde a uma determinada expressão regular;

5.24.16.16. Contar os itens em uma lista.

5.24.17. Deve suportar pelo menos os seguintes dispositivos:

5.24.17.1. Microsoft Active Directory

5.24.17.2. Microsoft Exchange

5.24.17.3. Microsoft NetBIOS

5.24.17.4. Microsoft SCCM

5.24.17.5. Microsoft SharePoint

5.24.17.6. Microsoft SMB

5.24.17.7. Microsoft Windows

5.24.17.8. Mozilla Firefox

5.24.17.9. Nmap

5.24.17.10. Palo Alto Networks Panorama

5.24.17.11. Solarwinds Log Manager

5.24.17.12. Splunk

5.24.17.13. SSH

5.24.17.14. Symantec Endpoint Protection

5.24.17.15. syslog-ng

5.24.17.16. Tenable SecurityCenter

5.24.17.17. VirusTotal

5.24.17.18. Wireshark

5.24.18. Deve possuir um guia de API bem documentado com diversas possibilidades de consumo não limitando-se há:

5.24.18.1. Listar requisições dos usuários;

5.24.18.2. Criar novas requisições;

5.24.18.3. Atualizar informações sobre requisições e chamados;

5.24.18.4. Enviar solicitação de troca de senha para usuário;

5.24.18.5. Deletar requisição;

5.24.18.6. Gerenciar e executar playbooks.

5.25. **Item 5 - Operação assistida**

5.25.1. Os Serviços deverão ser prestados no período das 8h00 às 18h00, de segunda-feira a sexta-feira, remotamente, nas dependências da CONTRATADA, conforme disposto no item 14 - Local para Execução dos Serviços e/ou Entrega dos Produtos.

5.25.2. A CONTRATADA deverá seguir o processo de mudança estabelecido pelo CONTRATANTE.

5.25.3. A CONTRATADA deverá implementar conceitos de Threat Hunting, monitorando de forma contínua todos os eventos correlacionados;

5.25.4. As manutenções preventivas e/ou corretivas, que representem risco de interrupção do(s) serviço(s), deverão ser agendadas e realizadas fora do horário regular, salvo quando expressamente autorizado;

5.25.5. As manutenções programadas, que impliquem em extensiva parada do ambiente serão realizadas durante um final de semana. Tais atividades realizadas fora do horário regular não ensejarão qualquer pagamento adicional em relação ao estabelecido no contrato, portanto a CONTRATADA deverá prever esta situação em sua composição de custos;

5.25.6. Todos os serviços de manutenção corretiva e preventiva são considerados de natureza contínua e deverão minimizar a necessidade de parada do ambiente em produção;

5.25.7. A contrata deverá de forma proativa, analisar políticas e processos de segurança relacionados as soluções contratadas, gerando propostas de melhorias contínuos.

5.25.8. Os serviços devem ser executados de acordo com normas, procedimentos e técnicas adotadas pelo CONFEA;

5.25.9. Deverá ser fornecido ao CONTRATANTE acesso à console dos produtos ofertados para que seja possível o acompanhamento, auditoria e direcionamento de ações no ambiente;

5.25.10. A CONTRATADA deverá comunicar a CONTRATANTE quanto ocorrência de qualquer incidente de segurança, seguido de todas as ações de remediação realizadas.

5.25.11. Os contatos para notificação de incidentes críticos ou fluxos para aprovação de ações serão documentados durante o período de implementação.

5.25.12. A CONTRATADA deverá assumir atividades de customização de interpretação de logs/eventos que possam não ser interpretados nativamente pelo SIEM. Tais atividades não deverão ter nenhum custo adicional.

5.25.13. A CONTRATADA deverá customizar e disponibilizar dashboards/relatórios solicitados pela CONTRATANTE. Essas visões serão armazenadas na console do SIEM e poderão ser consultadas a qualquer momento. Tais atividades não deverão ter nenhum custo adicional e serão realizadas dentro do horário comercial.

5.25.14. Sempre que necessário, a CONTRATADA deverá customizar regras de detecção, atendendo boas práticas de segurança da informação e também a demandas específicas da CONTRATANTE.

5.25.15. Qualquer atividade realizada fora do horário comercial não deverá atribuir nenhum custo adicional para a CONTRATANTE.

5.25.16. Qualquer atualização de plataformas envolvidas na contratação não deverá ter nenhum custo adicional para a CONTRATANTE.

5.25.17. A CONTRATADA deverá realizar ações referentes a resposta a incidentes de segurança, envolvendo sempre que necessário responsáveis por soluções de segurança administradas por time terceiros, com o objetivo de manter a disponibilidade e qualidade de todos os serviços tecnológicos.

5.25.18. Sempre que necessário envolvimento de times terceiros que administram outras soluções da CONTRATANTE, a CONTRATADA deverá enviar os incidentes preenchidos, analisados e contextualizados, apenas para tomada de decisão e/ou execução de ações pontuais.

5.25.19. Toda interação com times terceiros deverão ser realizadas por e-mail ou através da ferramenta de chamados da CONTRATANTE, ficando a cargo da CONTRATANTE definir qual meio será adotado.

5.25.20. A CONTRATADA deverá ter fluxos de resposta a incidentes bem definidos para os mais variados tipos de incidentes existentes.

5.25.21. A CONTRATADA deverá criar relatórios gerenciais a serem entregues mensalmente, visando acompanhamento eficaz quanto ao funcionamento de todas as plataformas contratadas.

5.25.22. Todas as ações de resposta a incidentes executadas pela CONTRATADA deverão ser armazenadas em procedimentos operacionais, para consultas sempre que necessário.

5.25.23. A contratada deverá detectar e reportar qualquer tipo de incidentes que tenham características de reincidência.

5.25.24. Serão considerados incidentes de segurança, as seguintes ações:

5.25.24.1. Aplicações maliciosas detectadas em estações de trabalho e servidores;

5.25.24.2. Exploração de vulnerabilidades;

5.25.24.3. Uso indevido de credenciais;

5.25.24.4. Phishing ou spam;

5.25.24.5. Ataques de Força Bruta;

5.25.24.6. Execução de códigos ou scripts maliciosos;

5.25.24.7. Ataques de saturação;

5.25.24.8. Comunicações com IPs ou domínios maliciosos;

5.25.25. Atividades que tenham o intuito de comprometer a integridade de ativos e entidades da CONTRATANTE;

5.25.26. Atividades que tenham o intuito de comprometer a confidencialidade de informações da CONTRATANTE;

5.25.27. Atividades que tenham o intuito de comprometer a disponibilidade dos serviços tecnológicos oferecidos pela CONTRATANTE.

5.25.28. A CONTRATADA deverá disponibilizar um canal, por e-mail, possibilitando que a CONTRATANTE comunique qualquer incidente de segurança não detectado por soluções de segurança existentes, para que as devidas investigações sejam realizadas.

5.25.29. A CONTRATADA deverá operar todas as plataformas contidas nesta contratação, de forma a realizar todas as atividades pertinentes as mesmas (Exceto ações de infraestrutura específicas administradas pela CONTRATANTE), seguindo melhores práticas recomendadas pelos fabricantes e potencializando ao máximo a capacidade de entrega de cada plataforma.

5.25.30. A CONTRATADA deverá entregar um relatório de implementação das soluções (as-built), contendo todos os passos realizados para implementação e configuração das soluções.

6. **BEM E/OU SERVIÇO COMUM**

6.1. (X) Sim ( ) Não

6.2. 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.

7. **CARACTERIZAÇÃO DO OBJETO**

7.1. **Serviço continuado:** (X) Sim ( ) Não

7.2. **Da justificativa:**

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

7.4. Não obstante, observa-se que a essencialidade atrela-se à necessidade de existência e manutenção do contrato, pelo fato de eventual paralisação do serviço contratado implicar em fragilizar a segurança na rede de dados do Confea, podendo trazer prejuízos imensuráveis e irreversíveis ao Confea.

7.5. 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:

> "*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*".

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

> "Voto do Ministro Relator
>
> [...]
>
> 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.)"

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

7.8. Ademais, como o serviço é de natureza continuada, verifica-se vantajosidade no aumento do prazo e/ou habilitar a possibilidade de renovação 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.

7.9. Havendo interrupção, comprometerá a segurança e as atividades da Administração e cuja necessidade de contratação deverá estender-se por mais de um exercício financeiro e continuamente, sendo essencial para a rotina e segurança institucional, pois não se trata de uma demanda momentânea, uma vez paralisada ela tende a acarretar danos ao Confea.

8. **FORMA DE CONTRATAÇÃO (MODALIDADE LICITATÓRIA)**

8.1. (X) Pregão na forma eletrônica:

8.1.1. **Da Justificativa**

8.1.1.1. Diz respeito à segurança física das máquinas e proteção dos dados, sendo imprescindível e necessária a contratação.

8.1.1.2. Justifica-se por ser um serviço continuado e de suma prioridade para a segurança e bom andamento dos trabalhos do Confea.

9. **CRITÉRIO DE JULGAMENTO / ESCOLHA DO LICITANTE**

9.1. (X) Menor preço global

9.2. ( ) Melhor técnica

9.3. ( ) Técnica e preço

10. **REGIME DE EXECUÇÃO**

10.1. ( ) Empreitada por preço unitário

10.2. (X) Empreitada por preço global

11. **FORMALIZAÇÃO DA CONTRATAÇÃO**

11.1. (X) Termo de Contrato

11.2. ( ) Nota de Empenho

12. **VALOR ESTIMADO PARA CONTRATAÇÃO**

12.1. Estima-se o valor global de contratação de **R$ 788.173,85 (setecentos e oitenta e oito mil cento e setenta e três reais e oitenta e cinco centavos) para 12 (dozes) meses**, conforme pesquisa de preço realizada pela unidade demandante, demonstrada no quadro abaixo:

					Empresa 01		Empres	
Item	Part Number	Descrição	Unidade	Quantidade	Valor Unitário	Valor Total	Valor Unitário	Va

					Empresa 01		Empres	
1	EP-E-P-2W-PTM-499-1Y	Solução de proteção avançada para endpoints	Estações e servidores	335	R$ 451,32	R$ 151.192,20	R$ 362,27	R 12
2	EM-U-CA-2W-PTM-499-1Y	Solução para proteção avançada de e-mail corporativo	Usuários	385	R$ 139,24	R$ 53.607,40	R$ 114,52	R 44
3	NW-3500-HWSVR	Solução de segurança de rede avançada contra APTs	Dispositivos	1	R$ 268.420,00	R$ 268.420,00	R$ 261.083,32	R 26
4	HELIX-E-PTM-499-1Y	Solução de gerenciamento, orquestração e validação de segurança	Eventos por segundo (EPS)	350	R$ 802,73	R$ 280.955,50	R$ 708,20	R 24
5	N/A	Operação assistida	Meses	12	R$ 13.520,00	R$ 162.240,00	R$ 7.500,00	R 90
						R$ 916.415,10		R 76

MÉDIO		MÍNIMO		MEDIANA	
458,42	153.570,03	349,99	117.246,65	371,24	124.365,40
148,08	57.012,34	104,77	40.336,45	123,37	47.497,45
329.281,95	329.281,95	261.083,32	261.083,32	270.111,00	270.111,00
898,29	314.402,20	708,20	247.870,00	732,00	256.200,00
10.519,00	126.228,00	6.950,00	83.400,00	7.500,00	90.000,00
	980.494,52		**749.936,42**		**788.173,85**

12.1.1. Através de levantamento de possíveis empresas para fornecimento dos objetos almejados, foram solicitadas cotações às empresas, resultando na seguinte estimativa preliminar de preços cujo valor global para contratação é de **R$ 788.173,85 (setecentos e oitenta e oito mil cento e setenta e três reais e oitenta e cinco centavos)**.

12.1.2. Registra-se que foram valorados dois cenários, vigência de 12 meses e de 24 meses. Não houve vantajosidade financeira ao se adotar 24 meses.

12.1.3. Visto se tratar sobre renovação de licenças para solução já existente no Confea via part number, e por ser um objeto no qual várias empresas podem ofertar, e cujas validades das propostas são de 90 dias, datadas de outubro, adotou-se a **Mediana** visando proporcionar maior competitividade e minimizar os riscos de fracasso do processo licitatório.

12.1.4. Justifica-se não adotar os valores unitários mínimos de cada empresa, visto que pode caracterizar o fracasso do projeto pelo fato da possibilidade das empresas não serem aptas a executar o objeto pelo preço final, e nem sequer efetuar lances no certame licitatório, como já acontecido em pregões anteriores neste Confea.

13. DOTAÇÃO ORÇAMENTÁRIA

13.1. A despesa orçamentária para a contratação do objeto deste instrumento correrá no Centro de Custo 4.01.01.03 - SEG.

13.2. Informamos que não houve aquisições/contratações do objeto pretendido no exercício.

14. LOCAL PARA EXECUÇÃO DOS SERVIÇOS E/OU ENTREGA DOS PRODUTOS

14.1. Os produtos/serviços deverão ser entregues/executados com a previsão de 02 (dois) dias úteis após a assinatura do contrato para iniciar os serviços de configuração e 45 (quarenta e cinco) dias, após o início, para conclusão da implementação, na sede do Confea, localizado no SEPN 508, Bloco A, Edifício Engenheiro Francisco Saturnino de Brito Filho, Asa Norte, Brasília – DF.

14.2. 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.

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

14.4. Como padrão e quando não especificado em contrário, considerar-se-á como dia útil o período de 10 horas úteis, das 8h00 às 18h00, de segunda a sexta-feira, nos dias em que houver expediente no Confea. Considerar-se-á hora útil o intervalo de uma hora dentro de um dia útil.

14.5. 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.

15. PRAZO DE VIGÊNCIA E EXECUÇÃO

15.1. A vigência do contrato será de 12 (doze) meses, contados da data da assinatura do contrato, podendo ser prorrogado até 48 (quarenta e oito) meses, com base na legislação vigente no artigo 57, IV, da Lei 8.666, de 1993, dado que se trata de serviço continuado de utilização de programas de informática.

16. CRITÉRIOS TÉCNICOS PARA SELEÇÃO DO FORNECEDOR

16.1. 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. Comprovação de experiência mínima na execução de serviços semelhantes ao objeto da licitação.

16.3. 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.

16.4. 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 01, de 2019**.

17. VISTORIA OU VISITA TÉCNICA

17.1. Não se aplica.

18. **AMOSTRA E/OU LAUDO TÉCNICO**

18.1. Não se aplica

19. **PROVA DE CONCEITO E TESTE DE CONFORMIDADE**

19.1. Não se aplica.

20. **JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO**

20.1. O objeto não poderá ser parcelado em virtude das seguintes justificativas:

20.2. A adjudicação do certame para um único vencedor visa resguardar a efetividade do processo de aquisição;

20.3. A contratação global oferta condições mais vantajosas para a Administração do que a contratação por itens, com isso, o objeto não foi parcelado.

21. **GARANTIA DO CONTRATO**

21.1. A (s) contratada (s) deverá (ão) 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:

21.2. caução em dinheiro ou títulos da dívida pública;

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

21.4. seguro-garantia; ou

21.5. fiança bancária.

21.6. 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).

21.7. 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.

21.8. O bloqueio efetuado com base no item 21.3 desta cláusula não gera direito a nenhum tipo de compensação financeira à contratada.

21.9. A contratada, a qualquer tempo, poderá substituir o bloqueio efetuado com base no item 21.3 desta cláusula por quaisquer das modalidades de garantia, caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

22. **OBRIGAÇÕES DO CONTRATANTE**

22.1. Fazer cumprir fielmente as cláusulas do contrato;

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

22.3. 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;

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

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

22.6. 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;

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

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

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

22.10. 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.

23. **OBRIGAÇÕES DA CONTRATADA**

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

23.2. Observar as normas e regulamentos internos do contratante, bem como fazer com que seus empregados os observem;

23.3. 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 modalidades previstas na Lei nº 8.666, de 21 de junho de 1993;

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

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

23.6. 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;

23.7. 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;

23.8. Manter seus empregados devidamente identificados por crachás, desde o primeiro dia de trabalho nas dependências do contratante (será de inteira responsabilidade da contratada o cuidado na apresentação pessoal de seus empregados);

23.9. Exercer controle sobre a assiduidade e a pontualidade de seus empregados, substituindo qualquer empregado no caso de falta, ausência legal ou férias, de maneira que não prejudique o andamento e a boa execução dos serviços;

23.10. A contratada deverá fornecer escala nominal de férias, licenças, ausências justificadas dos prestadores de serviço e os respectivos substitutos, bem como substituição de profissional;

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

23.12. 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;

23.13. 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;

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

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

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

23.17. 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;

23.18. 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;

23.19. 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;

23.20. Estabelecer outros critérios, pertinentes à especificidade do objeto.

24. PAGAMENTO

24.1. Mediante a entrega dos produtos, o pagamento será feito em uma única vez, no prazo de **15 (quinze) dias úteis**, contado da data da atestação da nota fiscal/fatura (**itens 1 a 4**).

24.2. Mediante a prestação dos serviços, o pagamento será mensal para, no prazo de **15 (quinze) dias úteis**, contado da data da atestação da nota fiscal/fatura (**item 5**).

24.3. Serão adotados os documentos "Ordem de Serviço", "Termo de Recebimento Provisório" e "Termo de Recebimento Definitivo" para fins de pagamento, conforme disposto nos itens e subitens da seção "Mecanismos Formais de Comunicação".

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

24.5. A nota fiscal/fatura deverá ser acompanhada dos documentos que comprovem a sua regularidade fiscal, compreendendo INSS, FGTS, Receita Federal/ Municipal, Dívida Ativa da União, CNDT e Nada Consta de Falência.

24.6. A nota fiscal/fatura, que será emitida sem rasura, legível, em nome da Contratante, CNPJ, da qual constará o número do contrato e as informações para crédito em conta corrente:

24.7. nome e número do banco, nome e número da agência e número da conta;

24.8. a primeira via do documento fiscal de eventual fornecedor;

24.9. os documentos de comprovação de serviços executados por terceiros, da execução dos serviços, e quando for o caso, do comprovante de sua entrega.

25. DO REAJUSTE

25.1. O contrato poderá ser reajustado nos termos da Lei nº 10.192/2001 e do disposto na Lei nº 8.666/1993, com a finalidade de neutralizar os efeitos da inflação sobre a equação econômico-financeira estabelecida;

25.2. A periodicidade anual para a concessão dos reajustes será considerada conforme rege a Lei nº 10.192/2001, conforme art. 3°, §1°;

25.3. Para o reajuste será considerado o Índice de Custos de Tecnologia da Informação - ICTI, conforme previsão expressa contida no art. 24 da instrução Normativa SGD/ME nº 01, de 2019;

25.4. 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.

25.5. 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.

25.6. 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.

26. PENALIDADES ADMINISTRATIVAS

26.1. 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:

26.1.1. apresentar documentação falsa;

26.1.2. fraudar a execução do contrato;

26.1.3. comportar-se de modo inidôneo;

26.1.4. cometer fraude fiscal; ou

26.1.5. fizer declaração falsa.

26.2. Para os fins do item 26.1.3, 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.

26.3. 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 itens 26.4, 26.5 e 26.6 abaixo, com as seguintes penalidades:

26.4. advertência;

26.5. suspensão temporária de participação em licitação e impedimento de contratar com a Administração do Confea, por prazo não superior a dois anos;

26.6. declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a contratada ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior; ou

26.7. 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.

26.8. 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.

26.9. 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.

26.10. Em caso de inexecução total do objeto, a contratada fica sujeita à multa de, no máximo, 30% (trinta por cento) do valor do contrato.

26.11. 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.

26.12. O não-cumprimento de obrigação contratual acessória, a exemplo da garantia exigida no Item 21 (Garantia do Contrato), sujeitará a contratada à multa de até 10% (dez por cento) do valor empenhado.

26.13. A falha na execução do contrato estará configurada quando a contratada se enquadrar em qualquer das situações previstas na tabela 02, a seguir.

26.14. 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				
(X)	**ITEM**	**DETALHAMENTO DA INFRAÇÃO**	**GRAU**	**INCIDÊNCIA**
X	**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
X	**B**	Fornecer produtos com especificação e qualidade diversa e/ou inferior a demandada.	03	Por produto
X	**C**	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratados.	03	Por dia
X	**D**	Recusar a execução de serviço determinado pela fiscalização, sem motivo justificado.	02	Por ocorrência
X	**E**	Destruir ou danificar documentos por culpa ou dolo de seus agentes.	02	Por ocorrência
	F	Permitir situação que crie a possibilidade de causar ou que cause dano físico, lesão corporal ou consequências letais.		
X	**G**	Não manter as condições de habilitação originárias da contratação.	02	Por ocorrência
X	**H**	Descumprir qualquer das obrigações contratuais previstas no Termo de Referência e seus anexos.	01	Por ocorrência
X	**I**	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
X	**J**	Não observar os prazos para execução dos serviços e/ou entrega de produtos.	01	Por dia

	K	Permitir a presença de empregado não uniformizado ou com uniforme manchado, sujo, mal apresentado e/ou sem crachá.		
X	L	Não fornecer os materiais e equipamentos, ferramentas e produtos necessários à completa execução do objeto.	01	Por ocorrência
X	N	Não prestar as informações e os esclarecimentos que venham a ser solicitados.	01	Por ocorrência
X	N	Não apresentar, quando solicitado, documentação fiscal, trabalhista, previdenciária e outros documentos necessários à habilitação.	01	Por ocorrência

26.15. O valor da multa poderá ser descontado das faturas devidas à contratada.

26.16. Se o valor a ser pago à contratada não for suficiente para cobrir o valor da multa, a diferença será descontada da garantia contratual.

26.17. 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.

26.18. Esgotados os meios administrativos para cobrança do valor devido pela contratada ao contratante, aquela será encaminhada para inscrição em dívida ativa.

26.19. 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.

26.20. 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.

26.21. 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).

26.22. 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.

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

27. MODELO DE EXECUÇÃO DO CONTRATO

27.1. A Instrução Normativa nº 1, de 4 de abril de 2019, dispõe que "Art. 18. O Modelo de Execução do Contrato deverá contemplar as condições necessárias ao fornecimento da solução de TIC, observando, quando possível":

27.1.1. 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;

27.1.1.1. Consoante itens "Prazo de Vigência e Execução" e 17 "Local para execução dos serviços e/ou entrega dos produtos" deste Termo de Referência.

27.1.2. 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 pela 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.; e

27.1.2.1. Consoante itens "Critérios Técnicos para seleção do fornecedor" e "Especificações dos Requisitos da Contratação" deste Termo de Referência.

27.1.3. 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 da contratante e da contratada, quando couber;

27.1.3.1. Consoante item "Modelo de Gestão do Contrato" deste Termo de Referência.

27.1.4. II - quantificação ou estimativa prévia do volume de serviços demandados ou quantidade de bens a serem fornecidos, para comparação e controle;

27.1.4.1. Consoante item "Justificativa para a contratação/aquisição" deste Termo de Referência.

27.1.5. 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;

27.1.5.1. Consoante item "Mecanismos formais de comunicação" deste Termo de Referência.

27.1.6. IV - forma de pagamento, que será efetuado em função dos resultados obtidos; e

27.1.6.1. Consoante item "Pagamento" deste Termo de Referência.

27.1.7. 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

27.1.7.1. Consoante Anexo I deste Termo de Referência.

27.1.8. 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.

27.1.8.1. Consoante Anexo II deste Termo de Referência.

27.2. A empresa contratada deverá seguir o modelo de execução contratual conforme o objeto.

28. MODELO DE GESTÃO DO CONTRATO

28.1. A Instrução Normativa nº 1, de 4 de abril de 2019, dispõe que "Art. 19. O Modelo de Gestão do Contrato, definido a partir do Modelo de Execução do Contrato, deverá contemplar as condições para gestão e fiscalização do contrato de fornecimento da solução de TIC, observando":

28.1.1. 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;

28.1.1.1. Consoante item "Especificações dos Requisitos da Contratação" deste Termo de Referência.

28.1.2. 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 vistas de verificação e de roteiros de testes para subsidiar a ação dos Fiscais do contrato; e 5. garantia de inspeções e diligências, quando aplicáveis, e suas formas de exercício;

28.1.2.1. Consoante item "Especificações dos Requisitos da Contratação" deste Termo de Referência.

28.1.3. 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;

28.1.3.1. Através da elaboração de Portaria com a designação de Equipe de Fiscalização do Contrato pelo Confea embasado nas especificações técnicas contidas no item "Especificações dos Requisitos da Contratação" deste Termo de Referência.

28.1.4. 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;

28.1.4.1. Consoante item "Pagamento" deste Termo de Referência.

28.1.5. 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;

28.1.5.1. Consoante item "Penalidade Administrativas" deste Termo de Referência.

28.1.6. V - procedimentos para o pagamento, descontados os valores oriundos da aplicação de eventuais glosas ou sanções.

28.1.6.1. Consoante itens "Pagamento" e "Penalidades Administrativas" deste Termo de Referência.

28.2. A fiscalização do cumprimento das obrigações contratuais será exercida por empregados devidamente designados pela 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.

28.3. A equipe de fiscalização do CONTRATO, atuando nos termos dos artigos 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.

28.3.1. A Equipe de fiscalização 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.

28.3.2. A fiscalização acima mencionada não exclui e nem reduz a responsabilidade da empresa Contratada, inclusive perante terceiros, por qualquer irregularidade na execução dos serviços.

28.3.3. 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.

28.3.4. 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.

28.3.5. A fiscalização poderá esclarecer ou requerer correções de incoerências, falhas e omissões eventualmente constatadas.

28.3.6. A fiscalização exercerá rigoroso controle sobre o cronograma de execução dos serviços, para evitar atraso no cumprimento dos trabalhos.

28.4. Para o caso de impedimento de qualquer dos empregados indicados para as funções de fiscalização, serão designados pela CONTRATANTE empregados para atuar como substitutos.

28.5. 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:

28.5.1. presença do representante legal da CONTRATADA, que apresentará o preposto;

28.5.2. 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

28.5.3. esclarecimentos relativos a questões operacionais, administrativas e de gestão do CONTRATO.

28.6. 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.

28.7. Caberá à CONTRATADA o pronto atendimento às exigências inerentes ao objeto contratado, feitas pelo Gestor do Contrato ou por seu substituto.

28.8. 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 da CONTRATANTE (art. 70 da Lei nº 8.666/93).

28.9. A 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).

28.10. 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.

28.11. 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.

28.12. Em hipótese alguma, será admitido que a própria Contratada materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

28.13. 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.

28.14. 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.

29. **MECANISMOS FORMAIS DE COMUNICAÇÃO**

29.1. 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.

29.2. 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.

29.3. 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.

29.3.1. Na mesma ocasião, a CONTRATANTE informará os contatos do Gestor e dos demais fiscais.

29.4. A Ordem de Serviço é o instrumento formal pelo qual o Confea encaminha a demanda de serviço para a CONTRATADA.

29.5. 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.

29.6. As Ordens de Serviço serão emitidas, acompanhadas, revisadas e recebidas (aceitas) pelo Confea.

29.7. 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.

29.8. 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.

29.9. As Ordens de Serviço serão recebidas pelo Confea tanto em caráter provisório como em definitivo.

29.10. **Do Termo de Recebimento Provisório do objeto e da avaliação de qualidade e conformidade.**

29.10.1. 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° 01/2019: "**Termo de Recebimento Provisório** - declaração formal de que os serviços foram prestados ou os bens foram entregues, para posterior análise das conformidades e qualidades baseadas nos requisitos e nos critérios de aceitação, 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";

29.11. Após a execução dos serviços previstos para a Ordem de Serviço, será emitido o Termo de Recebimento Provisório no prazo de até **05 (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.

29.12. O recebimento provisório será realizado pelo fiscal técnico do contrato quando da entrega do objeto resultante de cada etapa de serviço. Após o aceite, consistirá na emissão do termo de recebimento provisório.

29.13. Os serviços entregues serão objeto de avaliação e aprovação pela equipe do Confea.

29.14. Será comunicada formalmente à CONTRATADA a não conformidade dos produtos.

29.15. Os bens 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 da contratante.

29.16. 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.

29.17. **Do Termo de Recebimento Definitivo.**

29.17.1. 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° 01/2019: "**Termo de Recebimento Definitivo** - declaração formal de que os serviços prestados ou bens fornecidos atendem aos requisitos estabelecidos e aos critérios de aceitação, 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".

29.17.2. Concluída a avaliação da qualidade e da conformidade dos serviços/produtos e de sua entrega, o gestor do contrato efetuará o recebimento definitivo dos serviços por meio do termo de recebimento definitivo, com base nas informações da etapa de avaliação da qualidade, contendo a autorização para emissão de nota(s) fiscal(is), a ser encaminhado ao preposto da contratada.

29.17.3. No prazo de até **10 (dez) dias úteis**, contados do recebimento provisório, após a verificação da qualidade e quantidade do(s) bens constantes neste instrumento, o objeto será recebido definitivamente, a respectiva Nota Fiscal atestada e o processo encaminhado para pagamento.

29.17.4. 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.

29.17.5. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

29.18. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

29.19. 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.

29.20. A Ordem de Serviço poderá ser replanejada a qualquer momento a critério do Confea, sendo registrada formalmente tal ação.

29.21. 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.

30. **SIGILO DAS INFORMAÇÕES**

30.1. Na execução dos serviços descritos neste Termo de Referência, a Contratada terá acesso a informações críticas do Sistema Confea/Crea, cabendo à Contratada:

30.1.1. Assinar e cumprir o Termo de Compromisso e Manutenção do Sigilo, conforme modelo constante no Anexo I;

30.1.2. Guardar sigilo das informações que receber durante a execução do contrato;

30.1.3. Responsabilizar-se pela divulgação não autorizada ou pelo uso indevido de qualquer informação pertinente ao Sistema Confea/Crea.

30.2. Caso se verifique a quebra de sigilo das informações disponibilizadas pelo Confea, serão aplicadas as sanções cabíveis.

31. **MAPA DE GERENCIAMENTO DE RISCOS**

31.1. A Instrução Normativa nº 1, de 4 de abril de 2019, 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 ou Projeto Básico; II - ao final da fase de Seleção do Fornecedor; III - uma vez ao ano, durante a gestão do contrato; e IV - após eventos relevantes".

31.2. 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. § 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".

31.3. Cumprindo com o disposto no artigo 38 da Instrução Normativa nº 01, de 2019, 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.

31.4. Para tal, foram utilizadas as definições constantes nas tabelas abaixo e que referem-se à descrição das probabilidades e dos impactos.

DESCRIÇÃO DAS PROBABILIDADES E IMPACTOS

Tabela - Risco de ocorrência de eventos

Probabilidade (Risco referencial)	Observações
Alta	A probabilidade de ocorrer é grande.
Média	A probabilidade de ocorrer ou não é equivalente.
Baixa	A probabilidade de ocorrer é pequena.

Tabela - Avaliação do Impacto

Impacto	Observações
Muito grande	Perda do recurso orçamentário; má aplicação de recursos públicos; indisponibilidade de todos os serviços ou perda de dados.
Grande	Perda do processo licitatório; degradação crítica do desempenho, indisponibilidade ou falhas graves em vários serviços, em algum(ns) serviço(s) essencial(is) ou equipamentos.
Moderado	Degradação moderada do desempenho ou falhas contornáveis de alguns serviços ou equipamentos, em um serviço essencial ou equipamentos.
Pequeno	Degradação leve do desempenho ou falhas contornáveis em serviços ou equipamentos não essenciais.
Muito pequeno	Degradação leve do desempenho em um serviço não essencial ou no fornecimento de produtos ou equipamentos.

31.5. **Fase do Planejamento da Contratação**

31.5.1. Risco 01: Equívocos na descrição do objeto.

31.5.2. Risco 02: Elaboração falha da estimativa e/ou estimativa de preço em descompasso com os valores praticados no mercado.

31.5.3. Risco 03: Erros materiais/formais no termo de referência.

31.5.4. Risco 04: Ciclo total do processo de contratação ultrapassar a data final do atual contrato.

31.5.5. Risco 05: Existência de outras demandas prioritárias de contratações.

31.5.6. Risco 06: Necessidade de adequação do Termo de Referência.

Risco 01: Equívocos na descrição do objeto		
Probabilidade		( ) Baixa (X) Média ( ) Alta
Impacto		( ) Muito Grande ( ) Grande (X) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Atraso na realização da contratação pleiteada	
2	Obsolescência de equipamentos ou serviços descontinuados	
ID	**Ação Preventiva**	**Responsáveis**
1	Realização de pesquisa intensa no mercado	Integrante Requisitante Integrante Técnico
ID	**Ação de Contingência**	**Responsáveis**
1	Análise das impugnações e recursos dos Editais para as devidas correções	Integrante Requisitante Integrante Técnico
2	Pesquisa de mercado	Integrante Requisitante Integrante Técnico
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Pessoal: Não observância dos requisitos mínimos do equipamento ou serviço	

2	Pessoal: Ausência de pesquisa no mercado potencial das melhores práticas e produtos
3	Processo: Ausência de um Manual de Produtos e Serviços de Tecnologia da Informação

Risco 02: Elaboração falha da estimativa e/ou estimativa de preço em descompasso com os valores praticados no mercado		
Probabilidade		( ) Baixa (X) Média ( ) Alta
Impacto		( ) Muito Grande (X) Grande ( ) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Atraso na realização da contratação pleiteada	
2	Licitação deserta (descontinuidade do serviço) ou contratação por preço elevado, exigências de qualificação técnica	
ID	**Ação Preventiva**	**Responsáveis**
1	Realização de pesquisa extensa no mercado	Integrante Requisitante Integrante Técnico
ID	**Ação de Contingência**	**Responsáveis**
1	Análise das impugnações e recursos dos Editais para as devidas correções	Integrante Requisitante Integrante Técnico
2	Pesquisa de mercado quanto aos preços praticados	Integrante Requisitante Integrante Técnico
3	No caso de preço elevado, deve o pregoeiro negociar a redução dos valores propostos, tendo como parâmetro os valores do contrato atual.	Pregoeiro
4	No caso de licitação deserta, avaliar a possibilidade de proceder à contratação direta por dispensa de licitação	Setor de Licitações do Confea Procuradoria Jurídica do Confea
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Pessoal: Não atendimento do mínimo de 3 (três) orçamentos	
2	Processo: Ausência de preços públicos	
3	Processo: Ausência de um Catálogo de fornecedores vinculado ao Manual de Produtos e Serviços de TI	

Risco 03: Erros materiais/formais no termo de referência		
Probabilidade		(X) Baixa ( ) Média ( ) Alta
Impacto		( ) Muito Grande ( ) Grande (X) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Retrabalho e atraso na realização da contratação pleiteada	
ID	**Ação Preventiva**	**Responsáveis**
1	Estabelecer no Termo de Referência ou Projeto Básico que haja suporte técnico e manutenção para os equipamentos adquiridos	Integrante Requisitante Integrante Técnico
2	Realização de interações com os demais setores do Confea para elaboração dos Termos de Referência ou Projetos Básico e demais documentos necessários ao processo	Integrante Requisitante Integrante Técnico Integrante Administrativo
ID	**Ação de Contingência**	**Responsáveis**
1	Análise das impugnações e recursos dos Editais para as devidas correções	Integrante Requisitante Integrante Técnico
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Pessoal: Não atendimento à estrutura formalizada dos documentos	
2	Processo: Elaboração do Termo de Referência ou Projeto Básico sem interação com outros setores	

Risco 04: Ciclo total do processo de contratação ultrapassar a data final do atual contrato		
Probabilidade		( ) Baixa (X) Média ( ) Alta
Impacto		(X) Muito Grande ( ) Grande ( ) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Atraso no procedimento licitatório	
ID	**Ação Preventiva**	**Responsáveis**
1	Dedicação prioritária da equipe	Integrante Requisitante Integrante Técnico Integrante Administrativo
2	Abertura de canal direto e realização de reuniões frequentes com a equipe para agilizar o trâmite administrativo da contratação	Integrante Requisitante Integrante Técnico Integrante Administrativo
3	Iniciar a elaboração dos estudos técnicos preliminares e termo de referência com a antecedência necessária	Integrante Requisitante Integrante Técnico Integrante Administrativo
ID	**Ação de Contingência**	**Responsáveis**
1	Negociação com a atual contratada para que aceite a prorrogação contratual por um prazo suficiente para o término do processo da nova contratação	Fiscal Requisitante Fiscal Técnico Fiscal Administrativo
2	Realização de contratação emergencial	Fiscal Requisitante Fiscal Técnico Fiscal Administrativo Setor de Licitações do Confea
3	Alocação dos empregados com capacitação técnica para atender as demandas mais emergenciais, enquanto a contratação nova não se inicia	Área Requisitante Área Técnica
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Pessoal: Falta de planejamento do Gestor da unidade e da Equipe constituída	

Risco 05: Existência de outras demandas prioritárias de contratações		
Probabilidade		( ) Baixa ( ) Média (X) Alta
Impacto		(X) Muito Grande ( ) Grande ( ) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Não possibilidade de condução do processo desejado	
ID	**Ação Preventiva**	**Responsáveis**
1	Definir cronograma de trabalho geral do Setor de Licitações e Contrato e priorizar ou delegar a atividade	Superintendência de Estratégia e Gestão Setor de Licitações e Contrato
ID	**Ação de Contingência**	**Responsáveis**
1	Redefinição de prioridades entre as Superintendências	Superintendência de Estratégia e Gestão Superintendência Administrativa e Financeira
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Pessoal: equipes com poucos empregados e sobrecarga de trabalho	

Risco 06: Necessidade de adequação do Termo de Referência		
Probabilidade		( ) Baixa ( ) Média (X) Alta
Impacto		( ) Muito Grande (X) Grande ( ) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Morosidade no processo licitatório	

2	Retrabalho à Equipe de Planejamento da Contratação	
ID	**Ação Preventiva**	**Responsáveis**
1	Promover alinhamentos gerais junto ao Setor de Licitações e Contratos e à Procuradoria Jurídica do Confea	Integrante Administrativo Integrante Técnico Integrante Administrativo
ID	**Ação de Contingência**	**Responsáveis**
1	Avaliar as necessidades de alterações e promove-las com brevidade e segurança	Integrante Administrativo Integrante Técnico Integrante Administrativo
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Processo: falta de unicidade de ações entre as unidades do Confea	

31.6. **Fase da Seleção do Fornecedor**

31.6.1. Risco 01: Morosidade no processo licitatório.

31.6.2. Risco 02: Impropriedades do processo licitatório.

31.6.3. Risco 03: Fracasso/deserto no processo licitatório.

31.6.4. Risco 04: Impugnação do edital.

31.6.5. Risco 05: Proposta do pregão com valor superior ao estimado.

31.6.6. Risco 06: Apresentação de recurso.

Risco 01: Morosidade no processo licitatório		
Probabilidade		(X) Baixa ( ) Média ( ) Alta
Impacto		( ) Muito Grande ( ) Grande (X) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Atraso na realização da contratação pleiteada	
ID	**Ação Preventiva**	**Responsáveis**
1	Acionar as áreas envolvidas na contratação quando se verificar demora demasiada em determinada fase	Ocupantes de cargos com poder de decisão
2	Estabelecer normativamente os prazos para a entrega de documentos	Integrante Requisitante Integrante Técnico Integrante Administrativo
ID	**Ação de Contingência**	**Responsáveis**
1	Atender com celeridade as demandas da Licitação	Integrante Requisitante Integrante Técnico Integrante Administrativo
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Processo: Ausência de prazos definidos na fase externa do processo administrativo de contratação em TI	
2	Processo: Ausência dos fluxogramas dos processos de contratação em TI	

Risco 02: Impropriedades do processo licitatório		
Probabilidade		(X) Baixa ( ) Média ( ) Alta
Impacto		( ) Muito Grande ( ) Grande (X) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Retrabalho e atraso na realização da contratação pleiteada	
ID	**Ação Preventiva**	**Responsáveis**
1	Seguir a legislação relacionada às contratações em geral e contratações de bens e serviços de TI	Integrante Requisitante Integrante Técnico Integrante Administrativo
2	Atender as recomendações do Controle Interno	Integrante Requisitante Integrante Técnico Integrante Administrativo
3	Agir com transparência e velar pela aplicação dos princípios norteadores da Administração Pública	Integrante Requisitante Integrante Técnico Integrante Administrativo

ID	Ação de Contingência	Responsáveis
1	Atender com celeridade as demandas da Licitação	Integrante Requisitante Integrante Técnico Integrante Administrativo
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Pessoal: Inobservância das legislações e princípios relacionados às contratações em TI	
2	Processo: Falta de controle das recomendações do Controle Interno	

Risco 03: Fracasso/Deserto no processo licitatório		
Probabilidade		(X) Baixa ( ) Média ( ) Alta
Impacto		( ) Muito Grande (X) Grande ( ) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Retrabalho para novo procedimento licitatório	
2	Anulação do processo de contratação pleiteada	
ID	**Ação Preventiva**	**Responsáveis**
1	Seguir a legislação relacionada às contratações em geral e contratações de bens e serviços de tecnologia da informação	Integrante Requisitante Integrante Técnico Integrante Administrativo
2	Proceder à especificação dos itens de forma que a maior quantidade possível de licitantes possa participar do certame	Integrante Requisitante Integrante Técnico
3	Seguir o trâmite administrativo para aprovação de documentos referentes à contratação	Integrante Requisitante Integrante Técnico Integrante Administrativo
4	Dar ampla publicidade ao edital	Setor de Licitações do Confea
ID	**Ação de Contingência**	**Responsáveis**
1	Atender com celeridade as demandas da Licitação	Integrante Requisitante Integrante Técnico Integrante Administrativo
2	Correção da documentação pertinente, estimativa e outros documentos necessários ao processo	Integrante Requisitante Integrante Técnico Integrante Administrativo
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Pessoal: Inobservância de preços públicos e requisitos mínimos necessários	
2	Pessoal: Especificações limitadas dos produtos e serviços do mercado	
3	Pessoal: Documentação elaborada sem observância das normas	

Risco 04: Impugnação do edital		
Probabilidade		( ) Baixa ( ) Média (X) Alta
Impacto		(X) Muito Grande ( ) Grande ( ) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Atraso no procedimento licitatório	
ID	**Ação Preventiva**	**Responsáveis**
1	Análise pormenorizada dos itens exigidos no Edital de forma a não extrapolar as regulamentações previstas em Lei	Integrante Requisitante Integrante Técnico Integrante Administrativo
2	Especificar o serviço de forma concisa e coerente com o que o mercado pode oferecer	Integrante Requisitante Integrante Técnico Integrante Administrativo
3	Observar atentamente as regulamentações e instruções na condução do processo licitatório	Integrante Requisitante Integrante Técnico Integrante Administrativo
ID	**Ação de Contingência**	**Responsáveis**
1	Adotar as providências necessárias ao saneamento do processo no curto prazo, se possível, de modo a permitir a realização da licitação	Integrante Requisitante Integrante Técnico Integrante Administrativo

Causas (Fonte + Vulnerabilidades)	
ID	**Descrição**
1	Planejamento: Falha na elaboração do Estudo Técnico Preliminar e do Termo de Referência por não abranger um amplitude maior de fornecedores e soluções

Risco 05: Proposta do pregão com valor superior ao estimado		
Probabilidade		(X) Baixa ( ) Média ( ) Alta
Impacto		( ) Muito Grande ( ) Grande (X) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Atraso na realização da contratação pleiteada	
ID	**Ação Preventiva**	**Responsáveis**
1	Acionar as áreas envolvidas na contratação quando se verificar demora demasiada em determinada fase	Ocupantes de cargos com poder de decisão
2	Estabelecer normativamente os prazos para a entrega de documentos	Integrante Requisitante Integrante Técnico Integrante Administrativo
ID	**Ação de Contingência**	**Responsáveis**
1	Atender com celeridade as demandas da Licitação	Integrante Requisitante Integrante Técnico Integrante Administrativo
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Processo: Ausência de prazos definidos na fase externa do processo administrativo de contratação em TI	
2	Processo: Ausência dos fluxogramas dos processos de contratação em TI	

Risco 06: Apresentação de recurso		
Probabilidade		( ) Baixa ( ) Média (X) Alta
Impacto		(X) Muito Grande ( ) Grande ( ) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Atraso na realização da contratação pleiteada	
ID	**Ação Preventiva**	**Responsáveis**
1	Acionar as áreas envolvidas na contratação quando se verificar demora demasiada em determinada fase	Ocupantes de cargos com poder de decisão
2	Estabelecer normativamente os prazos para a entrega de documentos	Integrante Requisitante Integrante Técnico Integrante Administrativo
ID	**Ação de Contingência**	**Responsáveis**
1	Atender com celeridade as demandas da Licitação	Integrante Requisitante Integrante Técnico Integrante Administrativo
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Processo: Ausência de prazos definidos na fase externa do processo administrativo de contratação em TI	
2	Processo: Ausência dos fluxogramas dos processos de contratação em TI	

31.7. **Fase da Contratação da Solução**

31.7.1. Risco 01: Não assinatura do contrato.

31.7.2. Risco 02: Atraso no fornecimento do objeto.

31.7.3. Risco 03: Equipamentos/softwares não possuem as funcionalidades exigidas.

31.7.4. Risco 04: Inexecução total do contrato.

31.7.5. Risco 05: Inexecução parcial do contrato.

31.7.6. Risco 06: Equipe técnica da contratada.

Risco 01: Não assinatura do contrato		
Probabilidade		(X) Baixa ( ) Média ( ) Alta
Impacto		(X) Muito Grande ( ) Grande ( ) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Atraso na realização da contratação pleiteada	
2	Revogação da contratação	
ID	**Ação Preventiva**	**Responsáveis**
1	Convocar, dentro do prazo e condições estabelecidas, o interessado para assinar o contrato	Setor de Licitações do Confea
2	Elaborar e promover a gestão orçamentária e financeira por meio de um plano de despesas orçamentárias anuais da GTI	Ocupantes de cargos com poder de decisão Fiscal Requisitante
ID	**Ação de Contingência**	**Responsáveis**
1	Convocar, dentro do prazo e condições estabelecidas, os licitantes remanescentes para manifestar o interesse de assinar o termo de contrato	Setor de Licitações do Confea
2	Realizar a gestão orçamentária e financeira junto às instâncias necessárias para realização de despesas	Superintendência de Estratégia e Gestão
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Fator externo: Desistência do fornecedor em atender as demandas	
2	Fator externo: Falta de recurso orçamentário e financeiro para atendimento da contratação	

Risco 02: Atraso no fornecimento do objeto		
Probabilidade		( ) Baixa (X) Média ( ) Alta
Impacto		( ) Muito Grande (X) Grande ( ) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Contratação com início postergado	
2	Paralisação de serviços ou inutilização de equipamentos	
3	Provimento extemporâneo dos setores demandantes	
4	Impossibilidade do fornecedor efetivar as entregas	
ID	**Ação Preventiva**	**Responsáveis**
1	Estabelecer um prazo razoável para entrega dos objetos licitados	Integrante Requisitante Integrante Técnico Integrante Administrativo
2	Estabelecer penalizações por atrasos, na forma prevista no instrumento convocatório ou no contrato	Integrante Requisitante Integrante Técnico Integrante Administrativo
3	Realizar um estudo técnico preliminar sobre a estrutura tecnológica do Confea	Integrante Requisitante Integrante Técnico Integrante Administrativo
ID	**Ação de Contingência**	**Responsáveis**
1	Aplicar penalizações por atrasos, na forma prevista no instrumento convocatório ou no contrato	Fiscal Requisitante Fiscal Técnico Fiscal Administrativo
2	Efetivar ações junto aos fornecedores para entrega dos equipamentos e início dos serviços	Fiscal Requisitante Fiscal Técnico Fiscal Administrativo
3	Agilizar as adaptações da estrutura para entrega dos produtos e início dos serviços	Fiscal Requisitante Fiscal Técnico Fiscal Administrativo
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Processo: Falta de controle nos trâmites da contratação	
2	Pessoal: Falta de controle na entrega dos produtos ou execução do serviço	

3	Processo: Falta de cronograma de contratação
4	Estrutura Física: Parque tecnológico não preparado para recepcionar as contratações

Risco 03: Equipamentos/softwares não possuem as funcionalidades exigidas		
Probabilidade		(X) Baixa ( ) Média ( ) Alta
Impacto		( ) Muito Grande (X) Grande ( ) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Não provimento adequado do Confea	
2	Contratações ineficazes	
ID	**Ação Preventiva**	**Responsáveis**
1	Realizar os estudos técnicos preliminares com profundidade e técnica devida para obter e atender às necessidades do Confea	Integrante Requisitante Integrante Técnico
2	Realizar reuniões com as áreas interessadas a fim de obter suas necessidades	Integrante Requisitante Integrante Técnico
ID	**Ação de Contingência**	**Responsáveis**
1	Adaptar os equipamentos e os serviços do Confea, com os meios disponibilizados	Fiscal Requisitante Fiscal Técnico
2	Iniciar os Estudos Estratégicos de Tecnologia da Informação	Ocupantes de cargos com poder de decisão
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Pessoal: Inexistência de pesquisa e estudo sobre demandas	
2	Pessoal: Ausência de Estudos Estratégicos de TI	

Risco 04: Inexecução total do contrato		
Probabilidade		(X) Baixa ( ) Média ( ) Alta
Impacto		( ) Muito Grande (X) Grande ( ) Moderado ( ) Pequeno ( ) Muito Pequeno
ID	**Dano**	
1	Impossibilidade de celebração contratual	
ID	**Ação Preventiva**	**Responsáveis**
1	Atentar aos requisitos de habilitação, quando da elaboração da documentação (Projeto Básico/Termo de Referência)	Integrante Requisitante Integrante Técnico Integrante Administrativo
2	Pesquisar o histórico contratual das licitantes contratadas	Integrante Requisitante Integrante Administrativo Setor de Licitações do Confea
ID	**Ação de Contingência**	**Responsáveis**
1	Aplicar penalizações, na forma prevista no instrumento convocatório ou no contrato	Fiscal Requisitante Fiscal Técnico Fiscal Administrativo
2	Convocar, dentro do prazo e condições estabelecidas, os licitantes remanescentes para manifestar o interesse de assinar o termo de contrato	Setor de Licitações do Confea
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Pessoal: Inobservância dos critérios de habilitação na documentação elaborada	

Risco 05: Inexecução parcial do contrato	
Probabilidade	(X) Baixa ( ) Média ( ) Alta
Impacto	( ) Muito Grande (X) Grande ( ) Moderado

	( ) Pequeno ( ) Muito Pequeno

ID	Dano
1	Provimento extemporâneo dos setores demandantes
2	Possibilidade de inexecução e rescisão do contrato, prejudicando a conclusão do serviço
3	Descumprimento das cláusulas contratuais
4	Interrupção dos serviços prestados ao Confea

ID	Ação Preventiva	Responsáveis
1	Atentar aos requisitos contratuais, quanto à inexecução parcial da contratação, quanto da execução contratual e fiscalizar o contrato atentando para a devida qualidade técnica na realização das atividades e para a manutenção das condições de contratação exigidas na habilitação	Fiscal Requisitante Fiscal Técnico Fiscal Administrativo
2	Pesquisar o histórico contratual das licitantes contratadas, quanto à execução dos contratos realizados com a Administração Pública	Integrante Requisitante Integrante Administrativo Setor de Licitações do Confea
3	Acompanhar a execução contratual para evitar subcontratações não autorizadas	Fiscal Requisitante Fiscal Administrativo
4	Prestar especial atenção na análise da documentação da empresa que atesta sua habilitação econômica, financeira e técnica	Pregoeiro

ID	Ação de Contingência	Responsáveis
1	Aplicar penalizações, na forma prevista no instrumento convocatório ou no contrato	Fiscal Requisitante Fiscal Técnico Fiscal Administrativo
2	Comunicação tempestiva e reiterada à empresa para regularização das pendências apontadas	Fiscal Requisitante Fiscal Técnico Fiscal Administrativo Gestor do Contrato
3	Abertura de processo administrativo para averiguação do problema e apuração de responsabilidade	Fiscal Requisitante Fiscal Técnico Fiscal Administrativo Gestor do Contrato
4	Convocar, dentro do prazo e condições estabelecidas, os licitantes remanescentes para manifestar o interesse de assinar o termo de contrato, caso a rescisão contratual venha ocorrer	Setor de Licitações do Confea

Causas (Fonte + Vulnerabilidades)	
ID	**Descrição**
1	Fator Externo: Não cumprimento de cláusulas contratuais, especificações, projetos ou prazos
2	Fator Externo: Subcontratação com terceiros não admitidos no Edital

Risco 06: Equipe técnica da contratada	
Probabilidade	(X) Baixa ( ) Média ( ) Alta
Impacto	( ) Muito Grande (X) Grande ( ) Moderado ( ) Pequeno ( ) Muito Pequeno

ID	Dano
1	Equipe Técnica da empresa não atende de forma eficiente durante a execução do contrato
2	Indisponibilidade de sistemas por erro no desenvolvimento ou falha na aplicação

ID	Ação Preventiva	Responsáveis
1	Reuniões periódicas durante as fases da execução do objeto e alinhamento das obrigações entre as partes	Fiscal Requisitante Fiscal Técnico

ID	Ação de Contingência	Responsáveis
1	Explicitar as prioridades, o detalhamento e o mapeamento das fases	Fiscal Requisitante Fiscal Técnico Fiscal Administrativo Gestor do Contrato
2	Estabelecer ações preventivas por falhas ou erros ou indisponibilidade de sistemas	Fiscal Requisitante Fiscal Técnico Fiscal Administrativo

		Gestor do Contrato
Causas (Fonte + Vulnerabilidades)		
ID	**Descrição**	
1	Planejamento: Dispor no Termo de Referência os perfis de profissionais necessários para execução do objeto	

32. **UNIDADE ORGANIZACIONAL RESPONSÁVEL PELAS INFORMAÇÕES**

32.1. A Gerência de Tecnologia da Informação - GTI é a unidade organizacional responsável pelas informações constantes neste instrumento e adoção de providências necessárias a continuidade do processo de contratação.

33. **DOS ANEXOS**

33.1. São partes integrantes deste Projeto os seguintes anexos:

33.1.1. Anexo I - Termo de Ciência de Manutenção de Sigilo

33.1.2. Anexo II - Termo de Compromisso e Manutenção de Sigilo

33.1.3. Anexo III - Termo de Recebimento Provisório

33.1.4. Anexo IV - Termo de Recebimento Definitivo

34. **ANEXO I - TERMO DE CIÊNCIA DE MANUTENÇÃO DE SIGILO**

TERMO DE CIÊNCIA DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO

Visa obter o comprometimento formal da contratada diretamente envolvida no projeto sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.

IDENTIFICAÇÃO

CONTRATO N°			
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 na Contratante.

CIÊNCIA	
CONTRATADA - Funcionários	
_____ Nome/CPF	_____ Nome/CPF
_____ Nome/CPF	_____ Nome/CPF
_____ Nome/CPF	_____ Nome/CPF

Brasília, _____ de _____ de 20_____.

35. **ANEXO II - TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO**

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 da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

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 pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto dos CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 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_____.

36. **ANEXO III - TERMO DE RECEBIMENTO PROVISÓRIO**

TERMO DE RECEBIMENTO PROVISÓRIO (TRP)

IDENTIFICAÇÃO

36.1. **Pregão Eletrônico nº**: XX/20XX.

36.2. **Contrato nº**: XXX/20XX.

36.2.1. **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.

36.2.2. **Nota de Empenho**: Nota de inscrição em restos a pagar nº XX (SEI nº XXXX), no valor de R$ XX (por extenso).

36.3. **Contratante**: Conselho Federal de Engenharia e Agronomia - Confea

36.4. **Contratada**:

36.4.1. **CNPJ**:

36.4.2. **Endereço**:

36.4.3. **Endereço Eletrônico**:

36.5. **Ordem de Serviço** nº: XX/20XX (SEI nº XXX)

36.5.1. **Objeto**:

36.5.2. **Valor dos Bens/Serviços Recebidos**: R$ XX (por extenso), com pagamentos anuais no valor de R$ XX (por extenso).

36.5.3. **Data da Entrega**: DIA/MÊS/ANO.

36.5.4. **Data do Recebimento**: DIA/MÊS/ANO.

DOCUMENTOS ENTREGUES

36.6. SEI nº XXX: nome do documento.

36.7. SEI nº XXX: nome do documento.

36.8. SEI nº XXX: nome do documento.

TERMOS

36.9. Por este instrumento, atesto, para fins de cumprimento do disposto no art. 33, inciso I, da Instrução Normativa nº 1, de 4 de abril de 2019, emitida pelo Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria de Governo Digital, 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 pela Contratante.

36.10. Ressaltamos que o recebimento definitivo destes serviços e/ou bens ocorrerá em até 5 (cinco) dias úteis, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Contrato acima identificado.

37. **ANEXO IV - TERMO DE RECEBIMENTO DEFINITIVO**

TERMO DE RECEBIMENTO DEFINITIVO (TRD)

IDENTIFICAÇÃO

37.1. **Pregão Eletrônico nº**: XX/20XX.

37.2. **Contrato nº**: XXX/20XX.

37.2.1. **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.

37.2.2. **Nota de Empenho**: Nota de inscrição em restos a pagar nº XX (SEI nº XXXX), no valor de R$ XX (por extenso).

37.3. **Contratante**: Conselho Federal de Engenharia e Agronomia - Confea.

37.4. **Contratada**:

37.4.1. **CNPJ**:

37.4.2. **Endereço**:

37.4.3. **Endereço Eletrônico**:

37.5. **Ordem de Serviço** nº: XX/20XX (SEI nº XXX)

37.5.1. **Objeto**:

37.5.2. **Valor dos Bens/Serviços Recebidos**: R$ XX (por extenso), com pagamentos anuais no valor de R$ XX (por extenso).

37.5.3. **Data da Entrega**: DIA/MÊS/ANO.

37.5.4. **Data do Recebimento**: DIA/MÊS/ANO.

TERMOS

37.6. 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).

37.7. De forma a subsidiar este Termo de Recebimento Definitivo, foram considerados as seguintes análises e documentos:

37.7.1. Termo de Recebimento Provisório (SEI nº XXXX e documentos correlatos).

37.7.2. Análise Técnica do Fiscal do Contrato (SEI nº XXXX documento correlatos).

Em cumprimento ao disposto na **Instrução Normativa que rege a contratação de bens e serviços de tecnologia da informação e comunicação**, o presente documento segue assinado pelos Integrantes da Equipe de Planejamento da Contratação, designada pelo documento de Instituição da Equipe de Planejamento da Contratação, bem como pela autoridade máxima da área de TIC.

Documento assinado eletronicamente por **Rodrigo de Souza Borges**, **Integrante Requisitante**, em 03/02/2022, às 16:57, 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 **Marcelo de Oliveira Coelho Santos**, **Integrante Técnico**, em 03/02/2022, às 17:02, 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 **Luciana Matias Mota**, **Assistente**, em 03/02/2022, às 18:04, 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 **Renato Gonçalves Barros**, **Superintendente de Estratégia e Gestão**, em 03/02/2022, às 19:13, 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 **0557428** e o código CRC **65C7FB05**.

Referência: Processo nº CF-01407/2021 SEI nº 0557428