CONSELHO FEDERAL DE ODONTOLOGIA

EDITAL DE LICITAÇÃO Nº 04/2025

PROCESSO Nº 1092/2024

1. **OBJETO** O objeto da presente licitação é a escolha da proposta mais vantajosa para o Conselho Federal de Odontologia a eventual contratação de empresa especializada em prover Solução Proativa em Nuvem de Detecção, Correlação e Mitigação de Ataques, com Serviço de Treinamento e Serviço de Instalação, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

GRUPO	ITEM	DESCRIÇÃO	QTD
1	1	Solução de Proteção de Endpoints com detecção e respostas estendidos.	175
	2	Solução de Proteção de Servidores Físicos, Virtuais e em Nuvem com detecção e respostas estendidos.	80
	3	Solução de Proteção de Ameaças Persistentes Avançadas com detecção e respostas estendidos.	1
	4	Solução Proativa de Validação de Integridade de Ativos	1
	5	Serviço de Instalação	1
	6	Serviço de Suporte	36
	7	Serviço de Treinamento	1

ANEXOS:

I. Termo de Referência

II. Modelo de Proposta

III. Planilha de Preços Estimados

EDITAL DE LICITAÇÃO Nº 04/2025

CONSELHO FEDERAL DE ODONTOLOGIA

UASG – 926655

PROCESSO Nº 1092/2024

Tipo de Licitação: **MENOR PREÇO**

Data e horário de abertura da sessão do Pregão Eletrônico: **17/01/2025, às 09:00h.**

Data e horário de início de recebimento das propostas: **03/01/2025, às 08:00h.**

Data e horário de término para recebimento das propostas: **17/01/2025às 09:00h.**

Endereço: **www.comprasgovernamentais.gov.br**

O CONSELHO FEDERAL DE ODONTOLOGIA, por intermédio do Pregoeiro e sua Equipe de Apoio, designados pela Portaria CFO-SEC nº 06, de 31 de janeiro de 2024, torna público para o conhecimento dos interessados que na data, horário e local acima indicados, fará realizar licitação na modalidade **PREGÃO na forma ELETRÔNICA**, do tipo **MENOR PREÇO**, mediante as condições estabelecidas neste Edital e seus anexos.

O procedimento licitatório obedecerá, integralmente, à Lei nº 14.133, de 1º de abril de 2021, ao Decreto nº 11.462/2023, de 31 de março de 2023, Decreto nº 10.024, de 20 de setembro de 2019, à Lei Complementar nº 123, de 14 de dezembro de 2006, à Lei 8.078, de 11 de setembro de 1990 – Código de Defesa do Consumidor , legislação correlata e demais exigências previstas neste Edital e seus anexos.

1. DO OBJETO

1. A presente licitação tem como objeto da presente licitação é a escolha da proposta mais vantajosa para o Conselho Federal de Odontologia a eventual contratação de empresa especializada em prover Solução Proativa em Nuvem de Detecção, Correlação e Mitigação de Ataques, com Serviço de Treinamento e Serviço de Instalação, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.1. Em caso de discordância existente entre as especificações do objeto descritas no CATMAT/CATSER e as constantes no Termo de Referência prevalecerão as últimas.

2. DA PARTICIPAÇÃO

2.1. Poderão participar deste pregão os interessados do ramo de atividade relacionada ao objeto que atenderem a todas as exigências, inclusive quanto à documentação, constantes deste Edital e de seus anexos, desde que:

2.1.1. Desempenhem atividades pertinentes e compatíveis com o objeto deste Pregão;

2.1.2. Atendam aos requisitos mínimos de classificação das propostas exigidos neste Edital;

2.1.3. Possuam registro cadastral atualizado no Sistema de Cadastramento Unificado de Fornecedores (SICAF).

2.2. Respeitadas as demais condições normativas e as constantes do Edital, poderá participar desta contratação consórcio de empresas, atendidas as condições previstas no Art. 15 da Lei nº 14.133/2021, e aquelas estabelecidas no Edital.

2.3. Fica vedada a participação de empresa consorciada em mais de um consórcio ou isoladamente de profissional em mais de uma empresa, ou em mais de um consórcio.

2.4. A empresa ou consórcio deverá assumir inteira responsabilidade pela inexistência de fatos que possam impedir a sua habilitação na presente licitação e, ainda, pela autenticidade de todos os documentos que forem apresentados.

2.5. As consorciadas deverão apresentar além dos demais documentos exigidos neste Edital, compromisso de constituição de consórcio, por escritura pública ou documento particular registrado em Cartório de Registro de Títulos e Documentos, discriminando a empresa líder, bem como a participação de cada consorciado.

2.6. O prazo de duração de consórcio deve, no mínimo, coincidir com o prazo de conclusão de objeto desta contratação, até sua aceitação definitiva.

2.7. Os consorciados deverão apresentar compromisso de que não alterarão a constituição ou composição do consórcio, visando manter válidas as premissas que asseguram a sua habilitação.

2.8. Os consorciados deverão apresentar compromisso de que não constituem nem se constituirão, para fins do consórcio, em pessoa jurídica e de que o consórcio não adotará denominação própria, diferente de seus integrantes. Os consorciados deverão apresentar compromisso que serão solidários entre si.

2.9. Conforme o § 1º do Art. 15 da Lei nº 14.133/2021 fica estabelecido o acréscimo percentual de 10% (dez por cento) sobre o valor exigido de licitante individual para a habilitação econômico-financeira, salvo justificação.

2.10. Não poderão participar desta licitação pessoas físicas ou jurídicas que se enquadrem nas hipóteses do Art. 14 da Lei nº 14.133/2021;

2.11. O Pregoeiro, auxiliado pela equipe de apoio, consultará os sistemas de registros de sanções SICAF, LISTA DE INIDÔNEOS DO TCU, CNJ E CEIS, visando aferir eventual sanção aplicada à licitante, cujo efeito torne-a proibida de participar deste certame.

3. DO ENQUADRAMENTO COMO MICROEMPRESAS, EMPRESAS DE PEQUENO PORTE E EQUIPARADOS

3.1. O enquadramento como microempresa – ME ou empresa de pequeno porte – EPP dar-se-á desde que atendidos os requisitos delineados na Lei Complementar nº 123/2006 e suas alterações.

3.1.1. A sociedade cooperativa que tenha auferido, no ano-calendário anterior ao presente, receita bruta superior a R$360.000,00 (trezentos e sessenta mil reais) e igual ou inferior a R$4.800.000,00 (quatro milhões e oitocentos mil reais), em conformidade com as disposições do art. 34 da Lei nº 11.488/2007, receberá o mesmo tratamento concedido pela Lei Complementar nº 123/2006 às ME/EPP.

3.1.2. A pessoa física ou o empresário individual que se enquadrar no inciso I ou II do art. 3º da Lei Complementar nº 123/2006, receberá o mesmo tratamento que a referida Lei concede às ME/EPP.

4. DA REPRESENTAÇÃO E DO CREDENCIAMENTO

4.1. O credenciamento dar-se-á pela atribuição de chave de identificação e de senha pessoal e intransferível, para acesso ao sistema eletrônico, no Portal de Compras do Governo Federal – Compras Governamentais, no sítio http://www.comprasgovernamentais.gov.br.

4.2. O credenciamento da licitante, bem como a sua manutenção, dependerá de registro cadastral, atualizado no Sistema de Cadastramento Unificado de Fornecedores – SICAF. Alternativamente o credenciamento poderá ser feito no Sistema de Credenciamento de Fornecedores do sítio Compras Governamentais, o que permite ao fornecedor obter Login e Senha e participar de Pregões e Cotações Eletrônicas sem que haja a necessidade de se cadastrar no SICAF.

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

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

4.5. A perda da senha ou a quebra de sigilo deverá ser comunicada imediatamente ao provedor do sistema para imediato bloqueio de acesso.

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Os licitantes encaminharão, quando solicitado pelo pregoeiro, exclusivamente por meio do sistema (as extensões aceitas para o arquivo são: SXW, DOC, RTF, TXT, ZIP, PDF e ODT), a proposta de preços atualizada ao último lance e após a aprovação da proposta os documentos de habilitação, quando solicitado pelo dirigente do certame.

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

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

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

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

5.6. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema.

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

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

6. DO PREENCHIMENTO DA PROPOSTA

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

6.1.1. Valor unitário e total do item;

6.1.2. Valor total do grupo.

6.1.3. Descrição detalhada do objeto, contendo as informações similares à especificação do Termo de Referência, indicando, no que for aplicável, o modelo, prazo de validade ou de garantia, número do registro ou inscrição do bem no órgão competente, quando for o caso.

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

6.3. A licitação será em Grupo Único, contendo 7 itens, dos quais:

GRUPO	ITEM	DESCRIÇÃO	QTD
1	1	Solução de Proteção de Endpoints com detecção e respostas estendidos.	**175**
	2	Solução de Proteção de Servidores Físicos, Virtuais e em Nuvem com detecção e respostas estendidos.	**80**
	3	Solução de Proteção de Ameaças Persistentes Avançadas com detecção e respostas estendidos.	**1**
	4	Solução Proativa de Validação de Integridade de Ativos	**1**
	5	Serviço de Instalação	**1**
	6	Serviço de Suporte	**36**
	7	Serviço de Treinamento	**1**

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

6.5. Quaisquer tributos, custos e despesas diretos ou indiretos omitidos da proposta ou incorretamente cotados serão considerados como inclusos nos preços, não sendo aceitos pleitos de acréscimos, a esse ou a qualquer título, devendo o objeto ser executado sem ônus adicional para o CFO.

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

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

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

6.9. Em caso de divergência entre as especificações constantes deste Edital e as registradas no sitio comprasgovernamentais.gov.br, prevalecerão as do Edital.

6.10. As licitantes deverão apresentar descrição detalhada dos equipamentos ofertados, e anexar a respectiva documentação técnica através de catálogos, folder, declaração do fabricante e/ou manuais, para comprovação das especificações técnicas mínimas, fazendo constar da proposta técnica a identificação e página do documento onde se encontra descrita cada uma das características ofertadas.

6.10.1. Caso as documentações não comprovem todos os requisitos técnicos dos equipamentos, a empresa licitante poderá apresentar documentação complementar do fabricante emitida com a finalidade específica para a licitação a que se refere o presente Termo de Referência.

6.11. Serão desclassificadas as propostas que não atenderem às exigências do presente Edital e seus anexos, sejam omissas ou apresentem irregularidades, ou defeitos capazes de dificultar o julgamento.

6.12. A apresentação da proposta implicará plena aceitação, por parte da licitante, das condições estabelecidas neste Edital e seus anexos.

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

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

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

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

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

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

7.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e as licitantes, após a fase de lances.

7.5. Aberta a etapa competitiva, as licitantes poderão registrar lances exclusivamente por meio do sistema eletrônico, sendo a licitante imediatamente informada do seu recebimento e respectivo horário de registro e valor.

7.5.1. O lance deverá ser ofertado pelo valor total do lote**.**

7.6. As licitantes poderão oferecer lances sucessivos, observado o horário fixado para a abertura da sessão e as regras de sua aceitação.

7.7. As licitantes somente poderão oferecer lances de valor inferior ao último por ela ofertados e registrados pelo sistema.

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

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

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

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

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

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

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

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

7.14. Durante a sessão pública, as licitantes serão informadas, em tempo real, dos valores dos menores lances registrados, vedada a identificação das empresas participantes do certame.

7.15. O critério de julgamento adotado será o menor preço global, conforme definido neste Edital e em seus anexos.

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

7.17. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de2015.

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

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

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

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

7.22. A microempresa ou empresa de pequeno porte, que venha a ser contratada para a prestação de serviços mediante cessão de mão-de-obra não poderá beneficiar-se da condição de optante pelo Simples Nacional, salvo as exceções previstas no § 5º-C do art. 18 da Lei Complementar nº 123/2006.

7.22.1. Para efeito de comprovação do disposto no subitem acima, a contratada deverá apresentar cópia do ofício, enviado à Receita Federal do Brasil, com comprovante de entrega e recebimento, comunicando a assinatura do contrato de prestação de serviços mediante cessão de mão-de-obra, até o último dia útil do mês subsequente ao da ocorrência da situação de vedação.

7.23. Quando houver propostas beneficiadas com as margens de preferência em relação ao produto estrangeiro, o critério de desempate será aplicado exclusivamente entre as propostas que fizerem jus às margens de preferência, conforme regulamento.

7.24. A ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação, de maneira que só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

7.25. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021. Se não houver desempate será assegurada a preferência conforme o § 1º do art. 60 da Lei nº 14.133, de 2021 e seus incisos.

7.26. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

7.27. Após o encerramento da etapa 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, observado o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas neste Edital.

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

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

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

8. DA DESCONEXÃO

8.1. No caso de desconexão do Pregoeiro, no decorrer da etapa de lances, o sistema eletrônico poderá permanecer acessível às licitantes para a recepção dos lances, retornando o Pregoeiro, quando possível, para sua atuação no certame, sem prejuízo dos atos realizados.

8.2. Quando a desconexão do Pregoeiro persistir por tempo superior a dez minutos, a sessão do Pregão na forma eletrônica será suspensa e reiniciada somente após a comunicação às participantes, no endereço eletrônico utilizado para divulgação.

9. DA ACEITABILIDADE DA PROPOSTA VENCEDORA

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

9.2. Será desclassificada a proposta ou o lance vencedor, que apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018 – TCU – Plenário), ou que apresentar preço manifestamente inexequível.

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

9.2.2. A inexequibilidade dos valores referentes a itens isolados da planilha de custos, desde que não comprometam o valor global ou contrariem instrumentos legais, não caracteriza motivo suficiente para a desclassificação da proposta.

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

9.4. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata.

9.5. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de **2 (duas) horas**, sob pena de não aceitação da proposta.

9.5.1. O prazo estabelecido poderá ser prorrogado pelo Pregoeiro por solicitação escrita e justificada do licitante, formulada antes de findo o prazo, e formalmente aceita pelo Pregoeiro.

9.5.2. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

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

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

9.8. O Pregoeiro deverá encaminhar, por meio do sistema eletrônico, contraproposta ao licitante que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.

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

9.8.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelo demais licitantes.

9.9. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, de eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

9.10. Encerrada a análise quanto à aceitação da proposta, o Pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

10. DA HABILITAÇÃO

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

10.1.1. SICAF;

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

10.1.3. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei nº 8.249, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

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

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

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

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

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

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

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

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

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

10.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de **2 (duas) horas**, sob pena de inabilitação.

10.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais, em suporte documental físico, quando houver dúvida em relação à integridade do documento digital.

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

10.6. Conforme art. 15 da Lei 14.133/2021, salvo vedação devidamente justificada no processo licitatório, pessoa jurídica poderá participar de licitação em consórcio, observadas as seguintes normas:

10.6.1. A comprovação de compromisso público ou particular de constituição de consórcio, subscrito pelos consorciados;

10.6.2. A indicação da empresa líder do consórcio, que será responsável por sua representação perante a Administração;

10.6.3. . A admissão, para efeito de habilitação técnica, do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, do somatório dos valores de cada consorciado;

10.6.4. A impedimento de a empresa consorciada participar, na mesma licitação, de mais de um consórcio ou de forma isolada;

10.6.5. . responsabilidade solidária dos integrantes pelos atos praticados em consórcio, tanto na fase de licitação quanto na de execução do contrato.

10.6.6. A obrigatoriedade de liderança por empresa brasileira no consórcio formado por empresas brasileiras e estrangeiras.

10.6.7. A constituição e o registro do consórcio antes da celebração do contrato.

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

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

10.8. Ressalvado o disposto no item 5.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação:

10.9. Habilitação Jurídica

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

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

10.9.3. No caso de sociedade empresária ou sociedade limitada unipessoal – SLU: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores.

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

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

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

10.9.7. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização.

10.9.8. Os documentos acima deverão estar acompanhados de todas as alterações ou consolidação respectiva.

10.10. Regularidades Fiscal e Trabalhista

10.10.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ ou no Cadastro de Pessoas Físicas, conforme o caso.

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

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

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

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

10.10.6. Prova de regularidade com a Fazenda Estatual do domicílio ou sede do licitante, relativa à atividade em cujo exercício contratada ou concorre.

10.10.7. Caso o fornecedor seja considerado isento dos tributos estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei.

10.10.8. Caso o licitante detentor do menor preço seja qualificado como microempresa ou empresa de pequeno porte, deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

10.11. Qualificação Econômico-Financeira

10.11.1. Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede da pessoa jurídica.

10.11-1.1. A certidão referida no subitem acima que não estiver mencionando explicitamente o prazo de validade, somente será aceita com o prazo máximo de 90 (noventa) dias, contados da data de sua emissão.

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

10.11.3. No caso de fornecimento de bens para pronta entrega, não será exigido da licitante qualificada como microempresa ou empresa de pequeno porte, a apresentação de balanço patrimonial do último exercício financeiro (Art. 3º do Decreto nº 8.538, de 2015).

10.11-3.1. No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade.

10.11-3.2. É admissível o balanço intermediário, se decorrer de lei ou contrato social/estatuto social.

10.11-3.3. Caso o licitante seja cooperativa, tais documentos deverão ser acompanhados da última auditoria contábil-financeira, conforme dispõe o artigo 112 da Lei nº 5.764, de 1971, ou de uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

10.11-3.4. A boa situação financeira da licitante será avaliada pelos Índices de Liquidez Geral (ILG), Índice de Solvência (IS) e Índice de Endividamento (IE), resultantes da aplicação das fórmulas abaixo, com os valores extraídos de seu balanço patrimonial ou apurados mediante consulta "*on line*" no caso de empresas inscritas no SICAF:

ILG = $\frac{Ativo\ Circulante + Ativo\ Realizável\ a\ Longo\ Prazo}{Passivo\ Circulante + Passivo\ Exígivel\ a\ Longo\ Prazo}$ Igual ou Superior a 1,00

IS = $\frac{Ativo\ Circulante + Ativo\ Realizável\ a\ Longo\ Prazo + Ativo\ Permanente}{Passivo\ Circulante + Passivo\ Exígivel\ a\ Longo\ Prazo}$ Igual ou Superior a 1,00

IE = $\frac{Passivo\ Circulante + Passível\ Exigível\ a\ Longo\ Prazo}{Ativo\ Total}$ Igual ou Inferior a 0,5

10.12. Qualificação Técnica

10.12.1. Para a comprovação da qualificação técnico-operacional, a licitante detentora do menor preço deverá apresentar atestado(s) de capacidade técnica expedido(s) por empresa pública ou privada, comprovando que prestou serviços pertinentes e compatíveis em características, quantidades e prazos em relação ao objeto da licitação.

10.12.2. Declaração indicando suas instalações e recursos disponíveis para a prestação dos serviços, no tocante à estrutura da empresa e disponibilidade de pessoal administrativo, informando o endereço completo onde se situam estas instalações.

10.13. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

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

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

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

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

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

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

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

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

11. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

11.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de **2 (duas) horas**, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

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

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

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

Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 12, II da Lei nº 14.133/21).

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

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

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

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

12. DA MANUTENÇÃO DAS CONDIÇÕES DE HABILITAÇÃO

12.1. Na assinatura do Contrato será exigida a comprovação das condições de habilitação consignadas neste Edital, as quais deverão ser mantidas pela licitante durante a vigência do Contrato, salvo quanto à manutenção do porte da empresa (Lei Complementar nº 123/2006).

12.1.1. Quando a vencedora da licitação não fizer a comprovação referida no subitem anterior ou quando, injustificadamente, recusar-se a assinar o Contrato, sem prejuízo das multas previstas neste Edital e no Contrato e das demais cominações legais, poderá ser convocada outra licitante, desde que respeitada a ordem de classificação, para, após comprovados os requisitos de habilitação e feita a negociação, assinar o Contrato.

13. DA IMPUGNAÇÃO DO INSTRUMENTO CONVOCATÓRIO

13.1. Até três dias úteis antes da data fixada para abertura da sessão pública, qualquer pessoa poderá impugnar o ato convocatório do Pregão, na forma eletrônica.

13.1.1. Caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos e pela área requisitante, se for o caso, decidir sobre a impugnação no prazo de até dois dias úteis contados da data de recebimento da impugnação.

13.1.2. Acolhida a impugnação contra o ato convocatório, será designada nova data para a realização do certame.

13.2. A impugnação poderá ser realizada na forma eletrônica pelo *e-mail* licitacoes@cfo.org.br, ou, ainda, por petição dirigida ou protocolada no endereço: SHIN CA 7 Lote 2 – CEP: 71.503-507 – Brasília – DF, de segunda a sexta-feira (exceto feriados), no horário de 09:00 às 12:00h e de 13:00 às 17:00h. Quando enviada por *e-mail*, o emitente deve aferir a confirmação de recebimento pelo pregoeiro.

14. DOS PEDIDOS DE ESCLARECIMENTOS

14.1. Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao Pregoeiro, até **3 (três) dias úteis** anteriores à data fixada para abertura da sessão pública, exclusivamente por meio eletrônico via *internet*, no endereço: licitacoes@cfo.org.br, devendo aferir a confirmação de recebimento pelo Pregoeiro.

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

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

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

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

15. DOS RECURSOS

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

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

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

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

15.3.2. o prazo para a manifestação da intenção de recorrer não será inferior a 30 (trinta) minutos.

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

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

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

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

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

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

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

15.9. O acolhimento de recurso importará invalidação apenas dos atos insuscetíveis de aproveitamento.

15.10. Os autos do processo permanecerão com vista franqueada aos interessados no CFO, situado no SHIN CA 7 – Lote 2 – Brasília – DF, de segunda a sexta-feira (exceto feriados), no horário das 09:00 às 12:00 e das 13:00 às 16:45 horas.

16. DA REABERTURA DA SESSÃO PÚBLICA

16.1. A sessão pública poderá ser reaberta:

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

16.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o Contrato, não retirar o instrumento equivalente ou não comprovar a

regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

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

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

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

17. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

17.1. O objeto da licitação será adjudicado à licitante declarada vencedora, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

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

18. DAS OBRIGAÇÕES DAS PARTES

18.1. As obrigações da CONTRATADA e da CONTRATANTE são aquelas estabelecidas no Termo de Referência – Anexo I (item 11).

19. DO PAGAMENTO

19.1. As condições de pagamento são aquelas estabelecidas no Termo de Referência – Anexo I (Item 18).

20. DOS RECURSOS ORÇAMENTÁRIOS

17. As despesas decorrentes deste objeto correrão à conta da Rubrica nº 6.2.2.1.1.01.04.04.004.013-Despesas com Soluções de informática.

DAS SANÇÕES ADMINISTRATIVAS

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

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

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

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

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

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

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

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

20.1.4. recusar-se, sem justificativa, a assinar o Contrato no prazo estabelecido pela Administração;

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

20.1.6. fraudar a licitação

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

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

20.1.7.2. induzir deliberadamente a erro no julgamento;

20.1.7.3. apresentar amostra falsificada ou deteriorada;

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

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

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

20.2.1.1. advertência;

20.2.1.2. multa;

20.2.1.3. impedimento de licitar e contratar e

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

20.3. Na aplicação das sanções serão considerados:

20.3.1. a natureza e a gravidade da infração cometida.

20.3.2. as peculiaridades do caso concreto.

20.3.3. as circunstâncias agravantes ou atenuantes os danos que dela provierem para a Administração Pública.

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

20.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 25 (vinte e cinco) dias úteis, a contar da comunicação oficial.

20.4.1. Para as infrações previstas nos itens 23.1.1, 23.1.2 e 23.1.3, a multa será de 5% a 10% do valor do contrato licitado.

20.4.2. Para as infrações previstas nos itens 23.1.4, 23.1.5, 23.1.6, 23.1.7 e 23.1.8, a multa será de 0,5% a 10% do valor do contrato licitado.

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

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

20.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 23.1.1, 23.1.2 e 23.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

20.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 23.1.4, 23.1.5, 23.1.6, 23.1.7 e 23.1.8, bem como pelas infrações administrativas previstas nos itens 23.1.1, 23.1.2 e 23.1.3 que justifiquem a imposição de

penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

20.9. A recusa injustificada do adjudicatário em assinar o contrato no prazo estabelecido pela Administração, descrita no item 23.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

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

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

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

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

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

21. DAS ALTERAÇÕES

21.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos artigos 124 ao 136 da Lei nº 14.133/21.

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

22. DAS DISPOSIÇÕES GERAIS

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

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

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

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

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

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

22.7. As licitantes assumem todos os custos de preparação e apresentação de suas propostas e o CFO não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

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

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

22.10. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem os processos, prevalecerá as deste Edital.

22.11. As respostas aos pedidos de esclarecimentos, bem como as demais informações relevantes, serão divulgadas mediante publicações no portal COMPRAS GOVERNAMENTAIS (www.comprasgovernamentais.gov.br) e no Portal da Transparência do CFO (http://transparenciacfo.org.br/), ficando as empresas interessadas em participar do certame obrigadas a acessá-las para a obtenção das informações prestadas.

O valor total estimado da licitação é de R$ R$ 600.276,20 (seiscentos mil, duzentos e setenta e seis reais e vinte centavos).

22.12. Este Edital e seus anexos estarão disponibilizados, na íntegra, nos endereços: www.comprasgovernamentais.gov.br e http://transparenciacfo.org.br, ou poderão ser retirados no Conselho Federal de Odontologia – SHIN CA 7 – Lote 2 – Brasília – DF, de segunda a sexta-feira (exceto feriados), no horário das 08:00 às 12:00 e das 13:00 às 16:45 horas. Telefone para contato: (61) 3033-4499.

Brasília – 03 de janeiro de 2024

CONSELHO FEDERAL DE ODONTOLOGIA

ANEXO I DO EDITAL

TERMO DE REFERÊNCIA

1. DO OBJETO

1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para o Conselho Federal de Odontologia a eventual contratação de empresa especializada em prover Solução Proativa em Nuvem de Detecção, Correlação e Mitigação de Ataques, com Serviço de Treinamento e Serviço de Instalação, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

GRUPO	ITEM	DESCRIÇÃO	QTD
1	1	Solução de Proteção de Endpoints com detecção e respostas estendidos.	**175**
	2	Solução de Proteção de Servidores Físicos, Virtuais e em Nuvem com detecção e respostas estendidos.	**80**

	3	Solução de Proteção de Ameaças Persistentes Avançadas com detecção e respostas estendidos.	**1**
	4	Solução Proativa de Validação de Integridade de Ativos	**1**
	5	Serviço de Instalação	**1**
	6	Serviço de Suporte	**36**
	7	Serviço de Treinamento	**1**

2. FUNDAMENTAÇÃO LEGAL E JUSTIFICATIVA

1.1. Dentre as justificativas para a execução do projeto, destacam-se:

1.2. A superfície de ataque cibernético, ou seja, a soma de todas as possíveis entradas para um sistema, nunca foi tão ampla. Com a crescente digitalização e a migração para a nuvem, as organizações estão cada vez mais expostas a ameaças. A proliferação de dispositivos IoT, a complexidade das redes e a constante evolução das táticas de hackers tornam a tarefa de proteger os ambientes digitais um desafio constante.

1.3. Atualmente o CFO possui soluções básicas de proteção cibernética e, consequentemente, aumentando o nível de exposição e riscos do ambiente tecnológico do CFO;

1.4. Nesse contexto, a visibilidade da superfície de ataque se torna crucial, especialmente para organizações governamentais. É preciso identificar todos os ativos conectados, as vulnerabilidades existentes e os possíveis vetores de ataque. A falta de conhecimento sobre a própria superfície de ataque é um dos principais fatores que contribuem para incidentes de segurança.

1.5. A utilização de soluções opensource potencializam a exploração de

vulnerabilidades no ambiente cibernético do CFO, possibilitando que atacantes tenham acesso ao parque computacional e aos dados.

1.6. Investir em soluções de detecção, correlação e mitigação, minimizam o risco da superfície de ataque, além de classificar e monitorar os ativos, identificar e corrigir vulnerabilidades de forma proativa. A adoção de soluções robustas e integradas de soluções de cibersegurança, possibilitam a continuidade e expansão do negócio.

1.7. A gestão mais eficiente e mais segura dos ativos do CFO, aumentando a segurança, diminuindo o tempo necessário para resposta e mitigação de ataques cibernéticos.

1.8. Atualmente, o mercado dispõe de ferramentas que contém inteligência artificial realizando um aprendizado de máquina e análise comportamental para detectar ameaças em tempo real em toda a infraestrutura de segurança. Ele coleta dados de várias fontes, incluindo endpoints, firewalls, nuvem e redes, e usa análise contextual para fornecer insights precisos sobre as ameaças.

1.9. O Gartner afirma que as soluções de segurança avançada integrada de prevenção, detecção e resposta são uma resposta à crescente complexidade das ameaças cibernéticas e às limitações das soluções de segurança tradicionais, que muitas vezes são incapazes de correlacionar eventos de segurança em toda a infraestrutura de TI da organização. Essas soluções são projetadas para preencher essa lacuna, fornecendo uma visão holística das atividades de segurança em toda a infraestrutura de TI da organização e permitindo que as equipes de segurança respondam rapidamente a ameaças.

1.10. O Gartner prevê que, até 2027, 50% das organizações usarão uma solução desse tipo para melhorar a detecção e resposta a ameaças. O Gartner também destaca a importância da integração das soluções de segurança avançada integrada de prevenção, detecção e resposta com outras ferramentas de segurança, como soluções de gerenciamento de informações e eventos de segurança (SIEM), soluções de prevenção de intrusões (IPS) e soluções de gerenciamento de vulnerabilidades (VMS), para fornecer uma visão mais abrangente das atividades

de segurança.

1.11. Neste sentido, promover a integração das soluções existentes no parque cibernético do CFO, possibilitando a visibilidade e mensuração do risco, a fim de permitir ações proativas de correção de vulnerabilidades.

1.12. Uma vez que o CFO não possui soluções dedicadas para gerar visibilidade centralizada de eventos de segurança, a pretensa contratação vai diretamente a encontro destas necessidades, contribuindo de forma considerável para o aumento do nível de maturidade em segurança da informação do ambiente tecnológico da Instituição em diversas camadas além do cumprimento aos requisitos legais.

3. CLASSIFICAÇÃO DOS BENS COMUNS

Considerando que os padrões, os níveis de qualidade, a qualificação técnica, as quantificações e as especificações dos itens a serem entregues estão adequadamente definidos por meio de especificações usuais no mercado e, de modo objetivo, no presente Termo de Referência, entende-se que a contratação que ora se pretende está enquadrada como bem comum, tendo a obrigatoriedade na modalidade Pregão, em conformidade com a Lei nº 10.520/02 e suas alterações.Em razão do acima exposto, a modalidade licitatória escolhida é Pregão Eletrônico, do tipo Menor Preço por Lote.

4. DESCRIÇÃO DOS OBJETOS E SERVIÇOS

Itens 1 e 2 - Solução de Proteção de Endpoints e Solução de Proteção de Servidores Físicos, Virtuais e em Nuvem com detecção e respostas estendidos.	
1	**Funcionalidades gerais**
1.1	Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução.
1.2	Deve permitir atualização incremental da lista de definições de vírus.
1.3	Deve permitir a atualização automática do *engine* do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável.
1.4	Deve permitir o *rollback* das atualizações das listas de definições de vírus e *engines*.
1.5	Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas.
1.6	Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotjix e configurações específicas de domínios da árvore de gerenciamento.
1.7	Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pelo console de administração da solução completa.
1.8	Deve possibilitar instalação "silenciosa".
2	**Proteção anti-malware para estações de trabalho Microsoft Windows**

2.1	A solução deve atender a estações de trabalho com solução de VDI com sistema operacional Windows.
2.2	Deve ser capaz de realizar a proteção a códigos maliciosos nos sistemas operacionais: Microsoft Windows 8 e versões superiores.
2.3	Suportar as seguintes plataformas virtuais: VMware Horizon 8 e versões superiores; VMware Vsphere ESXi 7 e versões superiores.
2.4	Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em: Processos em execução em memória principal (RAM); Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell); Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab; Arquivos recebidos por meio de programas de comunicação instantânea tais como Whatsapp, Telegram, Facebook Messenger, Microsoft Teams, Zoom, Google Meet; Arquivos recebidos a partir de sites Web; Arquivos acessados ou recebidos por e-mail.
2.5	Deve permitir diferentes configurações de detecção (varredura ou rastreamento): Em tempo real de arquivos acessados pelo usuário; Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo; Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza; Por linha de comando parametrizável.

2.6	Deve possuir funcionalidade de “Machine Learning” utilizando como fonte de aprendizado a rede de inteligência do fabricante, identificando os aspectos maliciosos, características de boa pontuação e correlacionando, no mínimo, com as seguintes técnicas de proteção a vetores de ataque: Reputação de URL para exploração de navegadores, websites infectados e Office Exploits; Reputação de arquivos para downloads de arquivos e anexos de e-mail.
2.7	Execução do instalador de software com classificação comportamental do instalador.
2.8	Execução do malware de software com classificação comportamental do instalador.
3	**Proteção *anti-malware* para estações de trabalho Linux**
3.1	A solução deve atender a estações de trabalho Linux.
3.2	Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais, no mínimo: Ubuntu Linux 20.04 e versões superiores; Suse Linux Enterprise.
3.3	Deve possuir integração com a solução de Detecção e Resposta Avançada de Ataques (XDR).
3.4	A console de gerenciamento deve permitir o gerenciamento das políticas de segurança através da Internet.
4	**Solução de segurança para proteção para Data Center**
4.1	A solução de deve atender a um ambiente de 60 (sessenta) sockets ou 30 (trinta) hosts, os quais são equivalentes.
4.2	Deve ser compativel com pelo menos os seguintes sistemas operacionais nas versões indicadas e versões superiores: Suse Linux Enterprise 12; CentOS 7; Windows Server 2008;

	Ubuntu 18; Red Hat Enterprise Linux Server 7.3.
4.3	Suportar as seguintes plataformas virtuais: VMware Vsphere ESXi 7 e versões superiores.
4.4	O console de gerenciamento deve ser on-premises, permitindo o gerenciamento das políticas de segurança através da Internet.
4.5	Deve possuir integração com a solução de Detecção e Resposta Avançada de Ataques (XDR).
4.6	Deve ser gerenciada por console Web, compativel com pelo menos os browsers Microsoft Edge, Firefox e Google Chrome.
4.7	Deve suportar certificado digital para gerenciamento.
4.8	O console de administração deve permitir o envio de notificações via SMTP.
4.9	Todos os eventos e ações realizadas no console de gerenciamento precisam ser gravados, visando a auditoria.
4.10	Deve permitir a criação de widgets para facilitar a administração e visualização dos eventos.

4.11	A funcionalidade de anti-malware deve possuir as seguintes características: Deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e agendamento, com possibilidade de tomada de ações distintas para cada tipo de ameaça; Deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura em determinados diretórios ou arquivos do sistema operacional; Deve possuir listas de exclusão separadas por módulo da proteção anti-malware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;
4.12	Em plataforma Windows, deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações; Deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo; O scan de arquivos comprimidos deve ser de no mínimo 6 camadas de compressão; O scan de arquivos comprimidos do tipo OLE deve ser de no mínimo 20 camadas de compressão. A funcionalidade de Proteção Contra URLs Maliciosas deve possuir as seguintes características: Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação; A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;
4.13	O módulo de Firewall deve possuir as seguintes características: Operar como firewall de host, através da instalação de agente nos servidores protegidos; Deve possuir a capacidade de controlar o tráfego baseado nos tipos de protocolos, endereços IP e intervalo de portas.
4.14	

5	**Detecção e Resposta Avançada de Ataques (XDR)**
5.1	Deve suportar a coleta de dados de diversas fontes, incluindo endpoints, rede, filtros da web e sensores de nuvem, para acelerar a detecção e resposta a incidentes e reduzir os tempos de resposta.
5.2	Deve permitir a integração com plataformas de segurança via API.
5.3	Deve ser capaz de ingerir diversas fontes de dados, entre elas Network Intrusion Detection Systems (NIDS), Endpoint Protection Platjorms (EPP), Endpoint Detection and Response (EDR), com objetivo de aprimorar o processo de detecção de ameaças e tomar ágil processo de correlação e investigação de alertas.
5.4	Deve permitir a integração com a ferramenta de gerenciamento de tickets OTRS (*Open-source Ticket Request System*) possibilitando a gestão unificada de incidentes.
5.5	A quantidade de coletores necessários para a total ingestão de eventos do ambiente não deve onerar ou gerar custos adicionais de licenciamento;
5.6	Deve fornecer ambiente gráfico para criação de fluxos de interação.
5.7	Deve permitir a automação das atividades de resposta a incidentes com base nas necessidades e processos mapeados.
5.8	Deve fornecer visibilidade de possíveis vazamentos de contas de usuário.
5.9	Deve fornecer informações de elevação de privilégio das contas nos dispositivos.
5.10	Deve ser compativel com a solução NSX da VMware para permitir integração com os ambientes virtualizados do CJF.
5.11	Deve realizar a coleta e análise dos dados de atividade de endpoints de desktop e servidor.
5.12	Deve realizar a coleta e análise dos dados de atividade de contas de e-mail.

5.13	Deve fornecer insights sobre a postura de segurança baseado em um índice geral de risco, exposição de dispositivos, ataques em andamento e outros fatores relacionados.
5.14	Deve realizar a descoberta dos ativos organizacionais expostos a ataques, incluindo dispositivos e ativos voltados para a Internet, contas, aplicativos em nuvem e ativos em nuvem.
5.15	Deve realizar a avaliação das comunicações com destino a internet relacionadas a atividades ou endereços maliciosos ou vulneráveis, identificando os usuários e dispositivos envolvidos, fornecendo informações de mitigação do risco detectado.
5.16	Possuir console Web para gerenciamento e administração da ferramenta.
5.17	Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e maliciosas para identificação e categorização de ameaças no ambiente.
5.18	Deve fornecer um índice de risco com base nas configurações de produtos integrados do fornecedor para reduzir o risco induzido por erros humanos.
5.19	Permitir criação de listas de exceção de objetos para redução de falso-positivo.
5.20	Os modelos de detecção deverão possuir níveis de severidade (score) individuais para cada modelo em pelo menos os seguintes níveis: crítico; alto; médio; baixo.
5.21	Deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar sua organização a se defender proativamente contra ameaças.
5.22	Deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e terceiros para ajudar na identificação de ameaças.
5.23	Os relatórios de ameaças do fabricante deverão gerar alertas de detecção caso sejam identificadas atividades presentes nos relatórios dentro do ambiente.
5.24	Deve ser possível identificar individualmente cada relatório de ameaça.

5.25	Deve permitir adicionar bases de inteligência terceiras de forma manual, por API, importando arquivos com base CSV ou STIX através de assinatura de feeds de inteligência de ameaças terceiros.
5.26	Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais.
5.27	O campo de busca deve permitir o uso de múltiplos operadores lógicos para no mínimo: E; Ou; Não.
5.28	Deve permitir indexar múltiplas buscas utilizando operadores lógicos.
5.29	Deve permitir salvar pesquisas com os critérios de busca e operadores lógicos utilizados para futuras consultas.
5.30	Deve permitir pesquisar por atividades de cada um dos contextos, mesmo que não tenham gerado qualquer tipo de detecção pelos modelos de detecção de ameaça.
5.31	Deve permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa raiz.
5.32	Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento.
5.33	Deve somar as pontuações (score) de cada modelo durante a correlação das atividades para melhor categorização do incidente.
5.34	Deve exibir todos os detalhes do incidente em uma única página, contendo no mínimo: Status do incidente; Score; Quantidade de contas de e-mail impactadas; Data e hora da detecção; Técnica do MITRE utilizada; Modelo(s) de detecção acionado(s); Objetos detectados dentro de cada modelo; Deve permitir alterar o status de cada evento, para no mínimo Novo, Em progresso/análise e Fechado ou escala equivalente.
5.35	Permitir adicionar comentários e notas a cada evento pelos analistas da ferramenta.

5.36	Durante o processo de análise da cadeia de processos deve ser possível verificar todos os objetos relacionados à esta análise, as atividades executadas pelos objetos e sua reputação conforme categorização do fabricante.
5.37	Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta.
5.38	Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção.
5.39	Permitir adicionar um comentário junto a cada ação tomada para registro e contextualização das ações.
5.40	Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores.
5.41	Permitir coletar e fazer o download de um arquivo para investigação local detalhada.
5.42	Permitir adicionar o remetente (sender) de um e-mail na lista de bloqueio, impedindo o mesmo de enviar novos e-mails os usuários da sua empresa.
5.43	Mover o e-mail selecionado para a área de quarentena de um específico usuário ou todos os usuários que contenham este e-mail em suas caixas.
5.44	Deletar o e-mail selecionado das caixas selecionadas.
5.45	Deve permitir verificar todas as ações de respostas executadas no console ou por API.
5.46	Deve exibir os seguintes painéis de controle: Índice de risco da empresa; MITRE ATT&CK® Mapping for Enterprise; Visão geral de alertas; Top 10 vulnerabilidades em risco; Top 10 usuários em risco; Top 10 dispositivos em risco;
5.47	Deve permitir a geração e o download de relatórios únicos e/ou agendados.

5.48	Deve possuir a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado.
5.49	Deve permitir exportar sob demanda os logs em texto puro (CSV ou PDF).
5.50	Deve permitir investigação por palavras-chave customizadas para facilitar a busca de eventos.
5.51	Deve permitir recebimento e encaminhamento de logs via syslog.
5.52	Deve permitir receber logs de diferentes dispositivos.
6	**Proteção Host IPS e Host Firewall**
6.1	Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais: Microsoft Windows 8 e versões superiores; Windows Server 2008 e versões superiores.
6.2	Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall.
6.3	O módulo deve ser integrado como solução do *endpoint* e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional.
6.4	Todas as regras das funcionalidades de *firewall* e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio).
6.5	Deve permitir ativar e desativar o produto sem a necessidade de remoção.
6.6	Deve possuir capacidade de identificar e bloquear, no mínimo, os seguintes tipos de ataques: Denial of Service (DOS); Port scanning; Network Flooding.
6.7	Deve permitir a emissão de alertas via SMTP ou SNMP.
7	**Controle de aplicações de *endpoints***

7.1	Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais: Microsoft Windows 8 e versões superiores; Windows Server 2008 e versões superiores.
7.2	O módulo deve ser integrado como solução do *endpoint* e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional.
7.3	Deve permitir a criação de políticas de segurança personalizadas.
7.4	As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios: Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina; Range de endereços IPS; Sistema operacional;
7.5	Grupos de máquinas espelhados do Active Directory; Usuários ou grupos do Active Directory. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política.
7.6	As políticas de segurança devem permitir o controle do intervalo de envio dos logs.
7.7	As políticas de segurança devem permitir o controle do intervalo para envio de atualização de cada política.
7.8	As políticas de segurança devem permitir a definição de qual servidor de gerenciamento o agente de segurança deve comunicar-se.
7.9	As políticas de segurança devem permitir a ocultação do ícone do agente, que reside da barra de tarefas, e de notificações ao usuário.
7.10	As políticas de segurança devem permitir o controle através de regras de aplicação.
7.11	As regras de controle de aplicação devem permitir as seguintes ações: Permissão de execução; Bloqueio de execução; Bloqueio de novas instalações.

7.12	As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra.
8	**Proteção contra vazamento de informações (DLP) de Endpoints**
8.1	Deve ser capaz de realizar a proteção contra vazamento de informações nos seguintes sistemas operacionais: Microsoft Windows 8 e versões superiores.
8.2	O módulo deve ser integrado como solução do *endpoint* e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional.
8.3	Deve possuir nativamente templates para atender as seguintes regulamentações: PCI/DSS; HIPA; Glba; SB-1386; US PII.
8.4	Deve ser capaz de detectar informações, em documentos nos formatos: Documentos: Microsoft office (doc, docx, xls, xlsx, ppt, pptx) openoffice, rtf, wordpad, text; xml, html; Gráficos: visio, postscript, pdf, tiff; Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh; Códigos: c/c++, java, verilog, autocad.
8.5	Deve ser capaz de detectar informações, com base em: Dados estruturados, como dados de cartão de crédito, dados pessoais, endereços de e-mail, CPF, entre outros, através de palavras ou frases exatas, padrão de documentos conhecidos e formato pré-definido de identificação de dados; Dados não-estruturados, como documentos exportados, reformatados ou sem estrutura de dados definida, através de expressões regulares ou descoberta de dados por aprendizado de padrões e criação de fingerprinting.

8.6	Deve permitir a criação de modelos personalizados para identificação de informações.
8.7	Deve permitir a criação de modelos com base em regras e operadores lógicos.
8.8	Deve possuir modelos padrões.
8.9	Deve permitir a importação e exportação de modelos.
8.10	Deve permitir a criação de políticas personalizadas.
8.11	Deve permitir a criação de políticas baseadas em múltiplos modelos.
8.12	Deve permitir mais de uma ação para cada política, como: Apenas registrar o evento da violação; Bloquear a transmissão; Gerar alertar para o usuário; Gerar alertar na central de gerenciamento; Capturar informação para uma possível investigação da violação.
8.13	Deve permitir criar regras distintas com base se a estação está fora ou dentro da rede.
9	**MacOS**
9.1	Deve ser compativel com as seguintes versões do MacOS: MacOS 10.15 (Catalina); MacOS 12.0 (Monterey); MacOS 14.0 (Sonoma); MacOS 13.0 (Ventura); MacOS 11.0 (Big Sur).
9.2	Deve trabalhar de forma híbrida, fazendo uso de assinaturas, *machine learning* e detecção de comportamento para identificar *malwares* no endpoint.
9.3	Deve possuir uma regra pré-definida para análise de *malware* consultando extensões comumente utilizadas para otimizar o uso de recurso do *endpoint.*
9.4	A solução deve possuir uma regra pré-definida para análise de *malware* consultando somente arquivos Mach-O ou permitir ler todos os arquivos.
9.5	Deve permitir scanear compartilhamentos de rede, arquivos comprimidos e *Time Machine*.

9.6	Em caso de detecção a solução deve tomar uma das seguintes ações: Liberar acesso; Quarentenar; Limpar; Deletar. Deve permitir colocar programa, extensões ou arquivos em exclusão para evitar falso positivos e otimizar o uso de recurso.
9.7	Deve permitir colocar programa, extensões ou arquivos em exclusão para evitar falso positivos e otimizar o uso de recurso.
9.8	Deve possuir a função *Scan Cache*, otimizando o *scan* nas máquinas, armazenando informações dos arquivos que já são conhecidos como bons.
9.9	Deve possuir módulo de proteção contra alteração dos arquivos.
9.10	Deve ser capaz de liberar ou bloquear os seguintes dispositivos: CD/DVD; Compartilhamentos de rede; SD card; Dispositivos thunderbolt de armazenamento; Dispositivos de armazenamento USB; Deve ser possível adicionar dispositivos de armazenamento USB a lista de dispositivos permitidos utilizando nome do fabricante, ID do dispositivo e número de serial.
9.11	Deve ser possível configurar ao menos as seguintes ações: Acesso total; Somente leitura; Bloqueio.
Item 3 - Solução de Proteção de Ameaças Persistentes Avançadas com detecção e respostas estendidos.	
3.1	A solução deverá ser instalada de modo a detectar ameaças avançadas no ambiente da CONTRATANTE, inspecionando o tráfego de rede, independente de agentes instalados;
3.2	Deve ser dimensionada para inspecionar 500 Mbps de throughput;

3.3	A solução deve permitir que o administrador escolha uma implementação em modo in-line ou em modo de monitoramento através de tráfego espelhado;
3.4	Caso seja implementada no modo in-line, a solução deverá permitir criar um by-pass para casos de falhas de interface;
3.5	Quando in-line, a solução deverá ter a capacidade de analisar tráfego TLS; Funcionalidades e Requisitos específicos:
3.6	Deverá fornecer solução integrada de proteção contra ameaças avançadas de acordo com funcionalidades e características técnicas especificadas neste documento, contendo, no mínimo os seguintes módulos: Monitoramento, Identificação, Análise e Resposta de Incidentes de Segurança Detecção de ataques direcionados;" Monitoramento, Identificação, Análise e Resposta de Incidentes de Segurança Detecção de ataques direcionados; Analisador virtual de ameaças; Correlação de regras para detecção de conteúdo malicioso Análise de todos os estágios de uma sequência de ataques.
3.7	Esta solução deverá ser atendida através do fornecimento de solução de um único Fabricante, contendo: Serviço de Monitoração e Análise de Ameaças Digitais em rede;
3.8	Serviço de Monitoração e gestão de riscos que permita a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente;
3.9	Serviço que entenda ameaça digital como a representação de um software malicioso ou ação maliciosa tal como: spyware, phishing, worms, bot, trojan, adware, network Exploit, web Exploit, Cross-site scripting, spear phishing, information stealing malware e outras ações que podem compor ataques ao patrimônio computacional do ambiente;

3.10	Visibilidade e relatório de incidentes de conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos;
3.11	Análise e correlação de atividades maliciosas tais como: Detecção específica de malwares conhecidos e arquivos contaminados através de assinaturas de antivírus tradicional no tráfego da rede; Detecção de vermes de rede e de e-mail no tráfego de rede; Detecção de programas de exploração de vulnerabilidades (Exploits) na rede; Detecção de empacotamentos maliciosos no tráfego da rede;
3.12	Validação de tráfego web malicioso através de consultas a sistemas de reputação na Internet;
3.13	Visibilidade e relatório de estatísticas de ameaças, fontes de infecção na rede monitorada e máquinas comprometidas.
3.14	Permitir a rápida identificação da criticidade dos eventos de segurança;

3.15	Permitir realizar pesquisas avançadas e customizadas dos incidentes de segurança através da console de gerenciamento i. Possibilidade de criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de incidentes de segurança; ii. Permitir a customização de alertas em base ao tipo de incidente de segurança através da console de gerenciamento; iii. Permitir a integração com sistemas de serviço de diretório; iv. Capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP; v. A análise de SMTP poderá ser realizada em uma solução separada do sensor de HTTP e demais protocolos; vi. A capacidade de análise de artefatos em sandbox pode ser realizada através de no mesmo equipamento de análise; vii. A solução deverá possuir mecanismo de conhecimento de senhas de pelo menos 05 palavras chaves em seu vocabulário de conhecimento, para derivação de arquivos protegidos; viii. Capacidade de criar e salvar investigações customizadas dos incidentes de segurança; ix. Deve possuir pelo menos 1 sensor para inspecionar o tráfego de rede de throughput de 500 Mbps de análise; x. Deve possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques; xi. Deve detectar atividades maliciosas que trafegam na rede através de motor de análise de comportamento de tráfego até o nível 7 (camada de aplicação) em protocolo TCP/IP; xii. Capacidade de detectar ameaças web tais como vulnerabilidades e download de conteúdo malicioso;

3.16	Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP /RTP-TCP, RTSP/RDT-UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP, Bittorent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP;
3.17	Deve possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura; Capacidade de oferecer informações para análise forense de artefatos suspeitos de serem maliciosos;
3.18	Gerenciamento centralizado de todas as etapas dos eventos de segurança identificados como possíveis ameaças;
3.19	Capacidade de identificar artefatos maliciosos direcionados para dispositivos moveis rodando o sistema operacional Android, tais como telefones inteligentes e tablets;
3.20	Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF´s, executáveis, PPT, DOC, XLS, ZIP e RAR;
3.21	A solução deve detectar ameaças do dia zero, vulnerabilidade, URL’s maliciosas e spams dirigidos no protocolo SMTP;

3.22	Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;
3.23	Deve permitir o uso de base de conhecimento na Internet do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações de ações;
3.24	Deve permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança;
3.25	Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos (compactados);
3.26	Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística;
3.27	Deve possuir foco em proteção contra APTs (Advanced Persistent Threats);
3.28	Deve possuir tecnologia de proteção contra ameaças desconhecidas (ataques dirigidos e ameaças de dia zero), sendo que este módulo deve pertencer ao mesmo fabricante;
3.29	Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou switches;
3.30	Deverá possuir suporte para balanceamento de carga no sensor de inspeção de tráfego, possibilitando assim obter uma melhor performance;
3.31	Deverá permitir a análise específica de eventos de segurança de computadores suspeitos de atividade maliciosa;
3.32	Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em ponto único;

3.33	Deve possuir atualização automática de regras e assinaturas, sendo que estas devem ser disponibilizadas via web pelo fabricante da solução;
3.34	Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução;
3.35	Deve ser capaz de identificar movimentos laterais em uma rede corporativa;
3.36	Deve atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;
3.37	Deve possuir interface web para busca e investigação local de incidentes;
3.38	O ambiente controlado de sandbox deve contemplar, pelo menos, os sistemas operacionais CentOS, Windows 10, Windows 7, Windows Server 2003, 2008, 2012 R2, 2016 e 2019; 18.19.56. Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web;
3.39	Deve possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e Botnets;
3.40	Deve possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado;
3.41	Deve possuir regras que identifiquem comunicações p2p, instant messengers e streaming;

3.42	Deve possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características: i. Resumidos; ii. Visão Geral dos Incidentes de Segurança; iii. Discriminação dos Tipos de Incidentes Top Ameaças Analisadas; iv. Top Hosts Infectados Recomendações de Segurança Executivos; v. Deve possuir detalhes técnicos dos incidentes detectados; vi. Deve possuir estatística do tráfego analisado; vii. Deve possuir indicadores de risco do ambiente; viii. Recomendações de Segurança.
3.43	Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e dinamicamente atualizada, hosts com alto nível de risco, classificando os tipos de riscos/eventos detectados;
3.44	Deve possuir interface que apresente em Real Time estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas, etc;
3.45	Quando detectada uma ameaça, a solução deve prover, podendo esta realizar consultas em site do fabricante, informações sobre ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada;
3.46	As atualizações do produto (patterns e outros componentes) não devem causar downtime ou impacto na operação;
3.47	Deve ser capaz de identificar ameaças que afetam dispositivos móveis (Ex. Detecção de comunicação de aplicativo malicioso na plataforma Android);
3.48	Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso deportas comuns ou protocol tunneling;

3.49	Deve ser capaz de detectar tentativas de scan de rede;
3.50	Deve ser capaz de detectar propagação de malwares na rede;
3.51	Deve ser capaz de detectar tentativas de brute-force;
3.52	Deve ser capaz de detectar tentativas de fuga e roubo de informação; Deve ser capaz de detectar ameaças que se replicam na rede;
3.53	Deve ser capaz de detectar Exploits na rede;
3.54	O Monitoramento de protocolos de comunicação deve ser feito através de appliance único (ou virtual appliance);
3.55	A console de gerenciamento deve possuir mapa mundial, onde são marcadas origens de ataques e eventos de segurança monitorados pela solução;
3.56	Deve permitir busca por informações do destino e origem, incluindo estas: endereço IP, endereço MAC, porta e protocolo;
3.57	Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;
3.58	Capacidade de salvar uma investigação antes de ser finalizada;
3.59	Capacidade de restaurar uma investigação para continuá-la ou consultá-la;
3.60	Capacidade de emitir relatórios baseados nas investigações;
3.61	Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos;
3.62	Deve trabalhar com geo-localização para identificar a origem geográfica de um ataque;
3.63	Deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado;
3.64	Deve permitir exportar sob demanda os logs em texto puro (CSV ou similar);

3.65	Deve sugerir consultas a bases de reputação e whois quando encontrados hosts e nomes de domínio;
3.66	Deve permitir investigação por tags (palavras-chave) pré-configuradas para facilitar a busca de eventos;
3.67	Deve permitir recebimento de logs via syslog;
3.68	Deve permitir encaminhamento de logs via syslog;
3.69	Deve permitir receber logs de diferentes dispositivos;
3.70	Deve possuir engine de correlação de eventos;
3.71	Deve inserir tags personalizadas nos logs, de acordo com regras especificadas pelo usuário;
3.72	A solução de análise em sandbox deve ter a capacidade de analisar, de forma estática e dinâmica, ameaças com características de autoinicialização ou alteração de arquivos de sistema, rootkits/cloakings, arquivos mal-formados, engenharia social, dentre outros;
3.73	A análise de sandbox deve identificar e analisar ameaças que tenham características de evitar a segurança e análise em sandbox, e auto-preservação;
3.74	Deve enviar alertas via e-mail para pelo menos 100 e-mails diferentes;
3.75	Deve permitir a configuração de alarmes personalizados, com base em investigações;
3.76	Deve informar em sua console alarmes que dispararam, até que o usuário tome alguma ação;
3.77	A console de gerenciamento deverá ser web, apresentando alta disponibilidade de modo que na ausência da principal, o restante da solução permaneça ativa e funcionando;
3.78	A solução deve ser escalável horizontalmente, permitindo que novas instâncias sejam habilitadas, aumentando suas capacidades de detecção e analise;

3.79	A console de gerenciamento deverá ter dashboards para facilidade de monitoração. As janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração;
3.80	O administrador deve poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização;
3.81	Deverá possuir mapa geográfico que permita a identificação visual sobre a origem de ameaças demodo a facilitar a visualização de eventos críticos para que ações imediatas sejam providenciadas;
3.82	Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;
3.83	A console de gerenciamento deverá ser gerenciada por Internet Explorer, Google Chrome e Firefox;
3.84	Solução deverá ter mecanismo de busca em sua console de gerenciamento de modo que seja facilitada a busca por detecções;
3.85	Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;
3.86	Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque;
3.87	Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações: i. Uso de CPU Uso de Disco; ii. Uso de Memória; iii. Tráfego malicioso analisado; iv. Todo o tráfego analisado.

3.88	A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deverá conter no mínimo: i. Tipo de evento de detecções: Conteúdo malicioso, reputação de URL's, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware; ii. Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.
3.89	A solução deverá ter integração com ferramentas de SIEM;
3.90	Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa;
3.91	A solução deve prover serviço de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em transito através de logs de sensor;
3.92	Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo: i. Computadores infectados; ii. Origem de infecções; iii. Estatísticas de ameaças; iv. Riscos potenciais de segurança; v. Riscos de perda de informações; vi. Risco de sistema comprometido; vii. Infecções de malware.
3.93	A solução deverá apresentar função de pesquisa por logs contendo no mínimo: Critérios de pesquisa por dia, mês e ano.

3.94	Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos;
3.95	Possibilidade de pesquisa por ameaças, URL's maliciosas, análises virtuais, correlação de incidentes, nome de malware, protocolo e direção da detecção;
3.96	Os relatórios e logs deverão ser exportados nos formatos PDF ou CSV.
Item 4 - Solução Proativa de Validação de Integridade de Ativos	
4.1	A solução proposta deve ser oferecida como software e deve ser capaz de funcionar na plataforma x86, não sendo aceito solução software livre.
4.2	A solução proposta deve ser capaz de funcionar 100% on-premise ou SaaS
4.3	A solução proposta deve fornecer uma arquitetura de sistema unificada e uma interface de usuário para realizar testes de ataques reais (testes de penetração) e testes de ataques simulados (emulação cibernética do adversário)
4.4	A solução proposta deve suportar um processo totalmente automatizado capaz de simular o comportamento de um hacker real para analisar/descobrir as exposições da superfície de ataque dos alvos, as vulnerabilidades do sistema e, em seguida, explorar automaticamente as vulnerabilidades do sistema para validar o risco real dos alvos, utilizando exploits reais.
4.5	A solução proposta deve suportar uma arquitetura escalável que permita a análise de redes/sistemas em grande escala e a definição de perfis de ativos, a descoberta de vulnerabilidades e a extração da base de conhecimentos, a exploração automática de vulnerabilidades, a pós-exploração e a definição de prioridades/relatórios de riscos
4.6	A solução proposta deve suportar, pelo menos, 4 níveis de controle de nível ruído na rede para tarefas de testes de penetração, incluindo Modo Stealthy, modo Intermediário, modo normal e modo Noisy

4.7	A solução proposta deve poder ser executada na plataforma x86 e deve suportar o sistema operacional Linux 64 bits
4.8	A solução proposta deve poder ser implantada em servidores bare metal ou em ambientes virtuais VMware e Microsoft Hyper-V
4.9	A solução proposta deve poder ser implantada em plataformas de nuvem públicas, por exemplo, Amazon Web Service, Microsoft Azure e Google Cloud Platform
4.10	A solução proposta deve ser capaz de utilizar a capacidade de multiprocessamento simétrico da plataforma de servidor x86 para aumentar o desempenho de um servidor standalone.
4.11	A solução proposta deve ser capaz de executar vários threads de bots no servidor e cada thread pode executar as suas próprias tarefas de teste para melhorar o desempenho geral do sistema.
4.12	A solução proposta deve suportar, pelo menos, 100 threads simultâneas no servidor, se a configuração do hardware do servidor permitir. O número de threads simultâneas deve se basear nos recursos computacionais do servidor e será configurável pelos administradores do sistema
4.13	A solução proposta deve suportar a arquitetura de plugins/exploits para a descoberta e exploração de vulnerabilidades, e a base de conhecimentos de plugins deve estar 100% on-premise e pode ser atualizada offline em um ambiente em que o acesso à Internet não esteja disponível
4.14	A solução proposta deve suportar um ambiente amplo, os alvos suportados devem incluir hosts, servidores Web, sistemas de gestão de conteúdos Web, servidores de aplicações, sistemas de gestão de bases de dados, equipamento de rede, equipamento IoT, equipamento SCADA, etc.
4.15	A solução proposta deve ter uma base de conhecimentos de plugins de vulnerabilidade/exploits com mais de 36 000 plugins,
4.16	Cada plug-in deve incluir a pontuação CVSS, o vetor CVSS e as informações sobre o número CVE, se disponíveis

4.17	Cada plug-in deve ter associado um nível de severidade da vulnerabilidade e um nível de controle do risco de exploração.
4.18	O nível de severidade do plugin deve ser Alto, Médio, Baixo e Informativo
4.19	A solução proposta deve suportar plugins de vulnerabilidade/exploits desenvolvidos pelo administrador
4.20	A solução proposta deve suportar o modo de intervenção do usuário e ter logs dos ataques de teste de penetração de impacto elevado
4.21	A solução proposta deve suportar a capacidade de descoberta de ativos e de superfícies de ataque sem consumir qualquer licença. O administrador pode utilizá-la para descobrir a infraestrutura de TI e identificar ativos críticos e superfícies de ataque de portas abertas de servidores e superfícies de ataque de URL de sites Web.
4.22	A solução proposta deve permitir a descoberta eficaz de hosts e portas, minimizando o risco de bloqueio pelo firewall
4.23	A solução proposta deve suportar cenários pré-definidos para os seguintes casos de utilização de testes de penetração, por exemplo, penetração de sites e aplicações Web, penetração de intranets, penetração de hosts, penetração autenticada do Windows, penetração de ransomware, validação de senhas fracas, etc., simplificando a operação de pentest para os administradores do sistema
4.24	A solução proposta deve ser compatível com cenários de pentest de ataques internos (por exemplo, hosts/aplicações na Intranet) e externos (por exemplo, sites Web hospedados na nuvem, CDN, etc.)
4.25	A solução proposta deve suportar tanto o cenário de blackbox como o cenário de graybox (autenticada)
4.26	A solução proposta deve suportar cenário de penetração de ransomware, pode simular técnicas populares de intrusão de ransomware para explorar e validar os riscos dos alvos para potenciais ataques de ransomware

4.27	A solução proposta deve suportar scan de host e o scan de Web e permitir que o administrador do sistema configure parâmetros de rede (por exemplo, portas, método de scan) e parâmetros de Web crawler (por exemplo, modo de crawler, níveis de URL, política de página 404, filtro de sufixos, filtro de URL, whitelist de URL) para tarefas de scan
4.28	A solução proposta deve suportar testes de penetração autenticados em aplicações web. Para sites Web não padrão, a solução proposta deve fornecer um login sequence de início de sessão de um site Web que possa ser utilizado para o início de sessão automática de um site Web não padrão durante uma tarefa de teste
4.29	A solução proposta deve suportar o Web Scan tanto para páginas Web estáticas como para páginas Web dinâmicas para descoberta de vulnerabilidades e validação de riscos
4.30	A solução proposta deve suportar um modo inteligente de scan Web. O sistema selecionará automaticamente crawler dinâmico ou estático de páginas Web com base no framework Web utilizado pelo site Web analisado.
4.31	A solução proposta deve suportar a tecnologia de by-pass de senha para páginas Web e deve ser capaz de descobrir superfícies de ataque de sites Web protegidos por senhas
4.32	A solução proposta deve permitir que o administrador do sistema configure o modo proxy para Smart Crawling
4.33	A solução proposta deve suportar testes de penetração autenticados em Windows (Graybox), deve ser capaz de descobrir e verificar o risco de Credential Harvesting e o risco de EoP (Elevação de Privilégio)
4.34	A solução proposta deve suportar a capacidade de pesquisa de plugins de vulnerabilidade/exploits na interface de gerenciamento
4.35	A solução proposta deve suportar a integração com um scanner de vulnerabilidade de terceiros e ter um cenário dedicado para validar os resultados do scanner de vulnerabilidade, por exemplo, Tenable Nessus Pro, Rapid7 Nexpose e Qualys

4.36	A solução proposta deve suportar ataques de força bruta a serviços, incluindo, mas não se limitando a DB2, FTP, Micrsoft SQL Server, MySQL, PostgreSQL, RDP, Redis, Microsoft SMB, SNMP, SSH, Telnet, Web User Login, VNC, InfluxDb, Vmware ESXi, Weblogic, Drupal, Joomla, Apache CouchDB, Apache Tomcat, Apache ActiveMQ, Apache Axis2, RabbitMQ, SonarQube, etc.
4.37	A solução proposta deve detectar diferentes tipos de risco e mostrar a vulnerabilidade com o tipo de risco, por exemplo, divulgação de PII
4.38	A solução proposta deve suportar credenciais personalizadas e importação de dicionário para ataques de força bruta
4.39	A solução proposta deve suportar o teste de penetração de API Web através de, pelo menos, duas abordagens - teste Blackbox e teste Graybox
4.40	A solução proposta deve suportar o teste de penetração de API Web para descobrir as vulnerabilidades da API nas categorias da OWASP Top 10.
4.41	A solução proposta deve suportar o teste de penetração da API Web para detectar API endpoints, broken access, broken object level authorization e Hidden path e divulgação de informações sensíveis
4.42	A solução proposta deve suportar o administrador a manter o ambiente em conformidade com os padrões OWASP Top-10 (2017 e 2021), ISO27001, PCI-DSS
4.43	A solução proposta deve suportar a exploração automática de vulnerabilidades, com exploits reais, e deve ser capaz de mostrar o progresso da exploração em tempo real na sua interface Web
4.44	A solução proposta deve permitir que o administrador configure a exploração com base no tipo de sistema operacional, nos níveis de severidade da vulnerabilidade, nos níveis de controle dos riscos de exploração e em palavras-chave definidas pelo administrador
4.45	A solução proposta deve permitir ao administrador desativar a funcionalidade de exploração automática para proporcionar maior flexibilidade no controle dos riscos

4.46	A solução proposta deve permitir a execução de plugins de exploração individuais com base na configuração do administrador na interface de gerenciamento
4.47	A solução proposta deve ser capaz de mostrar a topologia de ataque do ambiente alvo com, pelo menos, 5 camadas de informação durante a exploração, incluindo, entre outros, o IP da máquina alvo, o serviço, a superfície de ataque, a vulnerabilidade e o risco de negócio
4.48	A solução proposta deve ser capaz de mostrar toda a informação da cadeia de ataque (Kill Chain) de uma vulnerabilidade explorada
4.49	A solução proposta deve suportar a configuração da shell reversa para validar a exploração de uma vulnerabilidade RCE
4.50	A solução proposta deve suportar a implantação de um persistent listeners em um host designado para permitir que os hosts explorados se conectem e validem a exfiltração de dados
4.51	A solução proposta deve ser capaz de fornecer provas de uma exploração bem-sucedida, incluindo, mas não se limitando a bancos de dados, snapshots, outputs da webconsole CLI, captura de tela do host comprometido, diretórios do sistema de arquivos, credenciais
4.52	A solução proposta deve ser capaz de fornecer validação com um clique para revalidar a vulnerabilidade e a correção
4.53	A solução proposta deve ser capaz de fornecer a funcionalidade de cleanup com um clique
4.54	A solução proposta deve suportar movimentação lateral da pós-exploração e pode utilizar um ativo comprometido como um pivô para descobrir e explorar ativos adicionais em redes adjacentes
4.55	A solução proposta deve ser capaz de calcular o risco do sistema alvo com base no impacto da vulnerabilidade explorada e nas informações da Kill Chain
4.56	A solução proposta deve poder calcular a pontuação global do sistema alvo com base no número de superfícies de ataque encontradas, no número e na severidade das vulnerabilidades e dos riscos,

	bem como na taxa de conversão de superfícies de ataque em vulnerabilidades e de vulnerabilidades em riscos
4.57	Para cenários de BAS, a solução proposta deve fornecer um agente de software que seja instalado em alvos de avaliação e simule ciberataques reais sem qualquer dano ou impacto real no ambiente
4.58	Para cenários de BAS, a solução proposta deve suportar plataformas Windows e Linux para instalar o agente de ataque simulado
4.59	Para cenários de BAS, a solução proposta deve suportar teste de assessment separado que possa ser executado de forma independente no agente de teste de avaliação
4.60	Para cenários de BAS, a solução proposta deve fornecer uma medição da taxa de bloqueio para todos os scripts de teste de avaliação executados
4.61	Para cenários de BAS, a solução proposta deve suportar o framework do MITRE ATT&CK ao utilizar o ataque simulado para avaliar os controles de segurança dos sistemas-alvo
4.62	A solução proposta deve ter um cenário específico para identificar e documentar a exposição da superfície de ataque das máquinas-alvo
4.63	A solução proposta deve suportar a priorização de vulnerabilidades com base no risco, fornecer uma tabela simples de riscos de alta prioridade que o administrador precisa mitigar o mais rápido possível
4.64	A solução proposta deve fornecer informações detalhadas sobre cada vulnerabilidade descoberta, incluindo, entre outros, o tipo de vulnerabilidade, a severidade, a pontuação CVSS (Common Vulnerability Scoring System), o vetor CVSS, a descrição, a solução, o link de referência, bem como a máquina vulnerável, superfície de ataque e o attack path para esta vulnerabilidade. A solução também deve fornecer uma ferramenta de validação da vulnerabilidade que ajude o administrador a revalidar a vulnerabilidade após a correção do software

4.65	A solução proposta deve fornecer informações detalhadas sobre cada risco validado, incluindo, entre outros, o tipo de risco, a máquina-alvo comprometida e a sua versão do sistema operacional, a superfície de ataque comprometida, o caminho de ataque, o privilégio do usuário e o tipo de shell que o hacker pode obter.
4.66	A solução proposta deve fornecer um relatório de teste que inclua informações sobre a Kill Chain que o administrador possa utilizar para mitigação
4.67	A solução proposta deve fornecer relatórios históricos e de tendências para a pontuação de saúde das máquinas alvo, o número total de riscos, o número total de vulnerabilidades, o número total de superfícies de ataque e a lista de riscos do teste anterior
4.68	A solução proposta deve fornecer relatórios de comparação para avaliar as alterações da postura de segurança das máquinas-alvo ao longo do tempo, por exemplo, alterações da pontuação de saúde, diferença de risco de negócio, vulnerabilidade e exposição da superfície de ataque de dois testes de validação de segurança
4.69	A solução proposta deve ter uma base de dados centralizada para gerenciar os ativos de TI para validação da segurança. Os ativos gerenciados devem incluir hosts com informações sobre a versão do sistema operacional, portas abertas do servidor e informações sobre aplicações ativas, sites Web e informações sobre aplicações, nomes de domínio e endereços IP, bem como o estado do agente de teste de avaliação
4.70	A solução proposta deve suportar o modelo de licenciamento por subscrição e o administrador deve poder executar um número ilimitado de testes de penetração durante o período da subscrição nos ativos ou aplicações e páginas Web licenciadas
4.71	A solução proposta deve suportar a migração de licenças quando a plataforma de servidor subjacente é alterada
4.72	A solução proposta deve suportar licenças baseadas na quantidade de sistemas alvo (Ativos IP e FQDN)

4.73	A solução proposta deve oferecer uma API RESTful para a integração de sistemas de terceiros
4.74	A solução proposta deve suportar a autenticação baseada em token para a API
4.75	A solução proposta deve oferecer uma console de administração local para a configuração segura do sistema, por exemplo, reset de senha, restart do sistema, shutdown/reboot do servidor, etc.
4.76	A solução proposta deve incluir uma interface de administração baseada na Web através de tráfego criptografado. Não deve ser acessada em texto claro
4.77	A solução proposta deve suportar a autenticação de dois fatores (2FA) para login
4.78	A solução proposta deve suportar a gestão de certificados SSL, deve permitir o administrador fazer o upload do seu próprio certificado SSL ou gerar o seu próprio certificado SSL auto-assinado para a WebUI
4.79	A solução proposta deve suportar atualizações online do sistema e da base de conhecimentos sobre vulnerabilidades/exploits quando o acesso à Internet estiver disponível
4.80	A solução proposta deve ser capaz de atualizar o sistema e a base de conhecimentos sobre vulnerabilidades/exploits em ambientes sem acesso à Internet
4.81	A solução proposta deve suportar o controle de acesso baseado em funções para que os administradores do sistema possam realizar diferentes tarefas, por exemplo, criar novas tarefas de pentest, fazer cópias de segurança do sistema/base de dados, analisar os registos do sistema, etc.
4.82	A solução proposta deve ser pelo menos apresentada nos idiomas inglês e português
4.83	A solução proposta deve suportar backup manual e automático para configurações de tarefas de testes de penetração e bases de dados/registos do sistema
4.84	A solução proposta deve permitir a migração da base de dados do sistema entre diferentes servidores

4.85	A solução proposta deve permitir que o administrador do sistema configure a notificação de tarefas de testes de penetração, por exemplo, por e-mail e syslog.
4.86	A solução proposta deve ser capaz de enviar syslogs compatíveis com CEF para integração com SIEMs ou outras plataformas de gestão centralizada
4.87	A solução proposta deve ser capaz de se integrar com plataforma de DevSecOps como, Jira Cloud, Jira Data Center, ServiceNow e GitLab, para rastreamento de problemas de segurança e bugs
4.88	A solução proposta deve ser capaz de se integrar com uma plataforma de mensagens instantâneas popular (pelo menos Slack) para enviar a notificação para o sistema de mensagens instantâneas, a fim de permitir que a equipa tome conhecimento do evento.
4.89	A solução proposta deve fornecer um relatório integrado para os resultados dos testes de penetração
4.90	A solução proposta deve fornecer relatórios padrão e suportar a funcionalidade de relatórios personalizados para diferentes administradores, por exemplo, executivos, operadores de TI, operadores de SOC, etc.
4.91	A solução proposta deve fornecer relatórios padrão que priorizem os riscos de negócio em relação às vulnerabilidades
4.92	A solução proposta deve fornecer um relatório padrão sobre as vulnerabilidades, os riscos com kill chain e informações gerais sobre a pontuação do sistema
4.93	A solução proposta deve fornecer um relatório padrão sobre asset profilling, incluindo fingerprints do sistema
4.94	A solução proposta deve fornecer um modelo de relatório de superfície de ataque para comunicar todas as superfícies de ataque expostas publicamente dos sistemas-alvo
4.95	A solução proposta deve fornecer modelos de relatório de conformidade OWASP Top-10:2017 e OWASP Top-10:2021 para tarefas de testes de penetração na Web

4.96	A solução proposta deve suportar vários formatos de relatório, incluindo, mas não se limitando a, PDF, HTML, CSV.
4.97	A solução proposta deve oferecer suporte multilingual para os relatórios, por exemplo, inglês, italiano, espanhol, português e coreano
4.98	A solução proposta deve permitir que um cliente adicione o logótipo da sua empresa na primeira página dos relatórios de pentest
4.99	A solução proposta deve permitir de forma nativa que um administrador criptografe o relatório de testes de penetração antes de fazer o download, a fim de proteger os dados sensíveis do usuário contidos no relatório.
4.100	A solução proposta deve ser bem reconhecida pelo setor da cibersegurança, deve ser nomeada como um sample vendor das categorias de “Automated Penetration Testing and Red Teaming Technology” da Gartner e de “Breach and Attacks Simulation” da Gartner
Item 5 - Serviço de Instalação	
5.1	Deverá ser realizado por corpo de profissionais devidamente capacitados para operar e configurar os equipamentos em questão;
5.2	Deverá seguir ritmo e calendário avalizado pelo gestor do contrato;
5.3	Da dinâmica do serviço de instalação: - Na reunião de alinhamento será definido pelo gestor do contrato e a Contratada o cronograma de instalação em cada unidade; - Concluída a instalação da solução a Contratada notificará o Gestor para o recebimento provisório; - A Contratada procederá com a documentação da rede implementada na unidade;

5.4	Dos serviços: - Serão contemplados todos os serviços de instalação física de todos os componentes adquiridos, bem como a montagem dos equipamentos; - Fornecimento de toda a implementação e configuração dos produtos adquiridos;
Item 6 - Serviço de Suporte	
6.1	A CONTRATADA deverá prover GARANTIA e SUPORTE TÉCNICO da solução fornecida, incluindo todos os seus componentes, pelo prazo de 36 (trinta e seis) meses contados a partir da emissão do Termo de Recebimento Definitivo – incluindo suporte do fabricante e fornecimento de peças de reposição e correção de falhas de software e hardware, caso aplicável.
6.2	A CONTRATADA deverá garantir o funcionamento da solução, incluindo todos os serviços, configurações e *tuning*, durante toda a vigência da garantia.
6.3	Toda a garantia deve ser ofertada pelo fabricante, podendo o atendimento de suporte técnico ser realizado pela empresa CONTRATADA ou pelo próprio fabricante.
6.4	O fabricante deve possuir site na internet com a disponibilização de manuais, drivers, firmwares e todas as atualizações existentes relativas à solução ofertada.
6.5	A CONTRATADA deverá ser pertencente à rede autorizada do fabricante e devidamente capacitada para tal função.
6.6	Os serviços referentes à garantia, assistência técnica (preventiva e corretiva), e respectivos serviços de suporte técnico a serem prestado pela CONTRATADA, devem estar disponíveis em regime 24x7 (24 horas por dia, 7 dias por semana) tanto na modalidade on-site (presencial), quanto na modalidade remota, para casos em que este tipo de modalidade não impacte o atendimento.
Item 7 - Serviço de Treinamento	
7.1	Os treinamentos deverão ser realizados e concluídos para até 2 (dois) servidores do CFO, dentro de prazo máximo de 120 (cento e vinte) dias.

7.2	A CONTRATADA deverá fornecer treinamento específico sobre a instalação, operação, configuração e uso do console de gerenciamento, de caráter teórico e prático, da solução de segurança contratadas para 02 (dois) servidores da CONTRATANTE, em Brasília/DF.
7.3	O treinamento deverá ser sem custo adicional ao preço formulado em sua proposta, incluindo o material didático oficial.
7.4	O programa para o treinamento deverá ser previamente aprovado pela CONTRATANTE e eventuais mudanças de conteúdo solicitadas deverão constar no material didático.
7.5	No caso do treinamento fornecido não ser satisfatório, mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, a CONTRATADA deverá realizar novo treinamento sem ônus adicional à CONTRATANTE.
7.6	Deverá ser emitido certificado de participação ao final do curso.
7.7	O escopo deste plano de treinamento para instalação, operação e configuração deve prever: i. informativo global dos componentes tecnológicos envolvidos na prestação dos serviços contratados; ii. compreensão geral da filosofia de funcionamento e de operação da solução adotada; iii. conhecimento e usabilidade dos recursos (hardwares e softwares) envolvidos; iv. funcionalidades do sistema em seus respectivos módulos.
7.8	O plano de treinamento deve prever, para cada tema, a carga horária, recursos e condições imprescindíveis para o perfeito aproveitamento do treinamento incluindo a documentação didática a ser utilizada.
7.9	Os instrutores ou responsáveis pelos treinamentos, certificados pelo fabricante, são de responsabilidade da CONTRATADA e estes devem apresentar ao CNPq as respectivas agendas de treinamento.

7.10	Todo o material de apoio técnico necessário à realização dos treinamentos em ambiente da CONTRATADA, tais como os equipamentos, acessórios, ferramentas, etc. devem ser providos pela CONTRATADA em quantidade suficiente para permitir adequado aprendizado pelos treinados.

5. DA COBERTURA DA GARANTIA

5.1. Durante o período de vigência da garantia, o CONTRATANTE terá o direito de recebimento de todas as novas licenças, versões ou releases dos softwares envolvidos, bem como de softwares que eventualmente venham a ser substituídos.

5.2. Deve cobrir defeitos em quaisquer dos componentes dos produtos fornecidos, incluindo a substituição completa ou parcial de produtos que venham a apresentar problemas de funcionamento, sem ônus adicional para o CONTRATANTE.

5.3. Deve englobar, também, todos os softwares envolvidos (firmwares, drivers, sistema operacional, sistema de gerenciamento etc.).

5.4. Durante o prazo de vigência da garantia a CONTRATADA deverá prestar suporte e assistência técnica aos bens, por meio de manutenção corretiva e preventiva, às suas expensas.

5.5. Durante o serviço de manutenção corretiva ou preventiva, a CONTRATADA deverá executar procedimentos técnicos destinados ao reparo de eventuais falhas apresentadas na solução, de modo a reinstalar a solução com defeito em seu pleno estado de funcionamento e de uso, dentre os quais se incluem a substituição, ajustes e reparos técnicos, em conformidade com manuais e normas técnicas especificadas pelo fabricante.

6. SUBSTITUIÇÃO DE PEÇAS E COMPONENTES

6.1. A substituição de componentes defeituosos, em qualquer caso, deverá ser realizada por item equivalente, ou que possua características superiores, desde que homologadas pelo fabricante como parte compatível da solução.

6.2. Se após a segunda manutenção corretiva, dentro de um período de 90 (noventa) dias, persistirem os mesmos problemas técnicos, a CONTRATADA deverá providenciar a substituição da solução por outro com características e capacidades iguais ou superiores, em até 5 (cinco) dias úteis, às suas expensas.

7. REGISTRO DE ATENDIMENTO

7.1. A CONTRATADA deverá disponibilizar serviço de atendimento de chamados técnicos, via ligação telefônica, ou diretamente via website, ambos em língua portuguesa, inclusive com registro de protocolo para fins de acompanhamento.

7.2. A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante, sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA. Não deve haver limite para aberturas de chamados, sejam de dúvidas/configurações e/ou resolução de problemas de hardware ou software.

7.3. A abertura de chamados poderá ser realizada através de telefone 0800 do Fabricante, através da página da WEB do Fabricante ou através de endereço de e-mail do Fabricante.

7.4. Os atendimentos técnicos deverão ser registrados com a identificação da solução, a descrição clara dos problemas identificados e os procedimentos

adotados para a sua resolução, além de outras informações que se façam necessárias para consultas posteriores.

8. DA MANUTENÇÃO PREVENTIVA

8.1. A manutenção preventiva será destinada a realizar quaisquer operações, como avaliações da rede, ajustes de configuração ou atualizações de softwares, que previnam perdas de desempenho, indisponibilidades ou exploração de vulnerabilidades da solução.

8.2. A manutenção preventiva também será acionada para analisar, detectar e expor problemas, ainda não identificados pela equipe técnica do CONTRATANTE, usando software e ferramentas de diagnóstico especializados. Essa análise imparcial e informativa deverá ser compilada em relatórios abrangentes que podem incluir recomendações sobre como melhorar o desempenho, otimizar a solução e corrigir problemas.

8.3. Durante a manutenção preventiva a CONTRATADA deverá analisar a solução, sua condição atual de funcionamento, seus registros (logs) de sistema e sugerir mudanças para uma melhor prática de utilização da solução. A equipe técnica do CONTRATANTE decidirá sobre a aplicação ou não das recomendações apresentadas.

8.4. Durante o período de vigência da garantia, quando for o caso, todos os firmwares e softwares deverão ser atualizados pela CONTRATADA a cada nova versão ou correção, sem nenhum custo adicional para ao CONTRATANTE.

9. DA MANUTENÇÃO CORRETIVA

9.1. A manutenção corretiva será destinada a resolver os defeitos apresentados pelos componentes de software de toda solução, compreendendo, também, a atualização de versões e correções dos componentes de software que se fizerem necessários.

9.2. A manutenção corretiva será realizada sempre que a solução apresentar defeito ou falha que impeça o seu funcionamento regular e requeira uma intervenção técnica especializada, ou mesmo a substituição de seus componentes, podendo ser solicitada a qualquer momento em que o sistema apresente pane, deficiência ou dificuldade de operação.

9.3. As visitas para prestação do serviço de manutenção corretiva, independentemente da quantidade necessária, não implicarão em custos adicionais para ao CONTRATANTE.

10. OBRIGAÇÕES DA CONTRATANTE

10.1. São obrigações do CFO:

10.1.1. Proporcionar à CONTRATADA todas as facilidades para o perfeito fornecimento do objeto licitado;

10.1.2. Fornecer as informações necessárias e os atos normativos, que no seu âmbito, regem as relações trabalhistas;

10.1.3. Permitir o acesso da contratada ao local determinado para a prestação dos serviços objeto deste contrato, devendo tomar as providências administrativas que garantem o livre desempenho de suas atividades;

10.1.4. Fiscalizar e acompanhar toda a execução dos serviços, por meio de um funcionário especialmente designado para isso, anotando em registro próprio todas as ocorrências relacionadas ao mesmo.

10.1.5. Rejeitar, no todo ou em parte, o serviço entregue em desacordo com as especificações;

10.1.6. Atestar a nota fiscal/fatura correspondente, após realizar rigorosa conferência das características dos serviços;

10.1.7. Providenciar o pagamento a vista conforme preço e condições pactuadas, sobre os quantitativos efetivamente executados, tomando por base os valores unitários cotados na proposta da CONTRATADA;

10.1.8. Notificar a CONTRATADA por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

10.1.9. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais, quando cabíveis;

10.1.10. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura fornecida pela CONTRATADA, em conformidade com o item 6, do Anexo XI da IN SLTI/MP nº 5, de 2017.

11. OBRIGAÇÕES DA CONTRATADA

11.1. São obrigações da CONTRATADA:

11.1.1. A contratada, além das responsabilidades resultantes da contratação, do cumprimento da Lei nº 14.133/2021, Lei nº 10.520/2002, Decreto nº 10.024/2019, demais legislações pertinentes e suas alterações, obriga-se a:

11.1.2. Efetuar a entrega dos bens em perfeitas condições, no prazo e locais indicados pela Administração, em estrita observância das especificações do Edital e da Proposta, acompanhado da respectiva Nota Fiscal constando detalhadamente as indicações da marca, fabricante, modelo, tipo, procedência

e prazo de validade;

11.1.3. Os bens devem estar acompanhados, ainda, quando for o caso, de manuais, bulas, cartilhas, notas explicativas, com versão em português, com todas as informações suficientes e adequadas de fórmulas, manipulação, apresentação, acondicionamento, utilização, contraindicação e riscos;

11.1.4. Responsabilizar-se pelos vícios e danos decorrentes do produto, de acordo com os Artigos 12,13,18 e 26, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

11.1.5. O dever previsto no subitem anterior implica na obrigação de, a critério da Administração, substituir, reparar, corrigir, remover, ou reconstruir, às suas expensas, no prazo máximo de 30 (trinta) dias corridos, o produto com avarias ou defeitos.

11.1.6. Atender prontamente a quaisquer exigências da Administração, inerentes ao objeto da licitação;

11.1.7. Comunicar à Administração, no prazo máximo de 10 (dez) dias corridos que antecedem a data de entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

11.1.8. Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que se está obrigada, exceto nas condições autorizadas no Termo de Referência ou no contrato;

11.1.9. Responsabilizar-se pelas despesas dos tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução do objeto;

11.1.10. Responsabilizar-se pelo ônus resultantes de quaisquer ações, demandas, custos e despesas decorrentes de danos, ocorridos por culpa sua ou de qualquer de seus empregados e prepostos, obrigando-se, outrossim, por quaisquer responsabilidades decorrentes de ações judiciais movidas por terceiros, que lhe venham a ser exigidas por força da Lei, ligadas ao cumprimento

do presente Edital e da Ata que vier a ser assinada;

11.1.11. Responsabilizar-se direta e exclusivamente pela execução do objeto deste edital e, consequentemente, responder, civil e criminalmente por todos os danos e prejuízos que, na execução dele, venha, direta ou indiretamente, a provocar ou causar para a Contratante ou para terceiros;

11.1.12. Manter, permanentemente, representante credenciado para atuar em seu nome e representá-lo junto à Contratante e à Fiscalização, com autoridade para resolver problemas relacionados com o fornecimento dos materiais ora adquiridos;

11.1.13. Recolher aos cofres da Contratante, conforme lhe seja instruído na devida oportunidade, as importâncias referentes às multas que lhe forem aplicadas ou às indenizações devidas, sob-pena de serem descontadas do pagamento de suas Notas Fiscais/Faturas.

12. CRITÉRIOS TÉCNICOS DE HABILITAÇÃO

12.1. Atestado(s) ou Certidão(ões) de Capacidade Técnica, emitido(s) por pessoa jurídica de direito público ou privado, comprovando que a licitante tenha fornecido solução de detecção, correlação e mitigação de ataques cibernéticos com características compatíveis com as exigidas neste edital.

13. DA ENTREGA

13.1. A Contratada terá um prazo de 30 (trinta) dias corridos para efetuar a entrega da solução.

14. DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

14.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da CONTRATANTE, especialmente designados, na forma da lei 14.133/2021.

14.2. O representante da CONTRATANTE deverá ter a experiência necessária para o acompanhamento e controle da execução dos serviços e do contrato.

14.3. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

14.4. O fiscal ou gestor do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos na lei 14.133/2021

14.5. A conformidade do material a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da CONTRATADA que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste Termo de Referência e na proposta,

14.6. informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

14.7. O representante da CONTRATANTE deverá promover o registro das ocorrências verificadas, adotando as providencias necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto na lei 14.133/2021.

14.8. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente,

podendo culminar em rescisão contratual, conforme disposto na lei 14.133/2021.

14.9. A fiscalização da execução dos serviços não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da CONTRATANTE ou de seus agentes e prepostos, de conformidade da lei 14.133/2021.

15. DA GARANTIA CONTRATUAL

15.1. A CONTRATADA, no prazo de até 10 (dez) dias após a assinatura do contrato, prestará garantia no valor correspondente a 5% (cinco por cento) do valor do Contrato, que será liberada de acordo com as condições previstas neste Termo de Referência, conforme disposto na lei 14.133/2021, desde que cumpridas as obrigações contratuais.

15.2. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, até o máximo de 2% (dois por cento).

15.2.1. O atraso superior a 30 (trinta) dias autoriza a CONTRATANTE a promover a retenção dos pagamentos devidos à CONTRATADA, até o limite de 5% (cinco por cento do valor do contrato a título de garantia, a serem depositados junto à CONTRATANTE, em dinheiro, com correção monetária.

15.3. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de mais 3 (três) meses após o término da vigência contratual.

15.4. A garantia assegurará, qualquer que seja a modalidade escolhida, o

pagamento de:

15.4.1. Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

15.4.2. Prejuízos causados à CONTRATANTE ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;

15.4.3. As multas moratórias e punitivas aplicadas pela CONTRATANTE à CONTRATADA.

15.5. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

15.6. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados a partir da data em que for notificada.

15.7. A CONTRATANTE não executará a garantia na ocorrência de uma ou mais das seguintes hipóteses:

15.7.1. Caso fortuito ou força maior;

15.7.2. Alteração, sem prévia anuência da seguradora, das obrigações contratuais;

15.7.3. Descumprimento das obrigações pelo contratado decorrentes de atos ou fatos praticados pela CONTRATANTE;

15.7.4. Atos ilícitos dolosos praticados por servidores/empregados da CONTRATANTE.

15.8. Não serão aceitas garantias que incluam outras isenções de responsabilidade que não as previstas neste item.

15.9. Será considerada extinta a garantia:

15.9.1. Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da CONTRATANTE, mediante termo

circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato.

15.10. No prazo de 90 (noventa) dias após o término da vigência, caso a CONTRATANTE não comunique a ocorrência de sinistros.

15.11. Os itens terão garantia mínima de 12 (doze) meses contra defeitos de fabricação, a contar do recebimento definitivo, com atendimento no Distrito Federal.

16. DAS SANÇÕES ADMINISTRATIVAS

16.1. Comete infração administrativa, nos termos das Leis nº 14.133/2021 e 10.520/2002 e do Decreto nº 3.555/2000, a CONTRATADA que no decorrer da licitação:

I. Não celebrar o Contrato, quando convocada dentro do prazo de validade da proposta;

II. Deixar de entregar ou apresentar documentação falsa exigida para o certame;

III. Ensejar o retardamento da execução de seu objeto;

IV. Não mantiver a sua proposta dentro de prazo de validade;

V. Falhar ou fraudar na execução do contrato;

VI. Comportar-se de modo inidôneo, e

VII. Cometer fraude fiscal.

16.2. A CONTRATADA que cometer qualquer das infrações acima discriminadas ficará impedida de licitar e contratar com a União pelo prazo de até 05 (cinco) anos, sem prejuízo da aplicação das multas previstas em Edital e no Contrato, e das demais cominações civil e penal, além de ser descredenciada no SICAF.

16.3. Ainda, a CONTRATANTE poderá aplicar à CONTRATADA, em caso de inadimplemento parcial ou total das suas obrigações, por qualquer uma das

hipóteses previstas na lei 14.133/2021, além das acima elencadas, as penalidades previstas do citado diploma legal, quais sejam:

16.3.1. Advertência escrita, sempre que verificadas pequenas irregularidades, a juízo da Fiscalização, para as quais a CONTRATADA tenha concorrido.

16.3.2. Multas moratória e/ou compensatória.

16.3.3. Suspensão temporária do direito de participar de licitação e impedimento de contratar com o CFO, pelo prazo de até 2 (dois) anos.

16.3.4. 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 o CONTRATANTE pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada.

16.4. As penas de multa ficam assim estabelecidas relativas ao fornecimento de bens e prestação de serviços:

16.4.1. Moratória diária de 0.3% (três décimos por cento), sobre o valor do contrato, em caso de atraso na execução do objeto, limitado a 30 (trinta) dias subsequentes. A partir do trigésimo primeiro dia, configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença. Neste caso, o objeto licitatório será adjudicado ao próximo colocado no certame.

16.4.2. Compensatória de 10% (dez por cento) sobre o valor do Contrato, em caso de inexecução total da obrigação assumida.

16.5. As sanções, quando couberem, serão aplicadas pela autoridade administrativa, mediante instauração de processo administrativo prévio em que serão assegurados o contraditório e a ampla defesa.

16.6. A suspensão temporária de atividade e de impedimento de contratar com a Administração serão aplicadas mediante procedimento administrativo, assegurada a ampla defesa, sempre que a CONTRATADA reincidir na prática de

infrações de maior gravidade à Administração.

16.7. As sanções supracitadas poderão ser aplicadas à CONTRATADA por período de até 2 (dois) anos.

16.8. As penalidades serão obrigatoriamente registradas no SICAF

17. DA DOTAÇÃO ORÇAMENTÁRIA

17.1. As despesas decorrentes deste objeto correrão à conta da Rubrica nº 6.2.2.1.1.01.04.04.004.013-Despesas com Soluções de informática.

18. DO PAGAMENTO

18.1. O pagamento será efetuado pelo CFO até o 10º (décimo) dia útil após a apresentação da nota fiscal/fatura contendo o detalhamento dos serviços executados e os materiais empregados, através de ordem bancária, para crédito em banco, agência e conta corrente indicadas pela CONTRATADA.

18.2. O pagamento somente será autorizado depois de efetuado o “atesto” pelo servidor/empregado competente, condicionado este ato à verificação da conformidade da nota fiscal/fatura apresentada em relação aos serviços efetivamente prestados e aos materiais empregados.

18.3. Havendo erro na apresentação da nota fiscal/fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para

pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CFO.

18.4. Nos termos do item 1, do Anexo VIII-A, da Instrução Normativa SLTI/MPOG nº 5, de 2017, será efetuada a retenção ou glosa do pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:

18.4.1. Não produziu os resultados acordados.

18.4.2. Deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida.

18.4.3. Deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

18.5. Antes de cada pagamento à CONTRATADA, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no Edital.

18.6. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, esta será comunicada, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa.

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

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

18.9. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela autoridade máxima do CFO, não será rescindido o contrato em execução com a CONTRATADA inadimplente no SICAF.

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

18.10.1. A CONTRATADA regularmente optante pelo SIMPLES NACIONAL não

sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na Lei Complementar nº 123/2006.

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

EM = I x N x VP, sendo:

EM = Encargos moratórios

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

VP = Valor da parcela a ser paga

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

$$I = \frac{(TX \div 100)}{365}$$

$TX = Porcentual\ da\ taxa\ anual$ = 6%

(6 ÷ 100)

$$I = \frac{}{365}$$

$$I = 0{,}00016438$$

18.12. A documentação de cobrança não aceita pelo CFO será devolvida à CONTRATADA para a devida correção, com as informações que motivaram sua rejeição pela fiscalização.

19. DAS VEDAÇÕES

19.1. É vedado à CONTRATADA:

a) Caucionar ou utilizar este instrumento para qualquer operação financeira;

b) Interromper a execução do objeto contratual sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

20. ALTERAÇÃO SUBJETIVA

20.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra

pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

ANEXO II DO EDITAL

MODELO DE PROPOSTA DE PREÇOS

1. Destacamos abaixo o modelo de proposta para contratação de empresa especializada em prover Solução Proativa em Nuvem de Detecção, Correlação e Mitigação de Ataques, com Serviço de Treinamento e Serviço de Instalação, conforme especificações e quantidades constantes neste Edital e seus anexos.

O objeto da presente licitação é a escolha da proposta mais vantajosa para o Conselho Federal de Odontologia a eventual contratação de empresa especializada em prover Solução Proativa em Nuvem de Detecção, Correlação e Mitigação de Ataques, com Serviço de Treinamento e Serviço de Instalação,			**PROPOSTA**	
ITEM	**QTD**	**DESCRIÇÃO**	**VALOR UNITÁRIA**	**VALOR TOTAL**
1	175	Solução de Proteção de Endpoints com detecção e respostas estendidos.	R$	R$

2	80	Solução de Proteção de Servidores Físicos, Virtuais e em Nuvem com detecção e respostas estendidos.	R$	R$
3	1	Solução de Proteção de Ameaças Persistentes Avançadas com detecção e respostas estendidos.	R$	R$
4	1	Solução Proativa de Validação de Integridade de Ativos	R$	R$
5	1	Serviço de Instalação	R$	R$
6	36	Serviço de Suporte	R$	R$
7	1	Serviço de Treinamento	R$	R$
VALOR TOTAL DA PROPOSTA R$				

2. Declaramos, ainda, que conhecemos os termos do Edital do Pregão Eletrônico XX/2025 e seus Anexos e que, se vencedora, forneceremos os serviços licitados pelos **PREÇOS UNITÁRIOS** propostos acima durante a vigência do contrato, sendo o faturamento de acordo com o valor TOTAL registrado acima.

3. Esta Proposta tem validade de 60 (sessenta) dias contados da data de abertura da Sessão Pública do Pregão Eletrônico XX/2025 destacado.

DADOS DA EMPRESA

Razão Social:		CNPJ:
Endereço:		Tel/Fax:
CEP:	Cidade:	UF:
Banco:	Agência:	C/C:

DADOS DO REPRESENTANTE LEGAL DA EMPRESA PARA ASSINATURA DO CONTRATO

Nome:

CONSELHO FEDERAL DE ODONTOLOGIA

CPF:	Cargo/Função:
RG:	Órgão Expedidor:
Nacionalidade	

Local e data	Nome e assinatura do responsável legal

Observação: emitir em papel que identifique a licitante.

ANEXO III DO EDITAL

PLANILHA DE PREÇOS ESTIMADOS

GRUPO	ITEM	DESCRIÇÃO	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	1	Solução de Proteção de Endpoints com detecção e respostas estendidos.	175	R$ 179,49	R$ 31.409,88
	2	Solução de Proteção de Servidores Físicos, Virtuais e em Nuvem com detecção e respostas estendidos.	80	R$ 755,58	R$ 60.446,40
	3	Solução de Proteção de Ameaças Persistentes Avançadas com detecção e respostas estendidos.	1	R$ 37.125,59	R$ 37.125,59
	4	Solução Proativa de Validação de Integridade de Ativos	1	R$ 76.104,00	R$ 76.104,00
	5	Serviço de Instalação	1	R$ 72.696,00	R$ 72.696,00
	6	Serviço de Suporte	36	R$ 7.597,07	R$ 273.494,34
	7	Serviço de Treinamento	1	R$ 49.000,00	R$ 49.000,00
VALOR TOTAL					600.276,20

SHIN CA 7 Lote 2 – Lago Norte
71.503-507–Brasília - DF
Tel: (61) 3033-4499
E-mail: licitacoes@cfo.org.br/ Site: www.cfo.org.br