FUNDAÇÃO CULTURAL PALMARES
SCRN 702/703 – Bloco B, - Bairro Asa Norte, Brasília/DF, CEP 70.720-620
Telefone: (61) 3424-0100 - http://www.palmares.gov.br

EDITAL Nº 10/2023

Processo nº 01420.102456/2023-20

# PREGÃO ELETRÔNICO

10/2023

## CONTRATANTE (UASG)

344041

## OBJETO

Aquisição de Solução corporativa para proteção e blindagem e compliance de ativos com garantia, suporte e instalação para o período de 36 (trinta e seis) meses, podendo ser prorrogado até 60 (sessenta) meses, visando o atendimento das necessidades de garantir a segurança das informações bem como prover um serviço de qualidade para os usuários da FCP, conforme especificações e quantitativos apresentados neste documento.

## VALOR TOTAL DA CONTRATAÇÃO

R$ 398.875,00 (trezentos e noventa e oito mil oitocentos e setenta e cinco reais)

## DATA DA SESSÃO PÚBLICA

Dia **20/12/2023** às **9h30min (horário de Brasília)**

## CRITÉRIO DE JULGAMENTO:

Menor preço por grupo

## MODO DE DISPUTA:

Aberto e fechado

## PREFERÊNCIA ME/EPP/EQUIPARADAS
Não

Sumário



**Fundação Cultural Palmares**

**PREGÃO ELETRÔNICO Nº 10/2023**

(Processo Administrativo n° 01420.102456/2023-20)

Torna-se público que a FUNDAÇÃO CULTURAL PALMARES, por meio da Coordenação de Logística/CGI, sediada SCRN 702/703, Bloco “B”, Entrada 18, Lotes 02, 04 e 06, Asa Norte, Brasília/DF, realizará licitação na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 2021, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

### 1. DO OBJETO

1.1. O objeto da presente licitação é a contratação de solução de tecnologia da informação e comunicação de aquisição de solução corporativa para proteção e blindagem e compliance de ativos com garantia, suporte e instalação para o período de 36 (trinta e seis) meses, podendo ser prorrogado até 60 (sessenta) meses, visando o atendimento das necessidades de garantir a segurança das informações bem como prover um serviço de qualidade para os usuários da FCP, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

| ITEM | ESPECIFICAÇÃO | CATSER | UNIDADE DE MEDIDA | QUANTIDADE | VALOR UNITÁRIO | VALOR TOTAL |
|---|---|---|---|---|---|---|
| 1 | Solução de software de segurança de estação de trabalho e servidores para 36 (trinta e seis) meses | 27499 | Unidade | 150 | R$ 2.052,50 | R$ 307.875,00 |
| 2 | Serviços de Instalação | 27022 | Unidade | 01 | R$ 53.000,00 | R$ 53.000,00 |
| 3 | Treinamento Técnico | 3840 | Unidade | 01 | R$ 38.000,00 | R$ 38.000,00 |
| | **TOTAL** | | | | | R$ 398.875,00 |

1.2. A licitação será realizada em grupo único, formados por 03 (três) itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

## 2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

2.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

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

2.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados

cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021 , para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015, bem como para bens e serviços produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010.

2.6. Não poderão disputar esta licitação:

2.6.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.6.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

2.6.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

2.6.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.6.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

2.6.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

2.6.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.6.8. agente público do órgão ou entidade licitante;

2.6.9. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.6.10. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

2.7. O impedimento de que trata o item 2.6.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a

efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.8. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.6.2 e 2.6.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

2.9. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.10. O disposto nos itens 2.6.2 e 2.6.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.11. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

2.12. A vedação de que trata o item 2.6.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

## 3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

3.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

3.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto no item 7.11.1 deste Edital.

3.4. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

3.4.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.4.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de

aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

3.4.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

3.4.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

3.5. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

3.6. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

3.6.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

3.6.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

3.7. A falsidade da declaração de que trata os itens 3.4 ou 3.6 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

3.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

3.9. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

3.10. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

3.11. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.11.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

3.11.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

3.12. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

3.12.1. valor superior a lance já registrado pelo fornecedor no sistema, quando

adotado o critério de julgamento por menor preço; e

3.12.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

3.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 3.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

3.14. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

3.15. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

## 4. DO PREENCHIMENTO DA PROPOSTA

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

4.1.1. valor unitário e total do item;

4.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

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

4.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

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

4.7. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional.

4.8. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

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

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

4.11. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de

prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

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

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

5.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

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

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

5.5. O lance deverá ser ofertado pelo valor unitário do item.

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

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

5.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 100,00 (cem) reais.

5.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.10. O procedimento seguirá de acordo com o modo de disputa adotado.

5.11. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.11.1. 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 até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

5.11.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

5.11.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, 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.

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

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

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

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

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

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

5.17. 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 Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

5.17.1. 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.

5.17.2. A melhor classificada nos termos do subitem 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.

5.17.3. 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.

5.17.4. 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.

5.18. Será assegurado o direito de preferência previsto no artigo 3º da Lei nº 8.248, de 1991, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010, nos seguintes termos:

5.18.1. Após a aplicação das regras de preferência para microempresas e empresas de pequeno porte, caberá a aplicação das regras de preferência, sucessivamente, para:

5.18.1.1. bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

5.18.1.2. bens e serviços com tecnologia desenvolvida no País; e

5.18.1.3. bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da Lei nº 8.248, de 1991.

5.18.2. Os licitantes classificados que estejam enquadrados no item 5.18.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.

5.18.3. Caso a preferência não seja exercida na forma do item 5.18.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 5.18.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 5.18.1.3 caso esse direito não seja exercido.

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

5.19. 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.

5.19.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

5.19.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

5.19.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

5.19.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

5.19.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

5.19.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

5.19.2.1. empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

5.19.2.2. empresas brasileiras;

5.19.2.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

5.19.2.4. empresas que comprovem a prática de mitigação, nos termos daLei nº 12.187, de 29 de dezembro de 2009.

5.20. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.20.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do

preço máximo definido pela Administração.

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

5.20.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

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

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

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

## 6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 2.6 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. SICAF;

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

6.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, *caput*)

6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

6.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

6.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com o item 3.6 deste edital.

6.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

6.7. Será desclassificada a proposta vencedora que:

6.7.1. contiver vícios insanáveis;

6.7.2. não obedecer às especificações técnicas contidas no Termo de Referência;

6.7.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.7.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.7.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

6.8. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

6.8.1. A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

6.8.1.1. que o custo do licitante ultrapassa o valor da proposta; e

6.8.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.9. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

6.10. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

6.11. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação;

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

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

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

## 7. DA FASE DE HABILITAÇÃO

7.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de

2021.

7.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

7.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

7.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

7.4. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia ou por meio digital.

7.5. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

7.6. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

7.7. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

7.8. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

7.9. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

7.9.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

7.10. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN nº 3/2018, art. 7º, *caput*).

7.10.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. (IN nº 3/2018, art. 7º, parágrafo único).

7.11. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.11.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 02 (duas)

horas, prorrogável por igual período, contado da solicitação do pregoeiro.

7.11.2. Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto no § 1º do art. 36 e no § 1º do art. 39 da Instrução Normativa SEGES nº 73, de 30 de setembro de 2022.

7.12. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

7.12.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.12.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

7.13. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

7.13.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.13.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

7.14. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.15. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 7.12.1.

7.16. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

7.17. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

7.18. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

## 8. DOS RECURSOS

8.1. 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.

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

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

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

8.3.1.1. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

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

8.3.3. 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 intimação da ata de julgamento.

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

8.5. 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.

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

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

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

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

8.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico www.palmares.gov.br.

## 9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

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

9.1.1. 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;

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

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

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

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

9.1.2.4. deixar de apresentar amostra;

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

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

9.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

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

9.1.5. fraudar a licitação;

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

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

9.1.6.2. induzir deliberadamente a erro no julgamento;

9.1.6.3. apresentar amostra falsificada ou deteriorada;

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

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

9.2. 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:

9.2.1. advertência;

9.2.2. multa;

9.2.3. impedimento de licitar e contratar e

9.2.4. 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.

9.3. Na aplicação das sanções serão considerados:

9.3.1. a natureza e a gravidade da infração cometida.

9.3.2. as peculiaridades do caso concreto

9.3.3. as circunstâncias agravantes ou atenuantes

9.3.4. os danos que dela provierem para a Administração Pública

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

9.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de **10 (dez) dias** úteis, a contar da comunicação oficial.

9.4.1. Para as infrações previstas nos itens 9.1.1, 9.1.2 e 9.1.3, a multa será de0,5% a 15% do valor do contrato licitado.

9.4.2. Para as infrações previstas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, a multa será de 15% a 30% do valor do contrato licitado.

9.5. 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.

9.6. 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.

9.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 9.1.1, 9.1.2 e 9.1.3, 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.

9.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, bem como pelas infrações administrativas previstas nos itens 9.1.1, 9.1.2 e 9.1.3 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.

9.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 9.1.3, 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.

9.10. 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 intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

9.11. 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 intimação, 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.

9.12. 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.

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

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

## 10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

10.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

10.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

10.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, mediante e-mail endereçado logistica.palmares@gmail.com ou logistica@palmares.gov.br, ou por petição dirigida ou protocolada no endereço SCRN 702/703, Bloco “B”, Entrada 18, Lotes 02, 04, e 06, Asa Norte – Brasília/DF, Fundação Cultural Palmares.

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

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

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

## 11. DAS DISPOSIÇÕES GERAIS

11.1. Será divulgada ata da sessão pública no sistema eletrônico.

11.2. 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.

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

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

11.5. 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.

11.6. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

11.7. 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.

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

11.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

11.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico https://www.gov.br/palmares/pt-br/acesso-a-informacao/licitacoes bem como no endereço SCRN 702/703, Bloco “B”, Entrada 18, Lotes 02, 04, e 06, Asa Norte – Brasília/DF, nos dias úteis, no horário das 09h00 horas às 17h00 horas, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

11.11. ANEXO I do Edital – Termo de Referência;

11.11.1. ANEXO II do Edital – Minuta de Contrato;

11.11.2. ANEXO I – Termo de Referência – Termo de Recebimento Provisório;

14.11.3. ANEXO II – Termo de Referência – Termo de Recebimento Definitivo;

11.11.4. ANEXO III – Termo de Referência – Termo de Compromisso e Sigilo de Dados e Informações;

11.11.5. ANEXO IV – Termo de Referência – Termo de Ciência da Declaração de Manutenção de Sigilo;

11.11.6. ANEXO V – Termo de Referência – Especificações Técnicas da Solução de TIC;

11.11.7. ANEXO VI – Termo de Referência – Estudo Técnico Preliminar;

Brasília - DF, 04 de dezembro de 2023.

AUREA DIAS DE OLIVEIRA Assinado de forma digital por AUREA DIAS DE OLIVEIRA Dados: 2023.12.04 19:23:53 -03'00'

---

## ANEXO II DO EDITAL

**MODELO DE TERMO DE CONTRATO**
**Lei nº 14.133, de 1º de abril de 2021**
**AQUISIÇÕES – LICITAÇÃO**

**FUNDAÇÃO CULTURAL PALMARES**

(Processo Administrativo n° 01420.102456/2023-20)

CONTRATO ADMINISTRATIVO Nº ...../...., QUE FAZEM ENTRE SI A UNIÃO, POR INTERMÉDIO DO (A) ..... E .....

A FUNDAÇÃO CULTURAL PALMARES, com sede no SCRN 702/703, Bloco “B”, Lotes 02, 04 e 06, Entrada 18, Asa Norte, na cidade de Brasília/DF, inscrito(a) no CNPJ sob o nº 32.901.688/0001-77, neste ato representado(a) pelo(a) ..... (cargo e nome), nomeado(a) pela Portaria nº ....., de ..... de ..... de 20..., publicada no DOU de ..... de ..... de ....., portador da Matrícula Funcional nº ....., doravante denominado CONTRATANTE, e o(a) ....., inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., doravante designado CONTRATADO, neste ato representado(a) por ..... (nome e função no contratado), conforme atos constitutivos da empresa **OU** procuração apresentada nos autos, tendo em vista o que consta no Processo nº 01420.102456/2023-20 e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico n. .../..., mediante as cláusulas e condições a seguir enunciadas.

### CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de solução de tecnologia da informação e comunicação de solução corporativa para proteção e blindagem e compliance de ativos com garantia, suporte e instalação para o período de 36 (trinta e seis) meses, podendo ser prorrogado até 60 (sessenta) meses, visando o atendimento das necessidades de garantir a segurança das informações bem como prover um serviço de qualidade para os usuários da FCP, nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

| ITEM | ESPECIFICAÇÃO | CATMAT | UNIDADE DE MEDIDA | QUANTIDADE | VALOR UNITÁRIO | VALOR TOTAL |
|---|---|---|---|---|---|---|
| 1 | Solução de software de segurança de estação de trabalho e servidores para 36 (trinta e seis) meses | 27499 | Unidade | 150 | R$ | R$ |
| 2 | Serviços de Instalação | 27022 | Unidade | 01 | R$ | R$ |
| 3 | Treinamento Técnico | 3840 | Unidade | 01 | R$ | R$ |
| | **TOTAL** | | | | | R$ |

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta do contratado;

1.3.4. Eventuais anexos dos documentos supracitados.

## CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 36 (trinta e seis) meses contados da assinatura do contrato, prorrogável para até 60 (sessenta) meses, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

2.1.1. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado.

2.1.2. O contratado não tem direito subjetivo à prorrogação contratual.

2.1.3. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.1.4. O contrato não poderá ser prorrogado quando o contratado tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

**CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS**

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

**CLÁUSULA QUARTA – SUBCONTRATAÇÃO**

4.1. Não será admitida a subcontratação do objeto contratual.

**CLÁUSULA QUINTA - PREÇO**

5.1. O valor mensal da contratação é de R$ ..... (.....), perfazendo o valor total de R$ ..... (....).

5.3. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

5.4. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

**CLÁUSULA SEXTA - PAGAMENTO**

6.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

**CLÁUSULA SÉTIMA - REAJUSTE**

7.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em __/__/__ (DD/MM/AAAA).

7.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI , mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade .

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

7.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

7.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

7.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s)

ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

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

7.8. O reajuste será realizado por apostilamento.

## CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE

8.1. São obrigações do Contratante, além das previstas no termo de referência :

8.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

8.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.1.3. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

8.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.1.5. Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.1.6. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.1.7. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

8.1.8. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

8.1.9. A Administração terá o prazo de 30 (trinta) dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.1.10. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 (trinta) dias.

8.1.11. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

8.2. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

## CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO

9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas, além das previstas no termo de referência :

9.1.1. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com

o Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

9.1.2. Comunicar ao contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

9.1.3. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133, de 2021) e prestar todo esclarecimento ou informação por eles solicitados;

9.1.4. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.1.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

9.1.6. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, junto com a Nota Fiscal para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

9.1.7. Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao contratante e não poderá onerar o objeto do contrato;

9.1.8. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual.

9.1.9. Paralisar, por determinação do contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

9.1.10. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

9.1.11. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116, da Lei n.º 14.133, de 2021);

9.1.12. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, da Lei n.º 14.133, de 2021);

9.1.13. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

9.1.14. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação,

exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021.

9.1.15. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do contratante;

9.1.16. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

9.1.17. Orientar e treinar seus empregados sobre os deveres previstos na Lei nº 13.709, de 14 de agosto de 2018, adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução deste contrato;

9.1.18. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina.

9.1.19. Submeter previamente, por escrito, ao contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

9.1.20. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

## CLÁUSULA DÉCIMA – OBRIGAÇÕES PERTINENTES À LGPD

10.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

10.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

10.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

10.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

10.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

10.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

10.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

10.10.1. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

10.11. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

10.12. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

## CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO

11.1. Não haverá exigência de garantia contratual da execução.

## CLÁUSULA DÉCIMA PRIMEIRA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

i. **Advertência**, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

ii. **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

iii. **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima deste Contrato, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

iv. **Multa:**

1. Moratória de 2% (dois por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 20 (vinte) dias;

2. moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.

i. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

3. Compensatória, para as infrações descritas nas alíneas “e” a “h” do subitem 12.1, de 15% a 25% do valor do Contrato.

4. Compensatória, para a inexecução total do contrato prevista na alínea “c” do subitem 12.1, de 10% a 20% do valor do Contrato.

5. Para infração descrita na alínea “b” do subitem 12.1, a multa será de 10% a 20% do valor do Contrato.

6. Para infrações descritas na alínea “d” do subitem 12.1, a multa será de 5% a 10% do valor do Contrato.

7. Para a infração descrita na alínea “a” do subitem 12.1, a multa será de 5% a 15% do valor do Contrato, ressalvadas as seguintes infrações:

12.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021)

12.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

12.4.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021)

12.4.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

12.4.3. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

12.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no **caput** e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de

inidoneidade para licitar ou contratar.

12.6. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para o Contratante;

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

12.7. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

12.8. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

12.9. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021).

12.10. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

12.11. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

## CLÁUSULA DÉCIMA SEGUNDA – DA EXTINÇÃO CONTRATUAL

13.3. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes .

13.3.1. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o Contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

13.3.2. A extinção nesta hipótese ocorrerá na próxima data de aniversário do

contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

13.3.3. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

13.4. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

13.4.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

13.4.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

13.4.2.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

13.5. O termo de extinção, sempre que possível, será precedido:

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

13.5.2. Relação dos pagamentos já efetuados e ainda devidos;

13.5.3. Indenizações e multas.

13.6. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, *caput*, da Lei n.º 14.133, de 2021).

13.7. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

## CLÁUSULA DÉCIMA TERCEIRA – DOTAÇÃO ORÇAMENTÁRIA

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:

I. Gestão/Unidade: : 344041/34208

II. Fonte de Recursos: : 100000000

III. Programa de Trabalho: : 0032 – Programa de Gestão e Manutenção do Poder Executivo

IV. Elemento de Despesa: 339040

V. Plano Interno: C20004PA024

VI. Nota de Empenho:

14.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

## CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS

15.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

**CLÁUSULA DÉCIMA QUINTA – ALTERAÇÕES**

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

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

16.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

16.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

**CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO**

17.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91,*caput*, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

**CLÁUSULA DÉCIMA SÉTIMA – FORO**

18.1. Fica eleito o Foro da Justiça Federal em ....., Seção Judiciária de..... para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

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

_____

Representante legal do CONTRATANTE

_____

Representante legal do CONTRATADO

TESTEMUNHAS:

1-

2-

# Termo de Referência 84/2023

## Informações Básicas

| Número do artefato | UASG | Editado por | Atualizado em |
|---|---|---|---|
| 84/2023 | 344041-MINC-FCP-FUNDACAO CULTURAL PALMARES/DF | CARLOS EDUARDO CARNEIRO E SOUSA | 04/12/2023 10:02 (v 1.1) |

**Status**

PUBLICADO

### Outras informações

| Categoria | Número da Contratação | Processo Administrativo |
|---|---|---|
| VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC | | 01420.102456/2023-20 |

## 1. Definição do objeto

#### 1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição de Solução corporativa para proteção e blindagem e compliance de ativos com garantia, suporte e instalação para o período de 36 (trinta e seis) meses, podendo ser prorrogado até 60 (sessenta), visando o atendimento das necessidades de garantir a segurança das informações bem como prover um serviço de qualidade para os usuários da FCP, conforme especificações e quantitativos apresentados neste documento, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

| ITEM | ESPECIFICAÇÃO | CATMAT | UNIDADE DE MEDIDA | QUANTIDADE | V A L O R UNITÁRIO | VALOR TOTAL |
|---|---|---|---|---|---|---|
| 1 | Solução de software de segurança de estação de trabalho e servidores para 36 meses | 27499 | Unidade | 150 | R$ 2.052,50 | R$ 307.875,00 |
| 2 | Serviços de Instalação | 27022 | Unidade | 01 | R$ 53.000,00 | R$ 53.000,00 |
| 3 | Treinamento Técnico | 3840 | Unidade | 01 | R$ 38.000,00 | R$ 38.000,00 |
| TOTAL | | | | | | R$ 398.875,00 |

1.2. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

1.3. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

1.6. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

1.7 A presente contratação se enquadra na categoria de bens e serviços comuns, de que trata a Lei nº 10.520, de 17 de julho de 2002, e o Decreto nº 5.450, de 31 de maio de 2005, por possuírem padrões de desempenho e características gerais e específicas usualmente encontradas no mercado.

1.8 A presente contratação adotará como regime de execução a Empreitada por Preço Unitário.

1.9 O prazo de vigência do contrato é de 36(trinta e seis) meses, podendo ser prorrogado por interesse das partes até 60(sessenta) meses.

# 2. Fundamentação da contratação

**2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO**

2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em Tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência

2.4 A solução de Antivírus não foi relacionada ao PAC2023, tornou-se prioridade na Fundação, ao notar-se que o atual contrato vencerá em dezembro de 2023. Com isso foi solicitado um ajuste para o período de 2023, conforme o Art. 16 do DECRETO Nº 10.947, DE 25 DE JANEIRO DE 2022.

2.5 A solução tornou-se prioridade para a COPTI considerando o cenário de constante risco de invasões se torna necessário o investimento na solução de Antivírus.

2.6 Além disso, houve uma economia significativa no processo de Antispam 01420.100481/2023-79, visto que a contratação não será mais necessária por conta da pretendida migração do Serviço de e-mail da Fundação Palmares para o serviço de nuvem.

# 3. Descrição da solução

**3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO**

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares.

3.2 A pretensão contratação de Solução Segurança Avançada para Endpoints, com proteção integrada contra-ataques complexos, direcionados e descoberta avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a
incidentes com instalação, configuração, treinamento, serviços de consultoria e suporte técnico em sistemas de segurança na solução fornecida para prevenção zero day.

3.3 Com a Lei em vigor da LGPD – Lei Geral de Proteção de Dados, datada de 1 de janeiro de 2021 e cientes ainda que a perda de dados contendo informações pessoais de servidores e cidadãos, titulares de dados, podem trazer prejuízos à FCP, entendemos indispensável a aquisição de uma Solução de Segurança robusta corporativa de estações de trabalho, servidores e conectividade segura e eficaz , a fim de contribuir com o alcance dos objetivos estratégicos.

3.4 As instituições e organizações devem proteger seus dados contra qualquer vazamento de dados que possa surgir de ameaças internas ou externas proteção para todos os setores e deve ser aplicado a todos os dispositivos e servidores que se conectam a sistemas corporativos ou manipulam dados. A legislação e os padrões institucionais (LGPD, GDPR etc.) acionam essa necessidade.

3.5 Dessa forma, a solução será composta de produtos e serviços que contenham no mínimo as seguintes funcionalidades:
a) Gerenciamento centralizado;
b) Facilidade e flexibilidade no redirecionamento do tráfego entre os circuitos de comunicação conectados à solução;
c) Possibilidade de redução de riscos de indisponibilidade do serviço de comunicação de dados voz e vídeo entre núcleos, entre os núcleos, representações e a sede da Fundação Cultural Palmares;

# 4. Requisitos da contratação

**4. REQUISITOS DA CONTRATAÇÃO**

4.24 Os Requisitos para a presente contratação estão descritos detalhadamente em tópico a seguir:

**4.24.1 Requisitos de Negócio:**

a) Garantir a disponibilidade e continuidade dos serviços de TI;

b) Garantir a proteção das informações;

c) Garantir a infraestrutura e os recursos tecnológicos adequados às atividades da Fundação Cultural Palmares;

d) Criar uma política de detecção de conteúdo para sistema ou serviço de TI em caso de falha ou em caso de ataque cibernético à rede de tecnologia da Fundação Cultural Palmares.

e) Automatização da descoberta de incidentes.

**4.24.2 Requisitos de Capacitação**

a) A Contratada deverá realizar o repasse de conhecimento aos funcionários da contratante que atuarão, diretamente, com a solução de segurança e conectividade adquirida, abrangendo todas as informações necessárias a sua operacionalização, disponibilizando materiais em mídias digitais, apostilas e outros recursos em português brasileiro.

**4.24.3 Requisitos de Manutenção**

a) O Suporte deverá ser especializado, podendo ser executado remotamente ou localmente dependendo da criticidade. A avaliação do chamado quanto a criticidade será feita pela FCP;

b) A documentação produzida durante a execução dos serviços, seja em papel ou meio eletrônico, será de propriedade da FCP, e não deverá ser divulgado sem sua expressa autorização.

**4.24.4 Requisitos de Segurança**

a) A solução que será implantada deve atender as recomendações da Política de Segurança da Informação e demais normativos da FCP.

**4.24.5 Requisitos Legais**

a) A presente contratação sujeita-se à legislação pertinente, mormente aos diplomas a seguir elencados, bem como às demais normas gerais que se apliquem, considerando-se a legislação consolidada com as respectivas alterações subsequentes:

- Lei nº 9.609, de 19 de fevereiro de 1998:

Art. 12. Violar direitos de autor de programa de computador:

Pena - Detenção de seis meses a dois anos ou multa.

§ 1º Se a violação consistir na reprodução, por qualquer meio de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena - Reclusão de um a quatro anos e multa.

§ 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

§ 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:

I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa público, sociedade de economia mista ou fundação instituída pelo poder público;

II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.

§ 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

- Lei nº 9.610, de 19 de fevereiro de 1998:

- Art. 102. O titular cuja obra seja fraudulentamente reproduzida, divulgada ou de qualquer forma utilizada, poderá requerer a apreensão dos exemplares reproduzidos ou a suspensão da divulgação, sem prejuízo da indenização cabível.

- Lei Nº 14.133, de 1º de Abril de 2021 - Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;

- Lei Federal n° 12.813/2013: dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego;

- Lei Federal nº 12.846/2013: dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências;

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

- Decreto n° 9.507, de 21 de setembro de 2018 - Dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;

- Instrução Normativa SEGES/ME Nº 65, DE 7 de Julho de 2021.

- Aplicação subsidiária da Instrução Normativa nº 5, de 26 de maio de 2017 – Dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública Federal Direta, Autárquica e Fundacional;

- Aplicação da Instrução Normativa GSIPR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal e suas Normas Complementares, em especial a Norma Complementar Nº 14/IN01/DSIC/GSIPR, de 19 de março de 2018, que estabelece princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem;

- Aplicação da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados

**4.24.6 Requisitos Temporais**

a) O prazo de vigência do contrato é de 36 (trinta e seis) meses, podendo ser prorrogado por interesse das partes até o limite de 60 (sessenta) meses, com base no artigo 105, da Lei 14.133, de 2021, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos:

- Os serviços tenham sido prestados regularmente;

- A Administração mantenha interesse na realização do serviço;

- O valor do contrato permaneça economicamente vantajoso para a Administração;

- A CONTRATADA manifeste expressamente interesse na prorrogação.

- A reunião inicial de alinhamento deverá ocorrer após a assinatura do contrato e ser executada em, no máximo, 5 (cinco) dias corridos após a assinatura do contrato.

- O prazo de entrega para os documentos que comprovem o fornecimento do licenciamento e todas as demais obrigações deverão ser disponibilizadas à CONTRATANTE no prazo máximo de 30 (trinta) dias corridos a serem contados a partir da abertura da Ordem de Fornecimento de bens/Serviço.

**4.24.7 Requisitos de Projetos e de Implementação**

a) Na reunião inicial a contratada deverá apresentar o projeto de implementação das licenças, fornecimento de equipamentos e da prestação dos serviços de manutenção/suporte.

b) O projeto deverá contemplar a instalação das versões dos softwares nas versões mais estáveis e que mitiguem os riscos de vulnerabilidades das estações de trabalho de usuários e servidores de rede. Todos os custos referentes aos softwares que forem alocados em NUVEM, devem ser mantidos pela CONTRATADA, tais como consoles e servidores.

**4.24.8 Requisitos de Garantia e de Manutenção**

a) Contratada deverá fornecer garantia da solução pelo prazo de 36 (trinta e seis) meses, contados a partir da data da emissão do Termo de Recebimento, não se limitando ao término da vigência contratual.

b) A garantia deverá prover, obrigatoriamente:

- Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;

- Atualização dos softwares fornecidos, se houver lançamento de novos softwares em substituição aos fornecidos, ou se, mesmo não se tratando de substituição, ficar caracterizada descontinuidade dos softwares fornecidos;

- Correções dos softwares fornecidos (patches), incluindo a correção de eventuais falhas (bugs) de software que prejudiquem o ambiente de produção ou vulnerabilidades que comprometam a segurança da solução;

c) A garantia deverá ser prestada durante todo o período de contrato e aditivos relativos às atualizações das licenças e proteção. Garantia para hardware durante o período do contrato;

d) Atualização do sistema operacional embarcado durante o período do contrato.

e) No preço deverá estar incluído todo o software necessário para atender as características exigidas, bem como as atualizações para todas as versões do produto que forem lançadas durante o período do contrato.

f) Os chamados de manutenção e suporte técnico deverão ser registrados em sistema provido pela CONTRATADA, e deverão estar disponíveis para acompanhamento em seu portal na internet.

g) A Contratada deve escalar o chamado para o suporte do fabricante sempre que necessário, seja devido à criticidade, impacto ou urgência do problema, como também caso o fabricante precise atuar no processo de correção.

h) Será disponibilizado canal de atendimento e chamado técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de site na Internet e/ou canal telefônico gratuito 0800;

i) Em caso de indisponibilidade do canal de atendimento disponibilizado, os chamados técnicos poderão ser abertos via e-mail, "website" do fabricante, telefone etc.;

j) O fornecedor deve informar página da Internet onde estejam disponíveis drivers atualizados, últimas versões do firmware e demais informações sobre detalhes técnicos dos equipamentos e/ou softwares, sem restrições de acesso público ou via cadastramento de pessoas autorizadas pelo CONTRATANTE para o acesso.

**4.24.9 Requisitos de Segurança**

a) A CONTRATADA deverá submeter-se à Política de Segurança da Informação e Comunicações e demais normas de segurança vigentes na CONTRATANTE.

b) Quanto ao acesso físico, a CONTRATADA:

c) Deverá credenciar junto à CONTRATANTE os seus profissionais, caso seja necessário o acesso às instalações da Sede da CONTRATANTE para prestação de serviços.

d) A CONTRATADA deverá apresentar os empregados devidamente uniformizados e identificados por meio de crachá.

e) Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca dos serviços, sem prévia autorização.

f) Observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação - TI da CONTRATANTE.

g) Será considerado ilícito a divulgação, o repasse ou utilização indevida de informações, bem como dos documentos, imagens, gravações e informações utilizados durante a prestação dos serviços.

h) Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer reprodução, utilização ou divulgação a terceiros, devendo a CONTRATADA zelar por si e por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados.

**4.24.10 Requisitos de Experiência Profissional e de Formação da Equipe**

a) A contratada deverá comprovar que possui em seu quadro permanente, profissional de nível superior ou outro devidamente reconhecido pela entidade competente, detentor de atestado de responsabilidade técnica por execução de serviço de características semelhantes com o objeto da contratação.

b) Requisitos de Metodologia de Trabalho O serviço de instalação deverá ser executado e supervisionado por pelo menos 1 (um) técnico certificado pelo fabricante da solução proposta.

c) A CONTRATADA deverá instalar os softwares e hardwares, com as licenças adquiridas.

d) Na reunião inicial, que marca o período de execução do contrato, deverá ser acordado entre a CONTRATANTE e a CONTRATADA os dias em que o engenheiro do fabricante realizará as tarefas prevista neste documento.

e) O preposto será responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto à CONTRATANTE.

f) Os equipamentos serão considerados recebidos de forma definitiva quando instalados nos respectivos ambientes, cabeados, configurados, operacionais, em plenas condições de funcionamento, integrados com a rede local e licenciados, bem como com outros equipamentos locais utilizados e com capacidade de permitir acesso remoto por parte da equipe da CONTRATANTE.

**4.24.11 Requisitos Sociais, Ambientais e Culturais**

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

b) Os profissionais da CONTRATADA que porventura desempenharem atividades em contato direto com a CONTRATANTE deverão:

c) Apresentar-se vestidos de forma adequada ao ambiente de trabalho físico ou virtual, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional da CONTRATANTE ou que ofenda o senso comum de moral e bons costumes;

d) Respeitar todos os servidores, funcionários e colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo;

e) Atuar no estabelecimento da CONTRATANTE com urbanidade e cortesia.

f) Não aplicação da Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010 - que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional pelo fato de ser tratar de contratação de licenças de software e de serviços especializados.

**4.24.12 Requisitos de Garantia, Manutenção e Assistência Técnica**

a) O prazo de garantia contratual dos bens, complementar à garantia legal, será de, no mínimo, 36 (trinta e seis) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

**4.24.13 Demais requisitos necessários e suficientes à escolha da solução de TIC**

| Demais requisitos necessários e suficientes à escolha da solução de TIC | |
|---|---|
| 1 | **Possuir alta disponibilidade**. É um sistema resistente a falhas de hardware e software, cujo objetivo é man serviços disponibilizados o máximo de tempo possível. |
| 2 | **Possuir escalabilidade**. É a característica que indica a capacidade de crescer atendendo às demandas sem p as qualidades que lhe agregam valor |
| 3 | **Possuir confiabilidade**. É a capacidade do sistema de realizar e manter seu funcionamento em circunstânci rotina, bem como em circunstâncias hostis e inesperadas |
| 4 | **Desempenho**. É a performance esperada em um sistema de computação para respostas de seus sistemas. |
| 5 | **Gerenciamento centralizado**. É a possibilidade de gerenciar todos os softwares de forma centrali possibilitando um maior controle do ambiente. |

# 5. Modelo de execução do objeto

**5. MODELO DE EXECUÇÃO DO OBJETO**

**Condições de Entrega**

5.1. A execução do objeto seguirá a seguinte dinâmica:
5.1.1. O prazo de execução deverá ser previsto para cada etapa.;
5.1.2. O local da entrega do objeto deverão ser prestados no endereço: SCRN 702/703 – Bloco B – Asa Norte - CEP 70.720-620 / Brasília – DF.
5.1.3. O horário de funcionamento será de segunda à sexta-feira das 08 as 12 horas e das 14 ás 18 horas

**Garantia, manutenção e assistência técnica**

5.1. *O prazo de garantia contratual dos bens, complementar à garantia legal, será de, no mínimo, 36(trinta e seis) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.*

# 6. Modelo de gestão do contrato

**6. MODELO DE GESTÃO DO CONTRATO**

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

6.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

6.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros

**Fiscalização**

6.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

**Fiscalização Técnica**

6.7. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

6.7.1. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

6.7.2. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

6.7.3. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

6.7.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).

6.7.5. O fiscal técnico do contrato comunicar ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

**Fiscalização Administrativa**

6.8. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

6.8.1. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

**Gestor do Contrato**

6.10. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. ( Decreto nº 11.246, de 2022, art. 21, IV).

6.11. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

6.12. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

6.13. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

6.14. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

6.15. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

6.16. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

**Critérios de Aceitação**

6.17 A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

a) Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não recondicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).

b) Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.

c) Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

d) O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.

e) Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

f) Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.

g) Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões “shareware” ou “trial”. O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.

h) A Contratante poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou uma amostra dos equipamentos, atentando para a inclusão nos autos do processo administrativo de todos os documentos que evidenciem a realização dos testes de aceitação em cada equipamento selecionado, para posterior rastreabilidade.

i) Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

j) Procedimentos de Teste e Inspeção

6.18 Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

6.19 A critério da CONTRATANTE, testes poderão ser realizados a fim de comprovar as funcionalidades e a especificação proposta neste TR

Níveis Mínimos de Serviço Exigidos

**Níveis Mínimos de Serviço Exigidos**

6.20 As tabelas a seguir apresentam os indicadores de nível de serviço - Instrumento de Medição de Resultado (IMR)

| ***Indicador 01: Indicador de Atraso de Entrega (IAE)*** | |
|---|---|
| *Item* | *Descrição* |
| *Finalidade* | *Medir o tempo de atraso na prestação de serviços constantes na Ordem de Serviço.* |
| *Meta a cumprir* | *IAE < = 0. A meta definida visa garantir a entrega das Licenças e serviços constantes as Ordens de Serviço dentro do prazo previsto.* |
| *Instrumento de medição* | *Por controle próprio da Contratante e lista de Termos de Recebimento Provisório e emitidos comparados com a data da emissão da OS.* |
| *Forma de Acompanhamento* | *A avaliação será feita conforme linha de base do cronograma registrada na OS. Será s data de entrega dos produtos da OS (desde que o fiscal técnico reconheça aquela registro em Termo de Recebimento Provisório) pela data de início da execução da OS.* |
| *Periodicidade* | *De acordo com cada OS encerrada e com seu respectivo Termo de Recebimento emitido.* |
| *Mecanismo de Cálculo* | *IAE = TExec – TEst TEst*<br><br>*Onde:*<br><br>*IAE – Indicador de Atraso de Entrega da OS;*<br><br>*TExec – Tempo de Execução – corresponde ao período de execução da OS, da su início até a data de entrega dos produtos da OS. A data de início será aquela constan caso não esteja explícita, será o primeiro dia útil após a emissão da OS.*<br><br>*A data de entrega da OS deverá ser aquela reconhecida pelo fiscal técnico, conform constantes no Termo de Referência. Para os casos em que o fiscal técnico rejeita a prazo de execução da OS continua a correr, findando-se apenas quando a Contratad as Licenças ou Serviço de Migração da OS e haja aceitação por parte do fiscal técnico.*<br><br>*TEst – Tempo Estimado para a execução da OS – constante na OS, conforme esti Termo de Referência* |
| *Início de Vigência* | *A partir da emissão da OS* |
| *Glosas* | *Para valores do indicador IAE:*<br><br>*De 0 a 0,10 – Pagamento integral da OS;*<br><br>*De 0,11 a 0,20 – Glosa de 0,5% sobre o valor da OS;*<br><br>*De 0,21 a 0,30 – Glosa de 1,0% sobre o valor da OS;*<br><br>*De 0,31 a 0,50 – Glosa de 5,0% sobre o valor da OS;* |

| | |
|---|---|
| | *De 0,51 a 1,00 – Glosa de 10% sobre o valor da OS;*<br><br>*Acima de 1 – Será aplicada Glosa de 12,5% sobre o valor da OS e Sanções Admi conforme previsão nesse Termo de Referência* |
| *Sanções* | *Conforme Tabela das Sanções Administrativas desse Termo de Referência.* |

| *Indicador 02: Suporte Atendido Dentro do Prazo (SADP)* | |
|---|---|
| *Item* | *Descrição* |
| *Finalidade* | *Assegurar que os chamados estejam dentro do prazo de início e fim de atendimento* |
| *Meta a cumprir* | *90% dos chamados dentro do prazo de início e fim de atendimento* |
| *Instrumento de medição* | *Registro/Resposta de cada solicitação de suporte técnico* |
| *Forma de Acompanhamento* | *Cálculo do prazo de Registro/Resposta de cada solicitação de suporte técnico em r Nível de Serviço* |
| *Periodicidade* | *Mensal* |
| *Mecanismo de Cálculo* | *Nº Chamados em atraso/ Nº de Chamados abertos no mês* |
| *Início de Vigência* | *Após 1 (um) dia útil da emissão do Termo de Recebimento Definitivo* |
| *Sanções* | *Conforme Tabela das Sanções Administrativas desse Termo de Referência.* |

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

6.21 Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

| ***Id*** | ***Ocorrência*** | ***Glosa / Sanção*** |
|---|---|---|
| *1* | *Não comparecer injustificadamente à Reunião Inicial.* | *Advertência.*<br><br>*Em caso de reincidência, multa 0,5% sobre o valor Contrato.* |
| | *Ter praticado atos ilícitos visando frustrar os objetivos da* | *A Contratada será declarada inidônea para licitar e contr a Administração.* |

| | | |
|---|---|---|
| *2* | *licitação.* | |
| *3* | *Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 48 (quarenta e oito) horas úteis.* | *Multa de 0,1% sobre o valor total do Contrato por dia útil d em prestar as informações por escrito, ou por outro meio autorizado pela Contratante, até o limite de 10 dias úteis.* |
| | | *Após o limite de 10 dias úteis, aplicar-se-á multa de 1 % total do Contrato.* |
| *4* | *Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega de OS)* | *Glosa de 0,1 % sobre o valor da OS para valores do indic de 0,11 a 0,20.* |
| | | *Glosa de 0,2 % sobre o valor da OS para valores do indic de 0,21 a 0,30.* |
| | | *Glosa de 0,3 % sobre o valor da OS para valores do indic de 0,31 a 0,50.* |
| | | *Glosa de 0,4 % sobre o valor da OS para valores do indic de 0,51 a 1,00.* |
| | | *Multa de 0,5 sobre o valor do Contrato e Glosa de 1% valor da OS, para valores do indicador IAE maiores que 1,0* |
| *5…* | *Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da contratante.* | *A Contratada será declarada inidônea para licitar ou contr a Administração Pública, sem prejuízo às penalidades dec da inexecução total ou parcial do contrato, o que poderá a a rescisão do Contrato, sem prejuízo das demais penalidad previstas na Lei nº14.133 de 2021.* |
| *6* | *Não cumprir qualquer outra obrigação contratual não citada nesta tabela.* | *Advertência.*<br>*Em caso de reincidência ou configurado prejuízo aos re pretendidos com a contratação, aplica-se multa de 3% total do Contrato.* |
| *7* | *Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.* | *A Contratada será declarada inidônea para licitar ou contr a Administração Pública, sem prejuízo às penalidades dec da inexecução total ou parcial do contrato, o que poderá a a rescisão do Contrato, sem prejuízo das demais penalidad previstas na Lei nº14.133 de 2021.* |

6.22 Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o Contratado:

6.22.1 Não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

6.22.2 Deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

# 7. Critérios de medição e pagamento

**7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO**

**Recebimento**

7.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

7.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 30 dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.3. O recebimento definitivo ocorrerá no prazo de 30(trinta) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

7.4. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até 7(sete) dias úteis.

7.5. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

7.6. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.7. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

7.8. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

**Liquidação**

7.9. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

7.9.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

7.10. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

7.10.1. o prazo de validade;

7.10.2. a data da emissão;

7.10.3. os dados do contrato e do órgão contratante;

7.10.4. o período respectivo de execução do contrato;

7.10.5. o valor a pagar; e

7.10.6. eventual destaque do valor de retenções tributárias cabíveis.

7.11. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

7.12. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

7.13. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

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

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

7.16. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

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

**Prazo de pagamento**

7.18. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

7.19. No caso de atraso pelo CONTRATANTE, os valores devidos ao CONTRATADO serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do Índice Nacional de Preços ao Consumidor Amplo (IPCA) de correção monetária

**Forma de pagamento**

7.20. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

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

7.22.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

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

**Cessão de crédito**

7.33. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.

7.33.1. *As cessões de crédito não fiduciárias dependerão de prévia aprovação do contratante.*

7.34. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

7.35. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, tudo nos termos do Parecer JL-01, de 18 de maio de 2020.

7.36. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração. (INSTRUÇÃO NORMATIVA Nº 53, DE 8 DE JULHO DE 2020 e Anexos)

7.37. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do contratado.

# 8. Critérios de seleção do fornecedor

**8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR**

**Forma de seleção e critério de julgamento da proposta**

8.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço.

8.2 O regime de execução do contrato será por EMPREITADA POR PREÇO UNITÁRIO.
8.3 O tipo e critério de julgamento da licitação é o MENOR PREÇO DO GRUPO/LOTE para a seleção da proposta mais vantajosa.
**Da Aplicação da Margem de Preferência**
Não será aplicada margem de preferência na presente contratação

**Exigências de habilitação**

8.4 Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

**Habilitação jurídica**

8.5 **Pessoa física**: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

8.6 **Empresário individual**: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

8.7 **Microempreendedor Individual - MEI**: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

8.8. **Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI**: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

8.9 **Sociedade empresária estrangeira**: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

8.10 **Sociedade simples**: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

8.11. **Filial, sucursal ou agência de sociedade simples ou empresária**: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

8.12 **Sociedade cooperativa**: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

8.16. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

**Habilitação fiscal, social e trabalhista**

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

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

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

8.20. 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;

8.21. Prova de inscrição no cadastro de contribuintes *[Estadual/Distrital] ou [Municipal/Distrital]* relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.22. Prova de regularidade com a Fazenda [Estadual/Distrital] ou [Municipal/Distrital] do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

8.23. Caso o fornecedor seja considerado isento dos tributos *[Estadual/Distrital] ou [Municipal/Distrital]* relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

8.24. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

**Qualificação Econômico-Financeira**

8.25 Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

8.26. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

8.27 Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando;

8.27.1. índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

8.27.2. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

8.27.3. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

8.27.4. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

8.28. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação capital mínimo de até 10% do valor total estimado da contratação.

8.29. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

8.30. *O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.*

**Qualificação Técnica**

8.31 A LICITANTE deverá apresentar Atestado(s) ou Certidão(ões) de Capacidade Técnico operacional, emitido(s) por pessoa jurídica de direito público ou privado, comprovando que a licitante forneceu, instalou e configurou solução de gateway de segurança de e-mails, compatíveis em características com os itens ofertados, objeto deste Termo de Referência.

(Base Legal: Cap. VI da Lei nº. 14.133/2021; IN 05/2017/MPOG; Art. 4º da Orientação Técnica nº. 001/2017/GAB /SUPEL):
Art. 3º Os Termos de Referência, Projetos Básicos e Editais relativos à aquisição de bens e materiais de consumo comuns, considerando o valor estimado da contratação, devem observar o seguinte:
I – até 80.000,00 (oitenta mil reais) - fica dispensada a apresentação de Atestado de Capacidade Técnica;
II - de 80.000,00 (oitenta mil reais) a 650.000,00 (seiscentos e cinquenta mil reais) - apresentar Atestado de Capacidade Técnica que comprove ter fornecido anteriormente materiais compatíveis em características;
III – acima de 650.000,00 (seiscentos e cinquenta mil reais) – apresentar Atestado de Capacidade Técnica compatível em características e quantidades, limitados a parcela de maior relevância e valor significativo;"
Parágrafo único. Não se aplica a regra do inc. I, aplicando-se a regra do inc. II deste artigo, quando tratar da aquisição de bens e materiais de natureza mais complexas tais como equipamentos médicos, odontológicos, de segurança, eletrônicos, computacionais.
8.32 Considerando os valores da aquisição, PARA O (s) ITEM (ns): às empresas deverão apresentar Atestado de Capacidade Técnica compatível em características.
8.33 O atestado deverá indicar dados da entidade emissora (razão social, CNPJ, endereço, telefone, fax, data de emissão) e dos signatários do documento (nome, função, telefone, etc.), além da descrição do objeto e quantidade expressa em unidade.
8.34 Na ausência dos dados indicados, antecipa-se a diligência prevista no artigo 64 da Lei Federal nº. 14.133/2021 para que sejam encaminhados em conjunto os documentos comprobatórios de atendimentos, quais sejam cópias de contratos, notas de empenho, acompanhados de editais de licitação, dentre outros. Caso não sejam encaminhados, o Pregoeiro os solicitará no decorrer do certame para certificar a veracidade das informações e atendimento da finalidade do Atestado.

# 9. Estimativas do Valor da Contratação

**Valor (R$):** 398.875,00

**9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO**

9.1. O valor estimado da contratação para 36 (trinta e seis) meses é de trezentos e noventa e oito mil e oitocentos e setenta e cinco reais.

9.2. O custo estimado da contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas.

# 10. Adequação orçamentária

**10. ADEQUAÇÃO ORÇAMENTÁRIA**

10.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

10.2. A contratação será atendida pela seguinte dotação:

I) Gestão/Unidade: 344041/34208

II) Fonte de Recursos: 100000000

III) Programa de Trabalho: 0032 – Programa de Gestão e Manutenção do Poder Executivo

IV) Elemento de Despesa: 339040

V) Plano Interno: C20004PA024

VI) Ação: 2000 – Administração da Unidade

# 11. Responsabilidades

**12. RESPONSABILIDADES**

**12.1. Deveres e responsabilidades da CONTRATANTE**

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

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

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

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

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

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

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

12.1.8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

12.2 **Deveres e responsabilidades da CONTRATADA**

12.2.1. Indicar formalmente e por escrito, no prazo máximo de 10 dias úteis após a assinatura do contrato, junto à contratante, um preposto idôneo com poderes de decisão para representar a contratada, principalmente no tocante à eficiência e agilidade da execução do objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato;

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

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

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

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

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

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

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

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

12.2.10. Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da contratante;

12.2.11. Não fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão;

12.2.12. <Outras obrigações que se apliquem, de acordo com o objeto da contratação, observando, no que couber, as “Ações de Responsabilidade da Contratada”, constantes no “Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade”. Guia disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaRequisitosdeSIparaContratacoesdeTI.pdf)>.

## 12. Da vigência do contrato

O contrato vigorará por 36 (trinta e seis) meses, contados a partir da data da sua assinatura, podendo ser prorrogado até 60 (sessenta) meses.

## 11. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

**IVANILDO FELICIANO DA SILVA**

Coordenador de Projeto de T.I

*Assinou eletronicamente em 01/12/2023 às 09:53:18.*

# Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - ANEXO I - TERMO DE RECEBIMENTO PROVISÓRIO.pdf (171.41 KB)
- Anexo II - ANEXO II - TERMO DE RECEBIMENTO DEFINITIVO.pdf (193.82 KB)
- Anexo III - ANEXO III - TERMO DE COMPROMISSO E SIGILO DE DADOS E INFORMAÇÕES.pdf (233.17 KB)
- Anexo IV - ANEXO IV - TERMO DE CI_NCIA DA DECLARAÇÃO DE MANUTENÇÃO DE SIGILO.pdf (144.94 KB)
- Anexo V - ANEXO V - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE TIC.pdf (172.38 KB)
- Anexo VI - ANEXO VI - ESTUDO TÉCNICO PRELIMINAR.pdf (376.07 KB)

# Anexo I - ANEXO I - TERMO DE RECEBIMENTO PROVISÓRIO.pdf

**FUNDAÇÃO CULTURAL PALMARES - FCP**

# TERMO DE RECEBIMENTO PROVISÓRIO – COMPRAS DE TIC

## Histórico de Revisões

| Data | Versão | Descrição | Autor |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

| INTRODUÇÃO |
|---|
| O Termo de Recebimento Provisório declarará, de forma sumária, que as compras foram entregues, para verificação posterior da conformidade do material com as exigências contratuais, baseada nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato.<br><br>**Referência: Inciso XXI, art. 2º, e alínea "i", inciso II, art. 33 da IN SGD/ME Nº 94/2022.** |

| 1 – IDENTIFICAÇÃO | | | |
|---|---|---|---|
| **CONTRATO/NOTA DE EMPENHO Nº** | | | |
| **CONTRATADA** | | **CNPJ** | |
| **Nº DA OFB** | | | |
| **DATA DA EMISSÃO** | | | |

| 2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S) E VOLUMES DE EXECUÇÃO | | | |
|---|---|---|---|
| **SOLUÇÃO DE TIC** | | | |
| | | | |
| **ITEM** | **DESCRIÇÃO DO BEM OU SERVIÇO** | **MÉTRICA** | **QUANTIDADE** |
| 1 | | | |
| | | | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| **TOTAL DE ITENS** | | | |

## 3 – RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea "i", da IN SGD/ME nº 94/2022, por este instrumento ATESTO que os produtos correspondentes à Nota Nº ____ acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram entregues, estando sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo destes produtos ocorrerá somente após a verificação desses requisitos e das demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

## 4 – ASSINATURA

**FISCAL TÉCNICO**

_____
<Nome do Fiscal Técnico do Contrato>
**Matrícula:** xxxxxx

<Local>, <dia> de <mês> de <ano>.

**PREPOSTO**

_____
<Nome do Preposto do Contrato>
**Matrícula**: xxxxxx

**FUNDAÇÃO CULTURAL PALMARES - FCP**

<Local>, <dia> de <mês> de <ano>.

# Anexo II - ANEXO II - TERMO DE RECEBIMENTO DEFINITIVO.pdf

**FUNDAÇÃO CULTURAL PALMARES - FCP**

# TERMO DE RECEBIMENTO DEFINITIVO
## Histórico de Revisões

| Data | Versão | Descrição | Autor |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

| **INTRODUÇÃO** |
|---|
| O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem às exigências contratuais, de acordo com os requisitos e critérios de aceitação estabelelcidos.<br><br>**Referência: Inciso XXII, Art. 2º e alínea "h" inciso I do art. 33, da IN SGD/ME Nº 94/2022.** |

| **1 – IDENTIFICAÇÃO** | | | |
|---|---|---|---|
| **CONTRATO/NOTA DE EMPENHO Nº** | | | |
| **CONTRATADA** | | **CNPJ** | |
| **Nº DA OS/OFB** | | | |
| **DATA DA EMISSÃO** | | | |

| **2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S)/SERVIÇOS E VOLUMES DE EXECUÇÃO** | | | | |
|---|---|---|---|---|
| **SOLUÇÃO DE TIC** | | | | |
| | | | | |
| **ITEM** | **DESCRIÇÃO DO BEM OU SERVIÇO** | **MÉTRICA** | **QUANTIDADE** | **TOTAL** |
| 1 | | | | |
| | | | | |
| | | | | |

**FUNDAÇÃO CULTURAL PALMARES - FCP**

| TOTAL DE ITENS | |
|---|---|

## 3 – ATESTE DE RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea "h", da IN SGD/ME nº 94/2022, por este instrumento atesto que o(s) bens correspondentes à _____ acima identificada foram entregues pela **CONTRATADA** e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato acima indicado.

| ITEM | EXIGÊNCIA CONTRATUAL | ATENDIMENTO | OBSERVAÇÃO |
|---|---|---|---|
| 1 | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

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

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

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

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

## 5 – ASSINATURA

**GESTOR DO CONTRATO**

_____

<Nome do Gestor do Contrato>
**Matrícula:** xxxxxxxx

**FUNDAÇÃO CULTURAL PALMARES - FCP**

<Local>, <dia> de <mês> de <ano>.

<As seções seguintes podem constar em documento diverso, pois dizem respeito à autorização para o faturamento, a cargo do Gestor do Contrato, e a respectiva ciência do preposto quanto a esta autorização>.

**5 – AUTORIZAÇÃO PARA FATURAMENTO**

**GESTOR DO CONTRATO**

Nos termos da alínea "n", inciso I, art. 33, da IN SGD/ME nº 94/2022, AUTORIZA-SE a **CONTRATADA** a <faturar os serviços executados / apresentar as notas fiscais dos bens entregues> relativos à supracitada <OS/OFB>, no valor discriminado no item 4, acima.

_____

<Nome do Gestor do Contrato>
**Matrícula:** xxxxxxxx

<Local>, <dia> de <mês> de <ano>

**7 – CIÊNCIA**

**PREPOSTO**

_____

<Nome do Preposto do Contrato>
**Matrícula**: xxxxxxx

<Local>, <dia> de <mês> de <ano>

# Anexo III - ANEXO III - TERMO DE COMPROMISSO E SIGILO DE DADOS E INFORMAÇÕES.pdf

**FUNDAÇÃO CULTURAL PALMARES - FCP**

# TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO
## Histórico de Revisões

| Data | Versão | Descrição | Autor |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

## INTRODUÇÃO

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

**Referência: Art. 18, Inciso V, alínea "a" da IN SGD/ME Nº 94/2022.**

Pelo presente instrumento o <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ n° <Nº do CNPJ>, doravante denominado **CONTRATANTE**, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n° <Nº do CNPJ>, doravante denominada **CONTRATADA**;

CONSIDERANDO que, em razão do **CONTRATO N.º <nº do contrato>** doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da **CONTRATANTE**;

Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO,** doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

## 1 – OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos

necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

[...]

[...]

[...]

## 2 – CONCEITOS E DEFINIÇÕES

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

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

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

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

[...]

[...]

[...]

## 3 – DA INFORMAÇÃO SIGILOSA

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

[...]

[...]

[...]

## 4 – DOS LIMITES DO SIGILO

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

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

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

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

[...]

[...]

[...]

## 5 – DIREITOS E OBRIGAÇÕES

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

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

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

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

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

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

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

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

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

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

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

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

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

[...]

[...]

[...]

## 6 – VIGÊNCIA

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

[...]

## 7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme previsto nos arts. 155 a 163 da Lei nº. 14.133, de 2021.

[...]

[...]

[...]

## 8 – DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

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

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

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

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

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

[...]

[...]

[...]

## 9 – FORO

A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE>, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

[...]

## 10 – ASSINATURAS

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

| **CONTRATADA** | **CONTRATANTE** |
|---|---|
| _____<br><Nome><br><Qualificação> | _____<br><Nome><br>**Matrícula:** xxxxxxxx |
| **TESTEMUNHAS** | |

**FUNDAÇÃO CULTURAL PALMARES - FCP**

| | |
|---|---|
| _____<br><Nome><br><Qualificação> | _____<br><Nome><br><Qualificação> |

<Local>, <dia> de <mês> de <ano>.

# Anexo IV - ANEXO IV - TERMO DE CI_NCIA DA DECLARAÇÃO DE MANUTENÇÃO DE SIGILO.pdf

**ANEXO IV - TERMO DE CIÊNCIA DA DECLARAÇÃO DE MANUTENÇÃO DE SIGILO**

Eu _____, funcionário da empresa _____, CNPJ: _____, titular do CPF: _____, pelo presente instrumento, na condição de prestador de serviços para a Fundação Cultural Palmares (FCP), sob o contrato de n° _____, declaro ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo, e comprometo-me a cumprir todas as orientações e determinações a seguir especificadas e demais normativos atinentes, em função do contato que terei com informações pertencentes à FCP, ou por ela custodiadas, em razão da permissão de acesso aos recursos computacionais necessários para a execução de minhas atividades profissionais, estando ciente, de acordo, aderente e responsável nos seguintes aspectos:

1. Obedecer, cumprir e respeitar as políticas, diretrizes e normas de segurança da informação da FCP, que regem o uso dos recursos a mim disponibilizados, sejam esses digitais ou impressos, bem como o manuseio das informações a que tenho acesso, ou possa vir a ter, em decorrência da execução de minhas atividades profissionais.

2. Qualquer meio de acesso a informações ou instalações, como identificador de usuário de rede, senhas de acesso a sistemas, aplicativos, internet, intranet, conta de correio eletrônico (e-mail), crachás, cartões, chaves, dispositivo eletrônico de criptografia ou afins), que a FCP me forneceu ou vier a me fornecer são individuais e intransferíveis e estarão sob minha custódia e serão utilizados exclusivamente no cumprimento de minhas responsabilidades funcionais, devendo ser por mim devolvidos ou disponibilizados à FCP em caso de desligamento, encerramento de serviços ou mudança de função.

3. Meus acessos à Internet e à Conta de Correio Eletrônico por meio dos recursos fornecidos a mim e pertencentes à FCP devem ser utilizados única e exclusivamente para a realização de atividades explicitamente especificadas nas Ordensde Serviço.

4. Todos os meus acessos efetuados, lógicos ou físicos, e informações por mim manipuladas (sistemas de informação, correspondências, cartas, correios eletrônicos, etc.) serão passíveis de verificação por representantes da FCP, que recebam atribuição para tal, a qualquer momento, independentemente de aviso prévio. Em decorrência disso, fico ciente que a FCP é o legítimo proprietário e custeador de todos os equipamentos, infraestrutura, informações e sistemas de informação que serão por mim utilizados.

5. Não devo adquirir, reproduzir, instalar, utilizar e/ou distribuir cópias não autorizadas de softwares ou programas aplicativos, produtos, inclusive aqueles desenvolvidos internamente na FCP.

6. Não é permitida a entrada ou saída de quaisquer informações pertencentes à FCP, quer essas sejam em meios magnéticos (CDs, fitas, disquetes, pen drives, etc.), em

meios físicos (papel, impressos, etc.) ou em meios lógicos (webmail, internet, etc.) sem o conhecimento e autorização de seu responsável.

7. Em caso de utilização de acesso remoto, desde que devidamente autorizado, aos recursos da FCP para a execução de minhas atividades profissionais, devo manusear as informações obedecendo aos mesmos critérios de segurança exigidos nas instalações internas, para o desempenho de minhas atividades.

8. Devo zelar pela segurança, pelo uso correto e pela manutenção adequada dos equipamentos pertencentes à FCP, compreendendo dentre outros aspectos:

i. Nunca deixar um equipamento ativo sem antes bloquear seu acesso ou desativar a senha quando dele se afastar ou se ausentar.

ii. Jamais emprestar minha senha ou utilizar a senha de outros.

iii. Nunca utilizar senhas triviais que possam ser facilmente descobertas.

iv. Não divulgar informações da FCP, de partes, de advogados e de prestadores de serviços.

v. Não deixar relatórios ou quaisquer mídias com informações confidenciais expostos em locais de fácil acesso.

vi. Não utilizar recursos e/ou equipamentos particulares, na rede da FCP, para a realização de qualquer tipo de atividade, seja ela profissional ou não, sem a devida avaliação e autorização da FCP.

vii. Somente utilizar software que tenha sido devidamente homologado pelo órgão ou gestor responsável.

viii.Respeitar as legislações de direitos autorais e de propriedade intelectual.

ix. Quando houver a necessidade de descartar as informações, fazer de forma a impedir o seu resgate independentemente do meio de armazenamento na qual a informação se encontra.

x. Informar imediatamente o órgão responsável e à Divisão de Tecnologia de Informação e Comunicação da FCP acerca de qualquer violação das regras de sigilo por quem quer que seja.

9. Reconheço que a lista acima é meramente exemplificativa e ilustrativa e que outras hipóteses de confidencialidade, que já existam ou que venham a surgir no decorrer da contratualidade, devem ser consideradas e mantidas em segredo, e que em caso de dúvida acerca da confidencialidade de determinada informação devo tratá-la sob sigilo, até que venha a ser autorizado a tratá-la diferentemente pelo órgão ou gestor responsável. Em hipótese alguma irei interpretar o silêncio da FCP como liberação de quaisquer dos compromissos ora assumidos.

10.Descumprindo os compromissos por mim assumidos neste Termo de Ciência da Declaração da Manutenção do Sigilo, estarei sujeito às penalidades aplicáveis, como medidas administrativas e/ou disciplinares internas, e/ou, ainda, ações penais, cíveis e/ou trabalhistas previstas em lei.

11.Estou ciente de que, para fins penais, de acordo com o art. 327 do Código Penal, equipara-se a funcionário público quem exerce cargo, emprego ou função em órgão público ou entidade paraestatal, e quem trabalha para empresa prestadora de serviço CONTRATADA ou conveniada para a execução de atividade típica da Administração Pública.

Brasília, DF, ___ de _____ de _____

| **CONTRATANTE** | |
|---|---|
| Área/Fiscal Requisitante da Solução | Gestor do Contrato |
| _____<br><Nome><br>Matrícula: <Matr.> | _____<br><Nome><br>Matrícula: <Matr.> |
| **CONTRATADA** | |
| **Preposto** | **Funcionário** |
| _____<br><Nome><br><Qualificação> | _____<br><Nome><br><Qualificação> |

# Anexo V - ANEXO V - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE TIC.pdf

## ANEXO V - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE TIC

| LOTE ÚNICO | | | |
|---|---|---|---|
| **Item** | **Especificação** | **Quant.** | **Métrica** |
| 1 | Solução Segurança Avançada para Endpoints, com proteção integrada contra-ataques complexos, direcionados e descoberta avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a incidentes, bem como serviços em nuvem e zero day | 150 | Unidade |
| 2 | Serviços de Instalação | 01 | Unidade |
| 3 | Treinamento Técnico | 01 | Turma |

Apresentar a composição de cada item do escopo de fornecimento, contendo marca, modelo, códigos, descritivo dos códigos, unidade, quantidades do conjunto, tudo com o objetivo de se identificar claramente quais os produtos e serviços estão sendo ofertados;

Apresentar documentação técnica (manuais e/ou catálogos do fabricante, em mídia eletrônica ou URL) comprovando o pleno atendimento a todos os requisitos técnicos, por meio de apresentação de uma planilha ponto-a-ponto, com indicação de nome do documento e página que comprova o atendimento.

Não será aceita comprovação por carta do fabricante ou distribuidor ou da licitante;

**ITEM 1 - Console de gerenciamento centralizado**

1.1.1 O software deve dispor de gerenciamento com administração centralizada, com facilidades para instalação, administração, monitoramento, atualização e configuração, com todos os módulos de um único fornecedor.
1.1.2 O acesso ao Console de Gerenciamento deve ser possível via tecnologia Web segura (HTTPS) compatível, no mínimo, com os navegadores Google Chrome, Mozilla Firefox, Microsoft Edge, Opera e Safari.
1.1.3 O acesso ao Console deve suportar várias sessões simultâneas.
1.1.4 Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas.
1.1.5 Mecanismo de comunicação randômico (pull) entre o cliente e o servidor, para consulta de novas configurações e assinaturas, evitando sobrecarga de rede e/ou no servidor.
1.1.6 Permitir o agrupamento dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio.
1.1.7 O servidor de gerenciamento deve possuir compatibilidade para instalação nos seguintes sistemas operacionais em todas as versões/distribuições/releases e Hypervisors:
a) Microsoft Windows 10;
b) Microsoft Windows 11;
c) Microsoft Windows Server 2012;
d) Microsoft Windows Server 2012 R2;
e) Microsoft Windows Server 2016;
f) Microsoft Windows Server 2019;
g) Microsoft Windows Server 2022;
h) Ubuntu 16.04.1 LTS x64 Desktop;

i) Ubuntu 16.04.1 LTS x64 Server;
j) Ubuntu 18.04.1 LTS x64 Desktop;
k) Ubuntu 18.04.1 LTS x64 Server;
l) Ubuntu 20.04 LTS x64;
m) RHEL Server 7 x64;
n) RHEL Server 8 x64;
o) CentOS 7 x64;
p) Debian 10 x64;
q) VMware vSphere/ESXi 6.5 e posterior;
r) VMware Workstation 9 e posterior;
s) VMware Player 7 e posterior;
t) Microsoft Hyper-V Server 2012, 2012 R2, 2016, 2019;
u) Oracle VirtualBox 6.0 e posterior;
v) Citrix 7.0 e posterior;
1.1.8 O servidor de gerenciamento deve possuir compatibilidade para instalação em sistemas operacional de 64-bits tanto em ambiente virtual quanto físico, disponibilizado pela CONTRATANTE.
1.1.9 A console de gerenciamento deve oferecer também, opção para gerenciamento em nuvem, disponibilizado pela CONTRATADA.
1.1.10 Possuir integração com LDAP e Active Directory, para importação da estrutura organizacional e autenticação dos Administradores.
1.1.11 Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede.
1.1.12 Possibilidade de criar grupos separando as regras aplicadas a cada dispositivo.
1.1.13 Possibilidade de instalação dos clientes em estações de trabalho e servidores podendo estes ser físicos ou virtualizados, via console de gerenciamento, de forma remota, sem intervenção do usuário (modo silencioso).
1.1.14 Possibilitar a remoção, de forma automatizada das soluções dos principais fabricantes atualmente instalados nas estações de trabalho e ou servidores da CONTRATANTE.
1.1.15 Descobrir automaticamente as estações da rede que não possuem o cliente instalado através de funcionalidade integrada ao console de gerenciamento.
1.1.16 Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota.
1.1.17 A console de gerenciamento deve apresentar funcionalidade que impeça o usuário de alterar as configurações do cliente gerenciado de modo que não se possa alterar, importar e exportar configurações, abrir a console do cliente, desinstalar ou parar o serviço do cliente.
1.1.18 Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação (minimamente os níveis de operador e administrador).
1.1.19 A solução deve possuir sistema RBAC (Role Based Access Control) para definir acessos customizados de usuários adicionais no console, oferecendo granularidade para configuração dos acessos, para segregar os acessos, limitando os acessos a não exclusivamente políticas, tarefas, e demais objetos do console.
1.1.20 O log deve ser centralizado e conter, no mínimo, os seguintes itens:
a) Nome da ameaça;
b) Nome do arquivo infectado;
c) Caminho da detecção;
d) HASH do arquivo;
e) Data e hora da infecção;
f) Ação tomada;
g) Endereço de IP da máquina;
h) Usuário autenticado na máquina;
i) Origem da ameaça (IP ou hostname da máquina) caso a ameaça tenha se propagado;

1.1.21 Fornecer, em tempo real, o status atualizado das estações de trabalho, com pelo menos as seguintes informações:
a) Nome da máquina;
b) Endereço IP da máquina;
c) Malwares não removidos;
d) Status da conexão;
e) Data da vacina;
f) Versão do antivírus instalado.
1.1.22 O console de gerenciamento deve prover alertas de segurança via E-mail, com informações de infecção de máquinas e ataques. Suportando no mínimo alertas dos seguintes módulos:
a) Detecções de Malware;
b) Detecções de Firewall;
c) Detecções via EDR;
1.1.23 Utilizar o protocolo HTTPS ou outro protocolo seguro para comunicação entre console de gerenciamento e o cliente gerenciado.
1.1.24 Capacidade de voltar (rollback) para versão de atualização (da solução ou vacina) através de procedimento específico no console de gerenciamento.
1.1.25 Interface da Console de Gerenciamento totalmente em português.
1.1.26 Deve permitir criar o backup da Base de dados da Console de gerenciamento.
1.1.27 O acesso a console de gerenciamento deverá ser autenticado.
1.1.28 A console deverá funcionar também através de um Appliance Virtual fornecido pelo fabricante.
1.1.29 O acesso ao console de administração do antivírus deve permitir a possibilidade de ser feito com duplo fator de autenticação integrado dentro da mesma console onde é possível ativá-lo sem a necessidade de nenhum add-on adicional.
1.1.30 Gerar pacotes de instalação dos clientes, para cada tipo de sistema operacional existente na estrutura da CONTRATANTE, possibilitando a gravação em mídia e a instalação do software em ambientes onde não seja possível a instalação via rede corporativa.
1.1.31 Permitir forçar a instalação do software cliente do antivírus nos computadores, reinstalando-o em caso de desinstalação ou corrupção do mesmo.
1.1.32 Atualização de vacinas sem a necessidade de reinicialização.
1.1.33 Suportar o gerenciamento de todos os clientes instalados nas máquinas (estações de trabalho, servidores, tablets e smartphones) a partir do servidor de Console de Gerenciamento, oferecendo a possibilidade de configuração centralizada e remota de todas as funcionalidades.
1.1.34 Gerenciar de forma remota as configurações do firewall local de cada máquina com o cliente instalado.
1.1.35 A solução deve oferecer recurso para isolar as máquinas da rede, mantendo apenas comunicação segura com o servidor de gerenciamento.
1.1.36 Criação de grupos e subgrupos de máquinas baseada na hierarquia do Active Directory e LDAP ou em identificador único de clientes, tal como endereço IP;
1.1.37 Forçar a configuração determinada no servidor para os clientes, protegendo o software cliente de alterações pelos usuários, com senha pré-determinada na console de gerenciamento.
1.1.38 Atualização/sincronização de configurações nos clientes sem a necessidade de reinicialização ou logoff.
1.1.39 Permitir a criação de tarefas de rastreamento em períodos de tempo pré-determinados e na inicialização do sistema operacional.
1.1.40 Permitir a criação de tarefas de atualização de vacinas e novas versões de software em períodos de tempo pré-determinados.
1.1.41 Permitir o uso de ferramentas para centralizar a distribuição de atualizações de software e atualizações dos módulos, não será aceito o uso de ferramentas de terceiros;

1.1.42 Permitir criação das tarefas para uma máquina, um grupo de máquinas e/ou para todas as máquinas.
1.1.43 Possuir no mínimo 42 modelos de relatórios pré configurados com filtros e conjuntos de filtros na console de gerenciamento.
1.1.44 No console de gerenciamento em nuvem, a solução deve permitir a criação de relatórios customizados. Não serão aceitos apenas os relatórios pré configurados da solução.
1.1.45 Geração de relatórios, permitindo a customização dos mesmos e a exportação para os seguintes formatos (no mínimo um deles):
a) CSV;
b) PDF;
1.1.46 Geração de relatórios que contenham as seguintes informações:
a) Máquinas com a lista de definições de vírus desatualizada, ou todas as máquinas e suas respectivas versões da lista de definições de vírus;
b) Versão do software instalado em cada máquina;
c) Vírus que mais foram detectados;
d) Máquinas que mais sofreram infecções em um determinado período de tempo;
1.1.47 Permitir o armazenamento em um banco de dados centralizado das informações coletadas nos clientes:
a) Registro de eventos (log);
b) Relatórios de eventos de vírus e status dos clientes;
c) Relatórios de Softwares instalados;
d) Relatórios de Hardware encontrados;
1.1.48 Deve ter a capacidade de enviar eventos para um servidor SIEM, suportando no mínimo os seguintes formatos:
a) JSON;
b) LEEF;
c) CEF;
1.1.49 Fornecer, em tempo real, o status atualizado das estações de trabalho;
1.1.50 Possibilitar a exportação, em formato PDF e CSV, de relatórios que atuem com inventário de hardware e software de todas as estações e servidores ativos na estrutura da console de gerenciamento.
1.1.51 Permitir a instalação remota do agente e produto de segurança através de GPO ou SCCM.
1.1.52 Possuir módulo de gerenciamento de dispositivos móveis Android e iOS.
1.1.53 Por meio do console de gerenciamento deve ser possível gerenciar dispositivos móveis iOS e Android e ter um banco de dados separado do restante dos servidores e estações de trabalho.
1.1.54 O módulo de gerenciamento de dispositivos móveis deverá possuir arquitetura padrão de soluções MDM (Mobile Device Management) do mercado.
1.1.55 A solução deverá disponibilizar o gerenciamento de dispositivos móveis também através do console em nuvem.
1.1.56 O gerenciamento em dispositivos IOS deverá requerer certificado do serviço de notificação por push da Apple, a fim de possibilitar uma comunicação segura entre o servidor e o device.
1.1.57 Possibilitar a instalação da solução de segurança aos dispositivos móveis de maneira manual através de QRcode, link gerado pela solução de gerenciamento e e-mail
1.1.58 Através da console de gerenciamento a solução deve possibilitar a ativação da opção de bloqueio de exploit por meio do módulo de firewall nas estações e servidores.
1.1.59 Atualização incremental e on-line das vacinas.
1.1.60 A solução deve possuir Sandbox na nuvem para analisar o comportamento de malwares, com SLA de 5 minutos até 1 hora de resposta.

1.1.61 Deve ter a capacidade de utilizar o módulo Sandbox na nuvem para bloquear ameaças de rede a fim de impedir que sejam executadas nas estações de trabalho.
1.1.62 O Sandbox na nuvem deve ser capaz de identificar e bloquear ameaças de dia zero.
1.1.63 A funcionalidade de Sandbox na nuvem deverá ser gerenciada na mesma console principal, permitindo o envio de arquivos para análise de maneira integrada.
1.1.64 A funcionalidade de Sandbox na nuvem deverá possibilitar que o usuário decida como tratar o arquivo analisado.
1.1.65 A tecnologia de Sandbox deve ser baseada em ferramentas de desenvolvimento como: inteligência artificial e machine learning.
1.1.66 Atualização em clientes móveis (notebook, laptop, netbook, ultrabook e similares) a partir do site do fabricante do antimalware ou de outra fonte definida pelo administrador.
1.1.67 Capacidade de configurar políticas móveis para quando um computador estiver fora da estrutura de proteção, possa atualizar-se via internet.
1.1.68 Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento e Site do Fabricante.
1.1.69 Possibilidade de eleição de qualquer cliente gerenciado como um servidor de distribuição das atualizações, podendo eleger mais de um cliente para esta função.
1.1.70 Nas atualizações das configurações e das definições de malwares não se poderá fazer uso de logon scripts, agendamentos ou tarefas manuais ou módulos adicionais que não sejam parte integrante da solução.
1.1.71 Qualquer atualização de vacinas deve ser possível sem a necessidade de reinicialização do computador ou serviço para aplicá-la.
1.1.72 Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária.
1.1.73 O sistema deve fornecer um único e mesmo arquivo de vacina de malwares para todas as versões do Windows e do antimalware, sendo aceitável arquivos diferentes, para plataformas 32-bits e 64-bits.

**1.2 Solução de Antivírus para estações e servidores**
1.2.1 A solução ofertada deve suportar sistemas operacionais com arquitetura 32-bits e 64-bits.
1.2.2 Gerenciado através de Console de Gerenciamento.
1.2.3 Interface do software cliente em português.
1.2.4 Manuais em português.
1.2.5 O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade para instalação com os seguintes sistemas operacionais em todas as versões/distribuições/releases:
a) Microsoft Windows 7;
b) Microsoft Windows 8;
c) Microsoft Windows 8.1;
d) Microsoft Windows 10;
e) Microsoft Windows 11;
f) Microsoft Windows Server 2008 R2;
g) Microsoft Windows Server 2012 R2;
h) Microsoft Windows Server 2016;
i) Microsoft Windows Server 2019;
j) Microsoft Windows Server 2022;
k) Red Hat;
l) SUSE;
m) Ubuntu;
n) CentOs;
o) Debian;
p) Fedora;

q) Linux Mint 20;
r) Linux Mint 21;
s) MacOS 10.12 Sierra;
t) MacOS 10.13 High Sierra;
u) MacOS 10.14 Mojave;
v) MacOS 10.15 Catalina;
w) MacOS 11 Big Sur;
x) MacOS 12 Monterey;
y) MacOS 13 Ventura;
z) Android 5 e versões posteriores;
aa) IOS 9 e versões posteriores.
1.2.6 O cliente deve ter a capacidade de continuar operando, mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede.
1.2.7 O cliente deve ter a capacidade de atualizar a versão do agente através do servidor de gerenciamento.
1.2.8 Quando o servidor de gerenciamento estiver inoperante ou o agente estiver incapaz de comunicar-se com o servidor por razões distintas, o agente deve ser capaz de atualizar vacinas e componentes através de comunicação com uma nuvem de dados fornecida pelo fabricante.
1.2.9 Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento.
1.2.10 Permitir o rastreamento de malware, agendado ou manual, com a possibilidade de selecionar como alvo uma máquina ou grupo de máquinas, com periodicidade mínima diária.
1.2.11 O cliente gerenciado deve implementar funcionalidade em que as configurações, alteração, desinstalação, desativação do serviço, importação e exportação de configurações possam ser bloqueadas por senha, através do console de modo a evitar que o usuário da estação de trabalho interfira no funcionamento da solução.
1.2.12 Atualização de configurações, sem interação (em background), nos clientes sem a necessidade de reinicialização ou logoff.
1.2.13 Capacidade de tratar ameaças que exploram a ausência de correções do Sistema Operacional (patches) fazendo com que as ameaças que se utilizam de vulnerabilidades sejam bloqueadas enquanto a correção oficial não esteja instalada/disponível corretamente, ou possuir análise heurística ou inteligência artificial (machine learning) capaz de identificar e bloquear qualquer ameaça externa que se utilize de vulnerabilidades dos sistemas operacionais.
1.2.14 Caso a solução encontre algum arquivo mal-intencionado (tais como ameaça dia-zero, ameaça persistente), deve possuir capacidade de análise e posterior bloqueio automático.
1.2.15 A função de Escaneamento de vírus deverá ter a possibilidade de configuração de exceções:
a) Excluir da verificação tipos de arquivos tais como .TXT (arquivo de texto simples).
b) Pastas e arquivos pré-determinados através do caminho ou Hash.
1.2.16 Deve permitir a instalação e desinstalação remota pela console de gerenciamento centralizada.
1.2.17 Possibilidade de instalação presencial através de mídia de instalação fornecida ou gerada através do servidor de antivírus.
1.2.18 Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, com frequência (no mínimo diária) e horários definidos no console de gerenciamento centralizado:
a) Permitir atualização incremental da lista de definições de vírus;
b) Permitir atualização por endereço do próprio fabricante, como opção além do servidor local;
c) Permitir configuração remota de ordem de preferência de endereços de atualização;

d) Permitir configurar conexão através de serviço Proxy local;
e) Permitir a atualização da lista de arquivos a serem verificados contra vírus através da lista de definições de vírus;
1.2.19 No sistema operacional Linux além de proteger e rastrear seus sistemas de arquivos, também aos arquivos armazenados em compartilhamentos SAMBA/CIFS ou que de alguma forma estejam disponibilizados para o acesso de clientes Windows em um servidor Linux.
1.2.20 Deve ser capaz de detectar e remover todos os tipos de malwares, incluindo vírus, ransomware, worm, trojan, spyware, rootkit, vírus de macro e códigos maliciosos.
1.2.21 Possuir mecanismo de detecção baseado em ferramentas de análise e detecção como:
a) Machine Learning
b) Instrusion Prevention System
c) Inteligência Artificial
1.2.22 Rastreamento em tempo real para vírus de macro e arquivos criados, copiados, renomeados, movidos ou modificados, inclusive em sessões DOS abertas pelo Windows.
1.2.23 Possuir módulo de proteção em tempo real do sistema de arquivos, o qual deve controlar todos os arquivos no sistema a fim de detectar código malicioso quando os arquivos são abertos, criados ou executados.
1.2.24 Possuir módulo de detecção proativa que forneça proteção contra uma nova ameaça durante a propagação inicial.
1.2.25 A solução para estações de trabalho Windows deve possuir módulo com funcionalidade de navegador seguro, para proteção de acesso a websites que contenham dados confidenciais. Não serão aceitos módulos convencionais de “Web Protection”, deverá oferecer camada adicional dedicada para tal proteção.
1.2.26 Empregar proteção baseada em nuvem conectada diretamente aos laboratórios de pesquisa e desenvolvimento do fabricante.
1.2.27 Possuir módulo nativo de detecção e proteção contra variantes de ransomware existentes no mundo, a fim de atuar como um escudo contra este tipo de ameaça.
1.2.28 A solução deve ser capaz de fazer a varredura em um estado ocioso para fornecer proteção proativa enquanto o equipamento não está em uso
1.2.29 Permitir diferentes configurações de varredura em tempo real, tornando o desempenho do produto mais estável, principalmente em máquinas com baixo desempenho de hardware.
1.2.30 Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo.
1.2.31 Detecção em tempo real e limpeza de programas maliciosos como spywares, ransomware, adwares, jokes, discadores, ferramentas de administração remota e programas quebradores de senha, realizando a remoção desses programas e a restauração de áreas do sistema danificados pelos mesmos, com possibilidade de criar uma lista de exclusão dos programas não desejados, onde a administração seja centralizada pela mesma console de gerenciamento do antivírus.
1.2.32 Rastreamento manual com interface gráfica, customizável, com opção de limpeza.
1.2.33 Rastreamento por linha de comando, parametrizável, com opção de limpeza.
1.2.34 Programação de rastreamentos automáticos do sistema com as seguintes opções:
a) Escopo: todos os drives locais, específicos ou pastas específicas;
b) Ação: somente alertas, limpar automaticamente, apagar automaticamente ou mover automaticamente para área de segurança;
c) Frequência: diária, semanal e mensal;
d) Exclusões: pastas ou arquivos que não devem ser rastreados;

1.2.35 Possuir área de segurança (quarentena) no computador no qual o cliente estiver executando.
1.2.36 Detecção de anomalias através dos métodos de assinatura, heurística e por comportamento.
1.2.37 Proteção contra ameaças via internet. A solução deve conter pelo menos:
a) Ajuste no nível de sensibilidade da detecção;
b) Lista de exceção.
1.2.38 Detecção em tempo real e possibilidade de bloqueio e remoção de malwares provenientes de downloads realizados no ambiente web.
1.2.39 Permitir que a funcionalidade de rastreamento em tempo real na navegação possa ser desabilitada;
1.2.40 Detecção em tempo real e possibilidade de bloqueio e remoção de malwares no conteúdo e anexos de mensagens de correio eletrônico, pelo antivírus cliente, analisando tráfego e suportando principais clientes (no mínimo outlook).
1.2.41 Permitir que a funcionalidade de rastreamento em tempo real de e-mail possa ser desabilitada.
1.2.42 Detecção em tempo real e possibilidade de bloqueio e remoção de malwares nas áreas de armazenamento de dispositivos removíveis, tais como:
a) PenDrive;
b) HD externo;
c) Celulares;
d) Tablets;
e) CD/DVD;
f) Impressora USB;
g) Armazenamento de FireWire;
h) Dispositivo Bluetooth;
i) Leitor de cartão inteligente;
j) Dispositivo de criação de imagem;
k) Modem;
l) Porta LPT/COM;
m) Dispositivo portátil;
1.2.43 O módulo de controle de dispositivos deve estar disponível para estações de trabalho Windows, macOS e Linux.
1.2.44 Detecção, análise e reparação de vírus em arquivos compactados, automaticamente, incluindo pelo menos 05 níveis de compactação, nos formatos mais utilizados no mercado.
1.2.45 Ferramenta de firewall bidirecional local no cliente, com possibilidade de configuração, ativação e desativação através da console de gerenciamento centralizada, contendo filtros especificados por aplicação, protocolo, IP, range de IPs, rede, porta e range de portas.
1.2.46 A ferramenta de firewall local deverá tratar tráfego de entrada e de saída de forma independente.
1.2.47 Deve permitir o bloqueio do “Autorun” nas portas USB ou bloquear automaticamente a execução de qualquer ameaça em dispositivos móveis.
1.2.48 Permitir bloquear a conexão de dispositivos removíveis.
1.2.49 Gerar registro (log) dos eventos de vírus em arquivo.
1.2.50 Gerar relatórios, ao menos, de:
a) Eventos de vírus;
b) Status dos clientes;
c) Status dos Updates;
1.2.51 Gerar notificações de eventos de vírus através de alerta por e-mail, ao menos.
1.2.52 Gerar relatórios incluindo tipos de vírus, nome do vírus e se precisa de atualização do Sistema Operacional.
1.2.53 Possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes

opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total.
1.2.54 Permitir a criação de exceções nos escaneamentos de arquivos.
1.2.55 Permitir o bloqueio de dispositivos com base nos seguintes critérios:
a) Fabricante;
b) Modelo;
c) Número de série;
1.2.56 Permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URLs acessadas.
1.2.57 A solução deve permitir a configuração de quais portas HTTPs serão escaneadas para verificação de conexões criptografadas.
1.2.58 O Firewall deve possuir funcionalidade deve suportar os protocolos TCP e UDP.
1.2.59 O Firewall deve reconhecer o tráfego DNS, DHCP e WINS com opção de bloqueio.
1.2.60 Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan e Spoofing e botnet.
1.2.61 Possibilidades de criação de assinaturas personalizadas para detecção.
1.2.62 Possibilidade de agendar a ativação de novas regras do firewall.
1.2.63 Possibilidade de criar regras diferenciadas por aplicações.
1.2.64 Bloqueio de ataques baseado na exploração da vulnerabilidade.
1.2.65 Permitir integração com navegadores WEB para prevenção de ataques.
1.2.66 Realizar proteção usando mecanismo de reputação on-line, reportando informações referentes ameaças durante a navegação web.
1.2.67 Possuir taxa de performance de rede inferior a 70MB (mega bytes) comprovada junto a instituições reconhecidas mundialmente em análises profundas de funcionalidades de fabricantes de soluções de segurança.
1.2.68 A solução deve prover proteção em tempo real contra vírus, trojans, worms, spyware, adwares e outros tipos de códigos maliciosos.
1.2.69 As configurações do antimalware deverão ser realizadas através da mesma console de todos os itens da solução.
1.2.70 Permitir a criação de listas de exceções de arquivos e diretórios (arquivos ou diretórios que não serão varridos em tempo real).
1.2.71 Permitir verificação das ameaças de maneira manual, agendada e em tempo real detectando ameaças no nível do Kernel do sistema operacional fornecendo a possibilidade de detecção de Rootkits.
1.2.72 Possibilitar que, nas varreduras agendadas, o disparo do processo ocorra por grupos com intervalos de tempo determinados, de forma a reduzir impacto em ambientes.
1.2.73 Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar e Ignorar.
1.2.74 Verificação de malwares nas mensagens de correio eletrônico, pelo antimalware da estação de trabalho, suportando clientes Outlook, ou que utilizem os protocolos POP3/SMTP.
1.2.75 Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados.
1.2.76 Deve suportar varredura de, no mínimo, os seguintes padrões de compactação:
a) CAB;
b) ZIP;
c) RAR;
d) LHA;
e) ARJ;
f) TAR;
1.2.77 Capacidade de terminar o processo e serviço da ameaça no momento de detecção.

1.2.78 Capacidade de identificação da origem da infecção, para malwares que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou endereço IP da origem com opção de bloqueio da comunicação via rede.
1.2.79 Possibilidade de bloquear verificação de malware em recursos mapeados da rede.
1.2.80 Capacidade de realizar monitoramento em tempo real por heurística correlacionando com a reputação de arquivos.
1.2.81 Não serão aceitas soluções de Antimalware que possuam engine de terceiros.
1.2.82 Permitir o bloqueio da execução de aplicações baseado em nome e pasta.
1.2.83 A solução deve permitir a detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações.
1.2.84 Capacidade de detecção de keyloggers por comportamento dos processos em memória.
1.2.85 Reconhecimento de comportamento malicioso de modificação da configuração de DNS e arquivo Hosts.
1.2.86 Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção de níveis distintos de sensibilidade de detecção.
1.2.87 Realizar inspeção de ameaças em ambiente isolado, com o emprego de ferramentas como:
a) Aprendizado de máquina;
b) Deep Learning;
c) Análise estatística e dinâmica;
d) Detecção baseada em comportamento;
e) Introspecção na memória;
1.2.88 Detecção do malware por DNA do vírus.
1.2.89 Deverá ter a capacidade de atualizar os patches do sistema operacional.
1.2.90 A solução deve ser capaz de detectar o uso do Hyper-V e ter uma verificação de malware específica disponível para este hypervisor.
1.2.91 Em servidores que usam “OneDrive for Business” deve ser possível explorar os arquivos armazenados nesta nuvem, procurando por arquivos comprometidos ou possível malware.
1.2.92 A solução de proteção de servidor deve incluir a detecção e bloqueio de intrusões, adicionando à lista negra os endereços que foram identificados com este comportamento malicioso.
1.2.93 A solução deve adicionar exclusões automaticamente para aplicativos de servidor críticos.
1.2.94 A solução deve possuir otimização de desempenho para infraestruturas mistas (física e virtual), podendo eliminar a duplicação de verificações de arquivos, excluindo arquivos já verificados e limpos.
1.2.95 Controlar acesso a sites, possibilitando o bloqueio dos mesmos.
1.2.96 Permitir criar políticas de bloqueio com base em categorias e lista de URL.
1.2.97 Permitir gerar relatórios de sites acessados e bloqueados.
1.2.98 Permitir a personalização das mensagens exibidas quando um ou mais sites forem bloqueados.
1.2.99 Deverá possuir um plug-in que se integre com o cliente de correio eletrônico como Outlook, Outlook Express e Windows Mail.
1.2.100 Para o módulo de proteção de e-mail, deve suportar minimamente os seguintes protocolos:
a) POP3;
b) POP3S;
c) IMAP;
d) IMAPS;
1.2.101 Deve permitir a configuração de ações personalizadas para detecções realizadas pelo módulo de proteção de e-mail, suportando minimamente as seguintes ações:

a) Mover o e-mail para uma pasta;
b) Excluir o e-mail;
c) Manter o e-mail;
1.2.102 Em equipamentos macOS, a solução deve possuir módulo para proteção de e-mails de entrada e saída.
1.2.103 Para a navegação na internet o produto deve contar o antiphising para proteger os usuários finais de sites web falsos que tentam obter informações confidenciais.
1.2.104 A solução de proteção anti-spam deve realizar as verificações utilizando o protocolo SSL.
1.2.105 O módulo de proteção anti-spam deverá ser nativo e integrado ao Endpoint.
1.2.106 Possuir protocolo de replicação que utilize o protocolo HTTPS e o serviço de notificação via push.

**1.3 Solução de Sandbox em nuvem**
1.3.1 Deve ser possível criar exclusões por caminho, nome de detecção e hash do arquivo (SHA-1).
1.3.2 A solução deve permitir a definição do tempo máximo para análise automática de artefatos.
1.3.3 Capacidade de sincronizar seu licenciamento com a nuvem e o console de administração no local (on-premise) ou na nuvem.
1.3.4 Detectar um arquivo suspeito executado pela primeira vez, um aviso deve ser exibido, se a verificação for concluída antes do arquivo ser executado pela primeira vez, o aviso de arquivo sob verificação não será exibido. Deve eliminar automaticamente as amostras dos arquivos/executáveis nos servidores onde o comportamento foi analisado.
1.3.5 Capacidade para enviar e-mails de SPAM para sua análise.
1.3.6 Deve classificar os artefatos em categorias, oferecendo no mínimo as seguintes categorias: desconhecido, limpo, suspeito, altamente suspeito e malicioso.
1.3.7 Deve disponibilizar as seguintes informações de um arquivo enviado ao Sandbox na nuvem: nome do equipamento que enviou o arquivo, o usuário conectado no dispositivo, o resultado da análise, hash no formato SHA-1, nome do arquivo analisado, tamanho do arquivo, categoria.
1.3.8 Deve oferecer proteção proativa, ou seja, que o arquivo/executável seja bloqueado até receber o resultado do Sandbox na nuvem.
1.3.9 A solução deve possuir integração com a solução de antimalware, para possuir maiores possibilidades de proteção e aplicação de políticas.
1.3.10 A solução de Sandbox em nuvem deve estar disponível minimamente para integração com os produtos para estações e servidores Windows e Linux.
1.3.11 Deve ser possível enviar um arquivo/executável manualmente para a solução de Sandbox em nuvem.

**1.4 Solução para criptografia de discos**
1.4.1 A solução deverá ser capaz de criptografar dispositivos Windows e macOS.
1.4.2 Para estações Windows, a solução deverá possuir tecnologia própria de criptografia. Não serão aceitas soluções que apenas oferecem gerenciamento do BitLocker (Microsoft).
1.4.3 Para estações macOS, a solução deve ser capaz de gerenciar o FileVault disponibilizado pela Apple.
1.4.4 A solução deverá ser capaz de criptografar os Endpoints desejados desde o início do sistema operacional.
1.4.5 A solução deverá dispor de diversas possibilidades de recuperação de senha para usuários remotos que estejam bloqueados.

1.4.6 A solução deverá poder programar as tarefas de criptografia sobre os Endpoints desejados com a possibilidade de pausar a execução para retomar desde o último estado.
1.4.7 A solução deverá ser administrada desde o mesmo console central junto com as outras soluções descritas neste termo de referência.
1.4.8 Possibilitar a opção de criptografar apenas o disco de inicialização.
1.4.9 Possibilitar que as estações de trabalho sejam criptografas sem que o recurso de TPM (Trusted Platform Module) esteja válido.
1.4.10 Através da console central deve ser possível invalidar a senha de login do usuário e solicitar que mude sua senha de login por meio de uma interface gráfica.
1.4.11 Deve possibilitar que o administrador recupere os dados caso o usuário não consiga acessar a máquina com suas credenciais.
1.4.12 Deve possibilitar que o administrador gere uma nova senha de recuperação para o usuário.

**1.5 Solução para gerenciamento de vulnerabilidades e patches**
1.5.1 Deve rastrear ativamente as vulnerabilidades dos sistemas operacionais e demais aplicações comuns, e instalar automaticamente os patches em todos os endpoints.
1.5.2 Deve poder configurar intervalo de tempos para a instalação automática de patches.
1.5.3 Deve detectar mais de 30.000 vulnerabilidades e exposições comuns (CVE)
1.5.4 Deve poder aplicar patches em aplicações comuns como Adobe Acrobat, Mozilla Firefox e Zoom Client.
1.5.5 Deve ser compatível com várias versões de Windows.
1.5.6 Deve priorizar e filtrar as vulnerabilidades segundo sua pontuação de exposição e gravidade.
1.5.7 Deve suportar multilocação em ambientes de rede complexos.
1.5.8 Deve permitir a visibilidade de vulnerabilidades em setores específicos da organização.
1.5.9 Deve oferecer visão geral unificada através da console Cloud, com suporte multi-idiomas e poucos requisitos de infraestrutura de TI.
1.5.10 Deve possuir controle das exceções para os patches de aplicações selecionadas.
1.5.11 Deve proporcionar um inventário atualizado de patches com nome do patch, nova versão da aplicação, CVE, gravidade/importância do patch e aplicações afetadas.

**1.6 Solução de proteção para Microsoft 365**
1.6.1 Deve contar com proteção para aplicações do Microsoft 365.
1.6.2 Deve proteger Exchange Online, Onedrive, Teams e Sharepoint Online.
1.6.3 A solução deve possuir módulo Anti-spam.
1.6.4 A solução deve possuir módulo Anti-phishing.
1.6.5 Deve permitir definir regras customizadas para os filtros da solução.
1.6.6 A solução deve possuir módulo Antimalware e bloquear automaticamente arquivos com detecções maliciosas.
1.6.7 Deve possuir integração com a solução de sandbox em nuvem, para análise detalhada de e-mails.
1.6.8 Deve contar com um console dedicado para administração através da nuvem disponibilizada pela CONTRATADA.
1.6.9 Deve poder configurar políticas de proteção.
1.6.10 A solução deve possuir filtros de detecção.
1.6.11 A solução deverá enviar notificações de detecções via e-mail
1.6.12 Deve ser uma solução “multitenant”, permitindo a integração de diversos “tenants” Microsoft para proteção através do mesmo console de gerenciamento.

1.6.13 Deve exibir informações em relatórios customizáveis.
1.6.14 Deve possuir painéis para visualização rápida, contendo estatísticas de segurança dos recursos protegidos.
1.6.15 A solução deve contar com quarentena para arquivos do Exchange online, Teams, Sharepoint e OneDrive.
1.6.16 Deve contar com opção de proteção automática para novos usuários criados dentro do espaço empresarial do Microsoft 365

**1.7 Outros requerimentos gerais**.
1.7.1 A solução ofertada não deve possuir restrições sobre a quantidade de equipamentos para ativação das licenças. A totalidade das licenças contratadas pode ser ativada completamente em servidores, estações de trabalho, ou dispositivos móveis, respeitando o limite total contratado.
1.7.2 Todos os módulos ofertados pelo fabricante, devem ser ativados utilizando uma única licença, sem a necessidade de aquisição de módulos separados (add-ons).
1.7.3 O fabricante deve possuir mais de 70 prêmios no VB100 do Virus Bulletin e o mínimo de 80 participações no mesmo
1.7.4 O fabricante deverá ter suporte local em idioma português.
1.7.5 O fabricante deve oferecer serviços de segurança da informação como por exemplo: teste de penetração, avaliação de vulnerabilidade ou análise de GAPs.
1.7.6 O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e engines e possuir analista dedicado a pesquisa de defesas contra ameaças e malwares originados no Brasil. Esta informação deve ser comprovada pelo Fabricante através de documentação oficial.
1.7.7 O fabricante deve possuir um laboratório de análise e detecção de malware na América Latina.
1.7.8 O fabricante deve possuir escritório próprio no Brasil.
1.7.9 Possuir manuais de apoio sobre a solução em português e inglês.
1.7.10 O fabricante deverá ter documentação publicada na internet no idioma português
1.7.11 O fabricante deve ser citado nos relatórios do MITRE ATT&CK como contribuinte de informações e técnicas de detecção nos últimos anos.
1.7.12 O fabricante deve possuir uma posição mínima de Challenger no Quadrante Mágico do Gartner nos últimos 4 anos (2019 – 2022).
1.7.13 O fabricante deve oferecer diretamente o serviço de Caça de Ameaças, também conhecido por Threat Hunting.
1.7.14 O fabricante deve oferecer programas de “colaborador seguro”.
1.7.15 Contar com a menção “Certified” na avaliação "Advanced Threat Protection Test 2021-Enterprise".
1.7.16 Ter sido considerado "Top Player" ao menos nos últimos 4 anos (2020 – 2023) dentro do relatório “APT Protection Market Quadrant” da Radicati.
1.7.17 Ter sido reconhecido como "Champion" dentro da “Global Cybersecurity Leadership Matrix” da Canalys ao menos nos últimos 3 anos (2019 – 2021).
1.7.18 O fabricante deve contar com a certificação ISO 9001 para o departamento de suporte que entregue o serviço.
1.7.19 O fabricante deve contar com a certificação de segurança ISO 27001.

**ITEM 2 - SERVIÇOS DE INSTALAÇÃO**
2.1. Para os serviços de instalação, configuração e transferência de conhecimento a CONTRATADA deverá apresentar, até o 3º dia da emissão da ordem de serviço/fornecimento de bens, um cronograma com as fases da implementação, dividido por solução contendo documentação detalhada das atividades de instalação, configuração e testes dos softwares de cada solução, em reunião presencial.
2.2. O prazo de inicio dos serviços não pode ser maior que 5 dias úteis da apresentação do cronograma.

2.3. Para todas as licenças fornecidas, deverão ser executados os serviços necessários para instalação, adequação ao ambiente da FCP, configuração e implementação das solução ofertada, inclusive nos casos em que intervenções manuais se fizerem necessárias.
2.4. Os serviços deverão ser prestados nas datas e horários definidos pela CONTRATANTE.
2.5. Todos os serviços devem ser executados por profissionais devidamente treinados e certificados pelo fabricante. Tais atestados devem ser fornecidos no inicio da execução dos serviços.
2.6. No serviço de implementação a CONTRATADA deve fazer a remoção total da solução existente antes da instalação da nova solução.
2.7. Deverá ser executado a migração de todas as políticas, regras e customizações configuradas no ambiente da FCP em caso de atualização de versão ou troca de produto.
2.8. Substituir imediatamente, a critério do CONTRATANTE, a qualquer tempo, e sem nenhum ônus adicional, qualquer profissional de seu corpo técnico cuja a presença seja considerada indesejada, desde que devidamente justificada.
2.9. Entregar a documentação técnica em meio eletrônico, completa e atualizada de todos os procedimentos realizados.
2.10. Uma vez implementada e testada a solução deverá ser emitido um termo de aceite pelo CONTRATANTE.
2.11. Para todas as soluções fornecidas a CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica da FCP durante o período de implantação da solução.

**ITEM 3 - TREINAMENTO TÉCNICO**
3.1. O repasse de informações deverá cobrir conhecimentos necessários para instalação, administração, configuração, otimização, resolução de problemas e utilização da solução;
3.2. A FCP, responsável pela infraestrutura, deverá disponibilizar 3 (três) técnicos para o acompanhamento das atividades de hands-on;
3.3. As horas de acompanhamento do hands-on deverão ser distribuídas ou organizadas da melhor maneira durante as atividades de instalação/configuração, mediante proposição da equipe técnica da FCP;
3.4. Não serão recebidos os serviços de hands-on prestados por profissionais que não estejam hábeis a demonstrar, na prática, as funcionalidades principais dos equipamentos e, particularmente, as atividades relacionadas à operação da solução;
3.5. A não realização do hands-on implicará na não aceitação da entrega definitiva do serviço;
3.6. Todas as despesas com instrutor(es), seu(s) deslocamento(s) e demais itens relacionados ao repasse do hands-on serão de responsabilidade da CONTRATADA;
3.7. A empresa deverá declarar, na proposta, que não realizará subcontratação para a execução dos serviços."

# Anexo VI - ANEXO VI - ESTUDO TÉCNICO PRELIMINAR.pdf

# Estudo Técnico Preliminar 70/2023

## 1. Informações Básicas

Número do processo: 01420.102456/2023-20

## 2. Descrição da necessidade

2.1 A pretensão contratação de Solução Segurança Avançada para Endpoints, com proteção integrada contra-ataques complexos, direcionados e descoberta avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a incidentes com instalação, configuração, treinamento, serviços de consultoria e suporte técnico em sistemas de segurança na solução fornecida para prevenção zero day.

2.2 Com a Lei em vigor da LGPD – Lei Geral de Proteção de Dados, datada de 1 de janeiro de 2021 e cientes ainda que a perda de dados contendo informações pessoais de servidores e cidadãos, titulares de dados, podem trazer prejuízos à FCP, entendemos indispensável a aquisição de uma Solução de Segurança robusta corporativa de estações de trabalho, servidores e conectividade segura e eficaz , a fim de contribuir com o alcance dos objetivos estratégicos.

2.3 As instituições e organizações devem proteger seus dados contra qualquer vazamento de dados que possa surgir de ameaças internas ou externas proteção para todos os setores e deve ser aplicado a todos os dispositivos e servidores que se conectam a sistemas corporativos ou manipulam dados. A legislação e os padrões institucionais (LGPD, PDPL, GDPR etc.) acionam essa necessidade.

2.4 Dessa forma, a solução será composta de produtos e serviços que contenham no mínimo as seguintes funcionalidades:

a) Gerenciamento centralizado;

b) Facilidade e flexibilidade no redirecionamento do tráfego entre os circuitos de comunicação conectados à solução;

c) Possibilidade de redução de riscos de indisponibilidade do serviço de comunicação de dados voz e vídeo entre núcleos, entre os núcleos, representações e a sede da Fundação Cultural Palmares;

## 3. Área requisitante

| Área Requisitante | Responsável |
|---|---|
| COPTI | Ivanildo Feliciano da Silva |

## 4. Necessidades de Negócio

**Necessidade 1:** Garantir disponibilidade aos serviços internos de TI

Equipamentos com garantia técnica e suporte técnico on-site

**Necessidade 2:** Atualização e Modernização das soluções de segurança.

Reduzindo o risco de indisponibilidade na rede da FCP.

**Necessidade 3:** Deverá fornecer Console de Gerenciamento para controle e operacionalização, além de controle de políticas, para cada tipo de módulo de segurança contratado.

**Necessidade 4:** Deverá permitir a instalação das licenças ou agentes em servidores, estações de trabalho e máquinas virtualizadas, via console de gerenciamento, com opção de remoção de soluções antivírus previamente instaladas;

**Necessidade 5:** Deverá possui painel de controles dashboard com acompanhamento e monitoramento em tempo real do status de cada endpoint.

**Necessidade 6**: As licenças fornecidas devem ser por subscrição e deverão permanecer ativas na vigência do contrato.

## 5. Necessidades Tecnológicas

5.1 Detecção de malware: A solução precisa ter a capacidade de identificar e bloquear diferentes tipos de malware, como vírus, worms, trojans, ransomware e outros softwares maliciosos. Isso pode envolver a utilização de assinaturas de malware, análise heurística, detecção de comportamento malicioso e aprendizado de máquina.

5.2 Atualizações de definições: É importante que a solução seja atualizada regularmente com as últimas definições de malware. Isso garante que ela possa reconhecer e combater as ameaças mais recentes.

5.3 Proteção de Endpoint e servidores: Soluções de proteção de servidores devem fornecer recursos como detecção e prevenção de intrusões, firewall de host, controle de acesso a aplicativos e serviços, além de auditoria e registro de eventos para monitorar atividades suspeitas e proteger os servidores contra-ataques.

5.4 Proteção de armazenamento: Soluções de proteção de armazenamento (storage) devem garantir a segurança dos dados armazenados. Isso pode incluir criptografia de dados em repouso, detecção de intrusões, controle de acesso baseado em função, backups e recuperação de dados, além de auditoria de eventos relacionados ao armazenamento.

5.5 Integração com plataformas e sistemas: É importante que as soluções de segurança possam ser integradas com as plataformas e sistemas existentes na infraestrutura de TI, como sistemas operacionais, servidores de e-mail, firewalls de rede, switches e roteadores. A integração permite uma maior visibilidade e controle sobre as ameaças e atividades maliciosas.

5.6 Gerenciamento centralizado: Uma necessidade importante é a capacidade de gerenciar todas as soluções de segurança a partir de uma única interface centralizada. Isso facilita a configuração, monitoramento e geração de relatórios, além de permitir uma resposta mais rápida a ameaças e incidentes de segurança.

5.7 Relatórios e auditoria: A solução de segurança deve oferecer recursos de geração de relatórios e auditoria para acompanhar a eficácia das medidas de proteção implementadas, identificar áreas de melhoria e atender aos requisitos de conformidade regulatória

5.8 Deve ser fácil de configurar e gerenciar.

5.9 Deve ter recursos avançados de segurança, incluindo criptografia de dados e autenticação de usuários.

## 6. Demais requisitos necessários e suficientes à escolha da solução de TIC

| Demais requisitos necessários e suficientes à escolha da solução de TIC | |
|---|---|
| | |

| | |
|---|---|
| 1 | **Possuir alta disponibilidade**. É um sistema resistente a falhas de hardware e software, cujo objetivo é manter os serviços disponibilizados o máximo de tempo possível. |
| 2 | **Possuir escalabilidade**. É a característica que indica a capacidade de crescer atendendo às demandas sem perder as qualidades que lhe agregam valor |
| 3 | **Possuir confiabilidade**. É a capacidade do sistema de realizar e manter seu funcionamento em circunstâncias de rotina, bem como em circunstâncias hostis e inesperadas |
| 4 | **Desempenho**. É a performance esperada em um sistema de computação para respostas de seus sistemas. |
| 5 | **Gerenciamento centralizado**. É a possibilidade de gerenciar todos os softwares de forma centralizada, possibilitando um maior controle do ambiente. |

### 6.1 Requisitos de Capacitação

6.1.1 A Contratada deverá realizar o repasse de conhecimento aos funcionários da contratante que atuarão, diretamente, com a solução de segurança e conectividade adquirida, abrangendo todas as informações necessárias a sua operacionalização, disponibilizando materiais em mídias digitais, apostilas e outros recursos em português brasileiro.

### 6.2 Requisitos de Manutenção

6.2.1 O Suporte deverá ser especializado, podendo ser executado remotamente ou localmente dependendo da criticidade. A avaliação do chamado quanto a criticidade será feita pela FCP;

6.2.2 A documentação produzida durante a execução dos serviços, seja em papel ou meio eletrônico, será de propriedade da FCP, e não deverá ser divulgado sem sua expressa autorização.

### 6.3 Requisitos de Segurança

6.3.1 A solução que será implantada deve atender as recomendações da Política de Segurança da Informação e demais normativos da FCP.

### 6.4 Requisitos Legais

6.4.1 A presente contratação sujeita-se à legislação pertinente, mormente aos diplomas a seguir elencados, bem como às demais normas gerais que se apliquem, considerando-se a legislação consolidada com as respectivas alterações subsequentes:

6.4.1.1 Lei nº 9.609, de 19 de fevereiro de 1998:

Art. 12. Violar direitos de autor de programa de computador:

Pena - Detenção de seis meses a dois anos ou multa.

§ 1º Se a violação consistir na reprodução, por qualquer meio de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena - Reclusão de um a quatro anos e multa.

§ 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

§ 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:

I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa público, sociedade de economia mista ou fundação instituída pelo poder público;

II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.

§ 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

6.4.1.2 Lei nº 9.610, de 19 de fevereiro de 1998:

Art. 102. O titular cuja obra seja fraudulentamente reproduzida, divulgada ou de qualquer forma utilizada, poderá requerer a apreensão dos exemplares reproduzidos ou a suspensão da divulgação, sem prejuízo da indenização cabível.

6.4.1.3 Lei Nº 14.133, de 1º de Abril de 2021 - Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;

6.4.1.4 Lei Federal n° 12.813/2013: dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego;

6.4.1.5 Lei Federal nº 12.846/2013: dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências;

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

6.4.1.7 Decreto n° 9.507, de 21 de setembro de 2018 - Dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta,

autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;

6.4.1.8 Instrução Normativa SEGES/ME Nº 65, DE 7 de Julho de 2021.

6.4.1.9 Aplicação subsidiária da Instrução Normativa nº 5, de 26 de maio de 2017 – Dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública Federal Direta, Autárquica e Fundacional;

6.4.1.10 Aplicação da Instrução Normativa GSIPR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal e suas Normas Complementares, em especial a Norma Complementar Nº 14/IN01/DSIC/GSIPR, de 19 de março de 2018, que estabelece princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem;

6.4.1.11 Aplicação da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados

**6.5 Requisitos Temporais**

6.5.1 O prazo de vigência do contrato é de 12 (doze) meses, podendo ser prorrogado por interesse das partes até o limite de 60 (sessenta) meses, com base no artigo 105, da Lei 14.133, de 2021, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos:

6.5.1.1 Os serviços tenham sido prestados regularmente;

6.5.1.2 A Administração mantenha interesse na realização do serviço;

6.5.1.3 O valor do contrato permaneça economicamente vantajoso para a Administração;

6.5.1.4 A CONTRATADA manifeste expressamente interesse na prorrogação.

6.5.1.5 A reunião inicial de alinhamento deverá ocorrer após a assinatura do contrato e ser executada em, no máximo, 5 (cinco) dias corridos após a assinatura do contrato.

6.5.1.6 O prazo de entrega para os documentos que comprovem o fornecimento do licenciamento e todas as demais obrigações deverão ser disponibilizadas à CONTRATANTE no prazo máximo de 30 (trinta) dias corridos a serem contados a partir da abertura da Ordem de Fornecimento de bens/Serviço.

**6.6 Requisitos de Projetos e de Implementação**

6.6.1 Na reunião inicial a contratada deverá apresentar o projeto de implementação das licenças, fornecimento de equipamentos e da prestação dos serviços de manutenção/suporte.

6.6.2 O projeto deverá contemplar a instalação das versões dos softwares nas versões mais estáveis e que mitiguem os riscos de vulnerabilidades das estações de

trabalho de usuários e servidores de rede. Todos os custos referentes aos softwares que forem alocados em NUVEM, devem ser mantidos pela CONTRATADA, tais como consoles e servidores.

### 6.7 Requisitos de Garantia e de Manutenção

6.7.1 Contratada deverá fornecer garantia da solução pelo prazo de 36 (trinta e seis) meses, contados a partir da data da emissão do Termo de Recebimento, não se limitando ao término da vigência contratual.

6.7.2 A garantia deverá prover, obrigatoriamente:

6.7.2.1 Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas; 6.7.2.2 Atualização dos softwares fornecidos, se houver lançamento de novos softwares em substituição aos fornecidos, ou se, mesmo não se tratando de substituição, ficar caracterizada descontinuidade dos softwares fornecidos;

6.7.2.3 Correções dos softwares fornecidos (patches), incluindo a correção de eventuais falhas (bugs) de software que prejudiquem o ambiente de produção ou vulnerabilidades que comprometam a segurança da solução;

6.7.2.4 A garantia deverá ser prestada durante todo o período de contrato e aditivos relativos às atualizações das licenças e proteção. Garantia para hardware durante o período do contrato;

6.7.2.5 Atualização do sistema operacional embarcado durante o período do contrato.

6.7.2.6 No preço deverá estar incluído todo o software necessário para atender as características exigidas, bem como as atualizações para todas as versões do produto que forem lançadas durante o período do contrato.

6.7.2.7 Os chamados de manutenção e suporte técnico deverão ser registrados em sistema provido pela CONTRATADA, e deverão estar disponíveis para acompanhamento em seu portal na internet.

6.7.2.8 A Contratada deve escalar o chamado para o suporte do fabricante sempre que necessário, seja devido à criticidade, impacto ou urgência do problema, como também caso o fabricante precise atuar no processo de correção.

6.7.2.9 Será disponibilizado canal de atendimento e chamado técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de site na Internet e/ou canal telefônico gratuito 0800;

6.7.2.10 Em caso de indisponibilidade do canal de atendimento disponibilizado, os chamados técnicos poderão ser abertos via e-mail, "website" do fabricante, telefone etc.;

6.7.2.11 O fornecedor deve informar página da Internet onde estejam disponíveis drivers atualizados, últimas versões do firmware e demais informações sobre detalhes técnicos dos equipamentos e/ou softwares, sem restrições de acesso público ou via cadastramento de pessoas autorizadas pelo CONTRATANTE para o acesso.

## 6.8 Requisitos de Segurança

6.8.1 A CONTRATADA deverá submeter-se à Política de Segurança da Informação e Comunicações e demais normas de segurança vigentes na CONTRATANTE.

6.8.2 Quanto ao acesso físico, a CONTRATADA:

6.8.2.1 Deverá credenciar junto à CONTRATANTE os seus profissionais, caso seja necessário o acesso às instalações da Sede da CONTRATANTE para prestação de serviços.

6.8.2.2 A CONTRATADA deverá apresentar os empregados devidamente uniformizados e identificados por meio de crachá.

6.8.2.3 Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca dos serviços, sem prévia autorização.

6.8.2.4 Observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação - TI da CONTRATANTE.

6.8.2.5 Será considerado ilícito a divulgação, o repasse ou utilização indevida de informações, bem como dos documentos, imagens, gravações e informações utilizados durante a prestação dos serviços.

6.8.2.6 Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer reprodução, utilização ou divulgação a terceiros, devendo a CONTRATADA zelar por si e por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados.

## 6.9 Requisitos de Experiência Profissional e de Formação da Equipe

6.9.1 A contratada deverá comprovar que possui em seu quadro permanente, profissional de nível superior ou outro devidamente reconhecido pela entidade competente, detentor de atestado de responsabilidade técnica por execução de serviço de características semelhantes com o objeto da contratação.

6.9.2 Requisitos de Metodologia de Trabalho O serviço de instalação deverá ser executado e supervisionado por pelo menos 1 (um) técnico certificado pelo fabricante da solução proposta.

6.9.3 A CONTRATADA deverá instalar os softwares e hardwares, com as licenças adquiridas.

6.9.4 Na reunião inicial, que marca o período de execução do contrato, deverá ser acordado entre a CONTRATANTE e a CONTRATADA os dias em que o engenheiro do fabricante realizará as tarefas prevista neste documento.

6.9.4 O preposto será responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto à CONTRATANTE.

6.9.5 Os equipamentos serão considerados recebidos de forma definitiva quando instalados nos respectivos ambientes, cabeados, configurados, operacionais, em plenas condições de funcionamento, integrados com a rede local e licenciados, bem como com outros equipamentos locais utilizados e com capacidade de permitir acesso remoto por parte da equipe da CONTRATANTE.

## 6.10 Requisitos Sociais, Ambientais e Culturais

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

6.10.2 Os profissionais da CONTRATADA que porventura desempenharem atividades em contato direto com a CONTRATANTE deverão:

6.10.2.1 Apresentar-se vestidos de forma adequada ao ambiente de trabalho físico ou virtual, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional da CONTRATANTE ou que ofenda o senso comum de moral e bons costumes;

6.10.2.2 Respeitar todos os servidores, funcionários e colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo;

6.10.2.3 Atuar no estabelecimento da CONTRATANTE com urbanidade e cortesia.

6.10.3 Não aplicação da Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010 - que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional pelo fato de ser tratar de contratação de licenças de software e de serviços especializados

## 6.11 Demais requisitos necessários e suficientes à escolha da solução de TIC

6.11.1 A Estratégia de Governança Digital - EGD do Governo Federal, oficializada por meio do Decreto nº 8.638, de 15 de janeiro de 2016, tem como um de seus objetivos estratégicos, garantir a segurança da informação e comunicação do Estado e o sigilo das informações do cidadão. Ela tem como um de seus princípios a segurança e privacidade que define que “os serviços públicos digitais devem propiciar disponibilidade, integridade, confidencialidade e autenticidade dos dados e

informações, além de proteger o sigilo e a privacidade pessoais dos cidadãos na forma da legislação".

6.11.2 Para alcançar o objetivo acima, para minimizar os riscos de incidentes de segurança e disponibilidade da informação, e ainda considerando que a infraestrutura atual de TIC não garante disponibilidade de 100% das aplicações/sistemas/portais é necessário utilizar-se de uma solução de proteção e segurança dos servidores da FCP.

6.11.3 O presente estudo visa a contratação de uma solução com objetivo principal de proteger as estações de trabalho e de ampliar as camadas de segurança para servidores e data center, tendo em vista os recorrentes incidentes de ataques avançados, bem como forma de precaução às novas ameaças decorrentes de malwares que invadem e criptografam informações.

6.11.4 A contratação em estudo tem o propósito de preservar as condições de manutenção da solução de antivírus da Fundação sem que haja pausa ou interrupção na proteção, requalificação dos analistas e técnicos da FCP já capacitados, bem como adicionar proteção específica para os servidores físicos e virtuais.

6.11.5 De forma objetiva, pretende-se com este processo, equipar a FCP com uma Solução completa, que vai desde a proteção de endpoint até a proteção contra ameaças avançadas, passando pela segurança e proteção se servidores físicos, virtuais e solução de conectividade, com gestão centralizada, aumentado o índice de proteção e integridade das informações a cargo da FCP.

## 7. Estimativa da demanda - quantidade de bens e serviços

7.1 Apresenta-se a seguir o quadro contendo o quantitativo da demanda a ser contratada:

| Item | CATMAT / CATSER | Descrição | Unidade | Qtde. |
|---|---|---|---|---|
| 1 | 27499 | Solução Segurança Avançada para Endpoints, com proteção integrada contra-ataques complexos, direcionados e descoberta avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a incidentes, bem como serviços em nuvem e zero day. | Und | 150 |
| 4 | 27022 | Serviços de Instalação | Und | 1 |
| | | | | |

| | | | | |
|---|---|---|---|---|
| 5 | 3840 | Treinamento Técnico | Turma | 1 |

### 7.2 Relação da quantidade estimada x quantidade necessária

7.2.1 Os quantitativos propostos para contratação foram definidos com base na análise do parque tecnológico da FCP.

7.2.2 A Fundação Cultural Palmares possui hoje aproximadamente 110 (cento e dez) estações de trabalho, as quais necessitam obrigatoriamente de proteção contra-ataques e uma infinidade de vírus, malwares e outras ameaças à segurança da informação.

7.2.3 Em relação aos equipamentos servidores, que suportam máquinas físicas e virtuais, a FCP possui 20 máquinas físicas e 20 máquinas virtuais. De forma semelhante às estações de trabalho, não se vislumbra a possibilidade de deixar servidores sem proteção, principalmente porque estes são o alvo principal dos cibercriminosos, visto que processam e armazenam todas as informações do órgão. Sendo assim, a quantidade necessária e a quantidade estimada também devem coincidir.

7.2.4 Quanto à proteção contra ameaças avançadas, trata-se de plataforma única, portanto, coincidindo a estimativa e a necessidade.

7.2.5 No que concerne ao serviço de suporte, o qual será prestado sobre as licenças contratadas, sua necessidade coincide obrigatoriamente com a quantidade de licenças. Portanto, a relação entre estimativa e necessidade é de uma para uma.

7.2.6 No tocante à transferência de conhecimento, e tendo em vista a necessidade de transparência e economicidade, o serviço será cotado e pago por aluno, de modo que o fornecedor execute e receba pelos serviços efetivamente prestados. A quantidade trata de uma estimativa máxima a ser executada durante o período de vigência do contrato.

## 8. Levantamento de soluções

8.1 Antes de buscar possíveis soluções/opções que atendam a demanda da Fundação Cultural Palmares, foi elencado, baseado nos tópicos anteriores, os itens que serão utilizados pesquisa.

8.2 Segue abaixo a consolidação das camadas a serem avaliadas:

8.2.1 Compreende a contratação de empresa especializada no fornecimento de licenças de software de solução de proteção de estações de trabalho e servidores de rede incluindo implantação da solução, treinamento, manutenção especializada e suporte técnico pelo período de 36 (trinta e seis) meses.

8.2.2 O software promove o aumento dos níveis de segurança no ambiente institucional. Refere-se ao objetivo de identificar e bloquear, em tempo real, ataques, invasões ou abusos direcionados ao ambiente institucional, de forma a reduzir os riscos relacionados à imagem institucional, perda de informações e descumprimento de normas e regulamentos. Visa também atender a necessidade de possuir uma infraestrutura mais robusta, necessária para atender às demandas institucionais, internas e externas, através da implementação de recursos de segurança da informação.

8.2.3 Softwares proprietários são programas licenciados, com direitos exclusivos para o produtor. O software, normalmente, é abrangido por patentes e direitos autorais. Os programas de proteção de estações de trabalho e servidores de rede, em sua maioria, são softwares desenvolvidos por empresas especializadas em segurança e que fornecem suporte técnico.

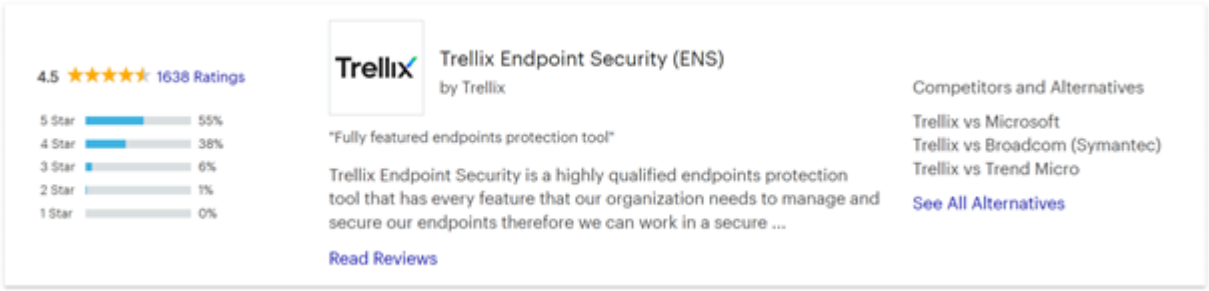
8.2.4 Para fins de levantamento de soluções disponíveis no mercado, considerando a solução de id 02, utilizou-se como parâmetro a pesquisa efetuada pelo GARTNER (empresa com atuação no ramo de pesquisas, consultorias, eventos e prospecções acerca do mercado de TI), o mercado de soluções de segurança para prevenção contra vazamento de informações apresenta diversos fabricantes e soluções conforme pode ser visto em levantamento anual acerca de soluções de segurança.

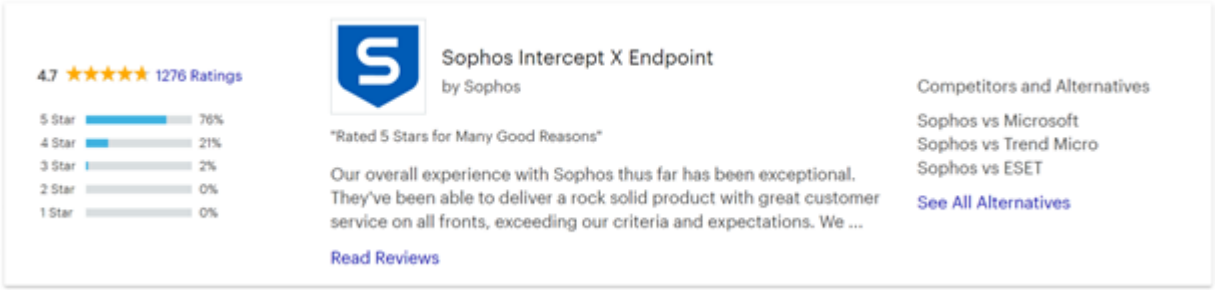
**8.3 Definição de proteção de estações de trabalho e servidores**:

8.3.1 Conjunto de soluções de segurança cibernética projetadas para detectar e responder a atividades suspeitas ou maliciosas em dispositivos finais, como computadores, laptops, servidores e dispositivos móveis. Essas soluções monitoram o comportamento dos endpoints em tempo real, coletam dados sobre atividades e podem responder automaticamente a ameaças ou fornecer informações para auxiliar nas investigações.

8.3.2 O Gartner avalia soluções que fornecem visibilidade do uso de dados em uma organização para um amplo conjunto de casos de uso e a aplicação dinâmica de políticas com base no conteúdo e contexto no momento de uma operação, abordando ameaças relacionadas a dados, incluindo os riscos de perda de dados inadvertida ou acidental, e a exposição de dados confidenciais usando monitoramento, filtragem, bloqueio e outros recursos de correção.

8.3.3 O estudo abaixo relaciona as alternativas existentes no mercado que se enquadram nas necessidades/benefícios elencadas pela Instituição:





| ESTUDO DE MERCADO | |
|---|---|
| | **TRENDMICRO**<br><br>Proteção em camadas defendendo contra-ataques persistentes e direcionados de ransomware e outros tipos malware de zero day;<br><br>Monitoramento e filtragem de remetentes maliciosos com diversas abordagens;<br><br>Proteção contra comprometimento de e-mail corporativo (BEC);<br><br>Análise dinâmica de sandbox para arquivos e URL / detecção de exploits;<br><br>Análise de conteúdo do e-mail usando uma variedade de técnicas para filtrar spam e phishing. |
| | |

| | |
|---|---|
| **Solução de proteção de estação de trabalho e servidores de rede** | **DARKTRACE**<br><br>Descoberta de dados, descoberta eletrônica e classificação de dados – automática, em tempo real;<br><br>Uso de inteligência artificial central para impedir as ameaças de e-mail mais avançadas, intervindo para proteger os funcionários de toda a gama de ameaças direcionadas à caixa de entrada; interrompe o spear phishing avançado e as falsificações digitais. |
| | **ESET**<br><br>Identifica ameaças avançadas e malwares sofisticados<br><br>Protege seus usuários em qualquer rede e dispositivo e detecta se uma mensagem foi armada após a entrega;<br><br>Identificação de funcionários de alto risco, identificando atividades que indicam furto de dados;<br><br>monitora os endpoints em tempo real, coletando dados sobre o comportamento dos dispositivos. Isso permite identificar atividades suspeitas assim que elas ocorrem, possibilitando uma resposta rápida<br><br>Resposta automatica a ameaças identificadas. |

Tabela – Estudo de Mercado.

8.3.5 As soluções de EDR (Endpoint Detection and Response) oferecem vantagens essenciais para a segurança cibernética. Elas garantem uma detecção avançada de ameaças, identificando comportamentos suspeitos em tempo real. Além disso, possibilitam respostas rápidas a incidentes, isolando ameaças e minimizando danos. A visibilidade aprimorada dos endpoints permite a identificação rápida de atividades anômalas, essencial para a segurança. As soluções de EDR também permitem investigações forenses detalhadas após incidentes, fornecendo informações cruciais para a análise de ataques.

8.3.6 Com a automação da detecção e resposta, o tempo de reação é reduzido, mitigando eficazmente o impacto dos ataques. Além disso, a proteção proativa e a conformidade regulatória são garantidas. A customização e escalabilidade das soluções de EDR permitem adaptação às necessidades específicas da organização. Sua integração com outras ferramentas de segurança fortalece a postura de defesa cibernética. Monitoramento contínuo assegura que ameaças em evolução sejam prontamente identificadas, protegendo a rede de forma abrangente.

### 8.4 Da existência de software público brasileiro

8.4.1 De acordo com a busca realizada no dia 07 de novembro de 2023, às 10:53, com as palavras chaves "EDR" e "Antivírus", o portal: softwarepublico.gov.br, retornou que não havia encontrado nenhum software correspondente.


## 9. Análise comparativa de soluções

9.1 A proteção física e lógica da informação deve ser provida por ferramentas especializadas, seguras, consolidadas e, acima de tudo, que preservem a confidencialidade, a integridade e a disponibilidade da informação.

9.2 Em observância ao disposto na Instrução Normativa SGD/ME IN SGD/ME nº 94 /2022, apresenta-se a seguir a avaliação de soluções e a capacidade de cada uma delas para atender aos requisitos de proteção de estações e servidores:

**Cenário 1**

| | |
|---|---|
| **Descrição** | Contratação de Solução Segurança Avançada para Endpoints, com proteção integrada contra-ataques complexos, direcionados e descoberta avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a incidentes, bem como serviços em nuvem e zero day.<br><br>De acordo com as necessidades levantadas e, após realização de estudos, somente uma solução de software proprietário atenderá as necessidades desta Fundação. |

| | |
|---|---|
| **Análise da Solução** | Trata-se da contratação de nova solução de mercado, desenhada "do zero", realizando investimento nas soluções.<br><br>Certamente configura-se uma alternativa válida. Cabe a cada um zelar pela boa aplicação dos parcos recursos, otimizando o seu uso, e promovendo ações no sentido de "fazer mais com menos".<br><br>Pelos motivos apresentados, **este cenário atende as necessidades da FCP.** |

**Cenário 2**

| | |
|---|---|
| **Descrição** | **Solução existente no portal de software público brasileiro.** |
| **Análise da Solução** | Trata-se da utilização das soluções disponíveis no Portal do Software Público, para atendimento da necessidade posta.<br><br>Em consulta Portal do Software Público (https://www.gov.br/governodigital/pt-br/software-publico/catalogo/catalogo), não foram identificados softwares com as características necessárias à solução desejada. Portanto, para o fornecimento das licenças, suporte técnico, garantia e atualização, não é possível a utilização de software público. É necessária a contratação de empresa especializada na solução.<br><br>Pelo motivo apresentado, **este cenário não é recomendado, por não atender as necessidades do FCP.** |

**Cenário 3**

| | |
|---|---|
| **Descrição** | **Desenvolvimento próprio da Fundação através de contratos com empresas especializadas na prestação do serviço de desenvolvimento de ferramentas e, para o atendimento das necessidades.**<br><br>Trata-se do desenvolvimento internamento na FCP, por intermédio de contratos de fábrica de software, de uma solução de segurança similar à que se pretende contratar. |

Uma solução desta monta seria fatalmente inviável e altamente custosa de ser desenvolvida internamente na FCP ou por meio de contrato de serviço.

Além disso, em se tratando da possibilidade de desenvolvimento de uma nova solução com a utilização da fábrica de software contratada, vale a pena destacar que o então Ministério do Planejamento, Orçamento e Gestão, através da Secretaria de Tecnologia da Informação, orienta na publicação *"Boas práticas, vedações e orientações para contratação de serviços de desenvolvimento e manutenção de software (Fábrica de Software)"*, disponível em desenvolvimento e manutenção de software, o seguinte:

1. Antes de decidir ... pela abertura de projetos de desenvolvimento de software, a Equipe de Planejamento da Contratação ou a Equipe de Gestão de Projetos do órgão deve realizar Estudo Técnico Preliminar, nos termos do disposto no art. 12 da Instrução Normativa SLTI/MP nº 4, de 11 de setembro de 2014, e executar as seguintes atividades:

**Análise da Solução**

...

1.5. Analisar a viabilidade de contratação de software proprietário.

...

2.5. É vedada a utilização dos serviços contratados para o desenvolvimento de softwares de atividades meio.

2.5.1. São considerados softwares de atividades meio os que são utilizados para apoio de atividades de gestão ou administração operacional, como, por exemplo, softwares de recursos humanos, ponto eletrônico, portaria, biblioteca, gestão de patrimônio, controle de frotas, gestão eletrônica de documentos, e não têm por objetivo o atendimento às áreas finalísticas para a consecução de políticas públicas ou programas temáticos.

2.5.2. Os softwares de atividades meio devem ser adquiridos no mercado por meio de adoção de software público ou livre, contratação de software como serviço, ou software licenciado.

O desenvolvimento de uma solução para atender ao objetivo desse estudo está alinhada à vedação exposta no item 2.5 da orientação citada acima. Diante do exposto, não é recomendado o desenvolvimento interno de uma solução desta monta. Além do mais, importante destacar que o custo-benefício para

desenvolvimento interno de uma solução deste tipo com todas as funcionalidades necessárias não seria viável técnica e economicamente.

Pelos motivos apresentados, **este cenário não é recomendado, por não atender as necessidades da ANTAQ.**

**Observância das alternativas às políticas, premissas e especificações técnicas vigentes**

| Requisito | ID do cenário | SIM | NÃO | NÃO SE APLICA |
|---|---|---|---|---|
| A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal? | 1 | X | | |
| | 2 | | X | |
| | 3 | | X | |
| A Solução está disponível no Portal do Software Público Brasileiro? | 1 | | X | |
| | 2 | | X | |
| | 3 | | X | |
| A Solução é um software livre ou software público? | 1 | | X | |
| | 2 | X | | |
| | 3 | X | | |
| A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG? | 1 | X | | |
| | 2 | X | | |
| | 3 | X | | |
| | 1 | | | X |

| | | |
|---|---|---|
| A Solução é aderente às regulamentações da ICPBrasil? (quando houver necessidade de certificação digital) | 2 | X |
| | 3 | X |
| A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos) | 1 | X |
| | 2 | X |
| | 3 | X |

## 10. Registro de soluções consideradas inviáveis

10.1 Conforme previsto no § 1º do art. 11 da IN SGD 94/2022, as soluções identificadas e consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação (breve descrição e justificativa), dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

10.2 De acordo com os estudos detalhados, são consideradas soluções inviáveis:

10.2.1 Solução existente no portal de software público brasileiro; e Desenvolvimento interno de uma Solução.

## 11. Análise comparativa de custos (TCO)

11.1 Considerando-se os valores obtidos na pesquisa de preços e consolidados supracitada, apresenta-se a seguir os custos totais de propriedade do licenciamento.

1. 1.1. **MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)**

| Item | Descrição | ANO 1 | ANO 2 | ANO 3 | TOTAL |
|---|---|---|---|---|---|
| | Solução Segurança Avançada para Endpoints, com proteção integrada contra-ataques complexos, direcionados e descoberta | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 1 | avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a incidentes, bem como serviços em nuvem e zero day | **R$** 307.850,00 | **R$** 0,00 | **R$** 0,00 | **R$** 307.850,00 |
| 4 | Instalação e Configuração | **R$** 53.000,00 | **R$** 0,00 | **R$** 0,00 | **R$** 53.000,00 |
| 5 | Treinamento | **R$** 34.000,00 | **R$** 0,00 | **R$** 0,00 | **R$** 38.000,00 |
| | **VALOR TOTAL** | **R$ 394.875,00** | **0,00** | **R$** 0,00 | **R$ 398.875,00** |

## 12. Descrição da solução de TIC a ser contratada

12.1 O objeto proposto para a contratação constitui a Solução Segurança Avançada para Endpoints, com proteção integrada contra-ataques complexos, direcionados e descoberta avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a incidentes, bem como serviços em nuvem e zero day, para atendimento quantitativo e qualitativo da demanda atual, provendo ao uma melhoria significativa da segurança e controle de acesso à informação sob sua responsabilidade, conforme condições, quantidades e exigências estabelecidas neste estudo técnico.

12.2 Considerando, pois, a situação atual da FCP, e no intuito de assegurar a conectividade e gerência o nível de proteção adequada aos sistemas computacionais, conclui-se que a solução proposta no Cenário 1 – **Contratação de solução** se mostra mais completa e viável à situação presente, tendo em vista todo o exposto neste ETP, cujos itens e quantitativos foram consolidados na tabela acima.

### 12.3 Justificativa da solução escolhida

12.3.1 A infraestrutura de tecnologia da informação da FCP conta com um aparato tradicional de segurança, destinado ao controle das comunicações entre redes e ao permissionamento de acesso a recursos, serviços e dados, e Segurança Avançada para Endpoints, com proteção integrada contra-ataques complexos, direcionados e descoberta avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a incidentes, bem como serviços em nuvem Tais dispositivos, contudo, não garantem proteção contra infecção por malware, captura de informações privadas ou sigilosas, acesso indevido a serviços de rede por usuário não autorizado, dentre outras vulnerabilidades.

12.3.2 Em resposta à sofisticação crescente das formas de ataque aos ambientes de tecnologia da informação, foram desenvolvidas novas estratégias de combate que

agregam diferentes mecanismos de proteção em plataformas integradas de segurança. Tais plataformas visam complementar as ferramentas de segurança de perímetro, com programas instalados e executados diretamente nas estações de trabalho, *notebooks* e servidores de rede. O mercado convencionou chamar essas plataformas de "*Endpoint Security*", expressão que poderia ser traduzida livremente para o português como "solução de segurança para as extremidades da rede". Entende-se aqui como "extremidade" os pontos de conexão à rede que estão nas extremidades de sua capilaridade, ou seja, conectados aos *switches* de distribuição e aos *switches*"*topo de rack*".

12.3 3 Trata-se de uma abordagem voltada às ameaças que privilegiam o ataque direto a esses computadores: contaminação por malware, intrusão em estação de trabalho, acesso indevido ou não autorizado a recursos de rede. Mais que isso, as soluções de segurança de *Endpoint* apresentam uma console integrada para todas essas ferramentas, o que permite a criação e aplicação de políticas de segurança de *Endpoint* em nível corporativo envolvendo todas essas disciplinas citadas.

12.3.4 O estudo aqui proposto almeja avaliar uma solução que integre e consolide todo o licenciamento, sob console de gerenciamento única.

12.3.5 Seguindo as boas práticas de gerenciamento de segurança, todos os componentes devem ser de um mesmo fabricante e geridos sob console(s) de gerenciamentos desse mesmo fabricante. Não se deve aceitar soluções que congregam componentes de diversos fabricantes distintos, posto que isso atenta contra a integração e estabilidade da solução como um todo.

12.3.6 A forma de contratação aqui proposta é comumente utilizada na Administração Pública Federal, por possuir grandes vantagens como preservação do investimento já realizado, redução de custos com aquisição de plataformas diversa e com integração de ferramentas, otimização da força de trabalho, com gerenciamento único e centralizado.

12.3.7 Apresentam-se a seguir algumas contratações de órgãos públicos federais, feitas no mesmo formato aqui proposto:

| **Órgão** |
|---|
| MTE – Pregão 01/2022 |
| PRODAM – Pregão 05/2023 |
| MP-MT – Pregão 072/2023 |
| FUNASA – Pregão 02/2022 |

| NORMA: INSTRUÇÃO NORMATIVA Nº 73, DE 5 DE AGOSTO DE 2020<br>Nº PROCESSO:<br>PREENCHER APENAS OS PARÂMETROS I, II, III E IV. | | | QTD | Parâmetro I - PAINEL DE PREÇOS<br>https://paineldeprecos.planejamento.gov.br/ | Preços Públicos | | | | Parâmetro IV - FORNECEDORES | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Fornecedor 1 | Fornecedor 2 | Fornecedor 3 |
| ITEM | PRODUTO/SERVIÇO | Unidade/período | | Valor unitário | Valor unitário | Valor unitário | Valor unitário | Valor unitário | Valor unitário | Valor unitário | Valor unitário |
| | | | | | MTE Pregão 01/2022 | FUNASA - Pregão 2/2022 | Prodam Pregão 05/2023 | MP-MT pregão 072/2023 | | | |
| 1 | Solução de software de segurança de estação de trabalho e servidores para 36 meses | UND | 150 | | R$ 580,00 | | R$ 230,00 | R$ 1.065,00 | R$ 3.040,00 | R$ 3.315,00 | R$ 3.102,20 |
| 2 | Instalação e configuração | UND | 1 | | | R$ 45.000,00 | | R$ 64.800,00 | R$ 53.000,00 | R$ 55.000,00 | R$ 45.000,00 |
| 3 | Repasse de Conhecimento | TURMA | 1 | | R$ 15.200,00 | R$ 43.998,00 | | R$ 44.200,00 | R$ 33.000,00 | R$ 35.000,00 | R$ 41.000,00 |
| Valor Total | | | | | | | | | | | |

| Metodologia: Média Simples<br>(normalmente é utilizada quando os dados estão dispostos de forma homogênea) | | | Metodologia: Média + Desvio Padrão<br>(média simples + metodologia complementar para desconsiderar os valores inexequíveis e os excessivamente elevados) | | | | | | | Metodologia: Mediana<br>(menos influenciada por valores muito altos ou muito baixos, a mediana pode ser adotada em casos onde os dados são apresentados de forma mais heterogênea e com um número pequeno de observações. Com o seu uso, entende-se que não é necessário usar metodologia complementar para desconsideração dos valores inexequíveis/excessivamente elevados) | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Número de preços para o item | MÉDIA SIMPLES (unitária) | VALOR TOTAL - média simples x qtd | DESVIO PADRÃO | Menor valor a considerar (MÉDIA - DP) | Maior valor a considerar (MÉDIA + DP) | Soma dos valores dentro do intervalo | Número de preços válidos dentro do intervalo | MÉDIA + DESVIO PADRÃO (unitária) - desconsiderados os inexeq./excessiv. elevados | VALOR TOTAL - média x qtd | Número de preços para o item | MEDIANA (unitária) | VALOR TOTAL - mediana x qtd |
| 6 | R$ 1.888,70 | R$ 283.305,00 | R$ 1.289,37 | R$ 599,33 | R$ 3.178,07 | R$ 7.207,20 | 3 | R$ 2.402,40 | R$ 360.360,00 | 6 | R$ 2.052,50 | R$ 307.875,00 |
| 5 | R$ 52.560,00 | R$ 52.560,00 | R$ 7.352,17 | R$ 45.207,83 | R$ 59.912,17 | R$ 108.000,00 | 2 | R$ 54.000,00 | R$ 54.000,00 | 5 | R$ 53.000,00 | R$ 53.000,00 |
| 6 | R$ 35.399,67 | R$ 35.399,67 | R$ 9.972,34 | R$ 25.427,32 | R$ 45.372,01 | R$ 197.198,00 | 5 | R$ 39.439,60 | R$ 39.439,60 | 6 | R$ 38.000,00 | R$ 38.000,00 |
| 17 | R$ 89.848,37 | R$ 371.264,67 | R$ 18.613,88 | R$ 71.234,48 | R$ 108.462,25 | R$ 312.405,20 | 10 | R$ 95.842,00 | R$ 453.799,60 | 17 | R$ 93.052,50 | **R$ 398.875,00** |

Especificação dos Produtos

| Item | Descrição | QTD | Métrica |
|---|---|---|---|
| **1** | Solução Segurança Avançada para Endpoints, com proteção integrada contra-ataques complexos, direcionados e descoberta avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a incidentes, bem como serviços em nuvem e zero day | 150 | Unidade |
| **2** | Instalação e Configuração | 1 | Unidade |
| **3** | Treinamento | 1 | Turma |

## 13. Estimativa de custo total da contratação

**Valor (R$):** 398.875,00

13.1 Considerando a pesquisa de preços realizada, apresenta-se a seguir o valor estimado para a contratação:

| Item | Descrição | QTD | Métrica | TOTAL |
|---|---|---|---|---|
| **1** | Solução Segurança Avançada para Endpoints, com proteção integrada contra-ataques complexos, direcionados e descoberta avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a incidentes, bem como serviços em nuvem e zero day | 150 | Unidade | R$ 307.875,00 |
| **4** | Instalação e Configuração | 1 | Unidade | R$ 53.000,00 |
| **5** | Treinamento | 1 | Turma | R$ 38.000,00 |
| **VALOR TOTAL ESTIMADO:** | | | | **R$ 398.875,00** |

13.2 O valor estimado da contratação para 36 (trinta e seis) meses é de **trezentos e noventa e oito mil e oitocentos e setenta e cinco reais.**

## 14. Justificativa técnica da escolha da solução

14.1 A FCP analisou as soluções relacionadas e concluiu que todas as soluções que atendam aos macros itens possuem os requisitos técnicos necessários para atender às necessidades do órgão. Desta forma, será escolhida a solução mais vantajosa para a Administração Pública e que atenda todos os requisitos solicitados.

14.2 Com esta contratação a FCP pretende alcançar os seguintes benefícios:

- Prover níveis adequados de segurança à rede de dados da FCP; Assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações;
- Aumento da eficiência contra as vulnerabilidades, segurança, proteção e autenticidade de dados sensíveis da organização;
- Possibilitar a identificação e o rastreamento das tentativas de invasão à rede;
- Proteção, autenticidade e acessibilidade as informações;
- Resolução remota de incidentes de segurança;
- Atualização, manutenção tecnológica e suporte com vistas a atender às novas características técnicas e operacionais da infraestrutura de Tecnologia da Informação Ampliação dos serviços de segurança;
- Maior integração entre as diversas ferramentas (softwares e hardwares) de segurança;

- Atualização tecnológica dos recursos humanos envolvidos na área de segurança (treinamentos);
- Proteção as redes das unidades anexas a FCP.
- Implementação de regras e políticas de segurança no que se refere ao uso da rede de dados;
- Filtrar conteúdo, com a capacidade de analisar em tempo real o acesso à internet, permitido ou bloqueando sites de acordo com a categoria; e
- Permitir a emissão de relatório de acesso, evitando o anonimato na rede e assegurando a boa utilização da internet.

## 14.3 **DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS**

14.3.1 Com o objetivo de ampliar a competitividade e gerar mais economia, a Lei Nº 14.133, de 1º de Abril de 2021 estabeleceu em seu art. 40º, §2º, a aplicação do princípio do parcelamento, referente às compras, deverão ser considerados:

- A viabilidade da divisão do objeto em lotes;
- O aproveitamento das peculiaridades do mercado local, com vistas à economicidade, sempre que possível, desde que atendidos os parâmetros de qualidade; e
- O dever de buscar a ampliação da competição e de evitar a concentração de mercado.

14.3.2 Em seu §3º, o parcelamento não será adotado quando:

- A economia de escala, a redução de custos de gestão de contratos ou a maior vantagem na contratação recomendar a compra do item do mesmo fornecedor;
- O objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido;

14.3.3 O processo de padronização ou de escolha de marca levar a fornecedor exclusivo. Ocorre que o raciocínio de parcelamento ou adjudicação por itens não deve ser levado a termos absolutos, pois a divisão da pretensão contratual, em alguns casos, pode prejudicar a economia de escala e gerar outros custos relacionados aos diversos contratos, além de potencializar riscos e dificuldades na gestão de uma pluralidade de contratos autônomos para atendimento da mesma pretensão contratual;

14.3.4 O Tribunal de Contas da União - TCU já entendeu que seria legítima a reunião de elementos de mesma característica, quando a adjudicação de itens isolados onerar "o trabalho da administração pública, sob o ponto de vista do emprego de recursos humanos e da dificuldade de controle, colocando em risco a economia de escala e a

celeridade processual" (Acórdão 5301/2013 - Segunda Câmara. Rel. Ministro André Luís de Carvalho);

14.3.5 Os serviços que compõem o objeto desta contratação são um conjunto indissociável, de mesma natureza e relação entre si, o que torna seu parcelamento em itens técnica e economicamente inviável. A adjudicação dos itens à empresas /instituições distintas, além de aumentar seu custo administrativo, poderia trazer prejuízos à qualidade e à unidade dos serviços prestados, na medida em que eventuais falhas de um contrato poderiam ser por ele imputadas às atividades desenvolvidas por outro, dificultando a atividade fiscalizadora da administração pública e incorrendo em alto risco de indisponibilidade da solução que é de extrema importância para a Fundação Cultural Palmares.

## 15. Justificativa econômica da escolha da solução

15.1 A pesquisa de preços leva em consideração os preços publicados na administração pública federal junto a fornecedores e contratações similares. Após a pesquisa foi considerado o MENOR valor encontrado para padronização dessa contratação. Buscando assim o melhor uso dos recursos financeiros.

## 16. Benefícios a serem alcançados com a contratação

- Prover níveis adequados de segurança à rede de dados do FCP;
- Assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações; Aumento da eficiência contra as vulnerabilidades, segurança, proteção e autenticidade de dados sensíveis da organização;
- Possibilitar a identificação e o rastreamento das tentativas de invasão à rede;
- Proteção, autenticidade e acessibilidade as informações;
- Resolução remota de incidentes de segurança;
- Atualização, manutenção tecnológica e suporte com vistas a atender às novas características técnicas e operacionais da infraestrutura de Tecnologia da Informação Ampliação dos serviços de segurança;
- Maior integração entre as diversas ferramentas (softwares e hardwares) de segurança;
- Atualização tecnológica dos recursos humanos envolvidos na área de segurança (treinamentos);
- Proteção as redes das unidades anexas do FCP.
- Implementação de regras e políticas de segurança no que se refere ao uso da rede de dados;
- Filtrar conteúdo, com a capacidade de analisar em tempo real o acesso à internet, permitido ou bloqueando sites de acordo com a categoria; e
- Permitir a emissão de relatório de acesso, evitando o anonimato na rede e assegurando a boa utilização da internet.

# 17. Providências a serem Adotadas

## 17.1 Necessidades de adequação do ambiente para execução contratual

17.1.1 Adequação de infraestrutura de TI.

17.1.2 Preparação e disponibilização de ambiente virtual adequado para receber a solução.

## 17.2 Recursos necessários à continuidade do negócio durante e após a execução do contrato

### 17.2.1 Recursos humanos

17.2.1.1 Os recursos humanos internos a serem alocados se referem aos fiscais técnico, administrativo e gestor do contrato que devem realizar suas atividades de acompanhamento e controle, conforme definido na IN nº 01/2019.

17.2.1.2 Técnico da contratada de Sustentação de Ambiente de TIC.

17.2.1.3 Servidores da FCP serão alocados para realização de definições, acompanhamento e gerência da solução.

### 17.2.2 Recursos Materiais

| Recurso | Quantidade Necessária | Disponibilidade | Ação | Respo |
|---|---|---|---|---|
| ede lógica e elétrica | Mensurado de acordo com a solução adquirida e com o posicionamento físico do servidor (Gerente) da Solução | Integral | Solicitar junto à contratada | via contr manuten rede elét lógica |
| | Sob demanda, sendo que | | | Empresa prestado serviços operacio TI (respo |

| | | | | |
|---|---|---|---|---|
| ost virtualizado para ospedar a aplicação ervidora ou gerência entralizada das oluções de antivírus | serão no mínimo dois servidores de aplicação e um para gerência, para a solução | Integral | Abertura de OS para implementação pelas empresas envolvidas | pelo amb virtualiza conjunto contrata implanta solução, acompar da DTI |
| | Dimensionado pela licitante de acordo com a especicação mínima da solução | Integral | Abertura de OS para implementação pelas empresas envolvidas | Solução acompar da DTI |
| anuais técnicos do suário e de ferência, contendo das as informações obre o produto com s instruções para stalação, onguração, operação administração da olução. | Documentação técnica referente à solução adquirida | Integral | Documentação exigida na contratação da Solução | Empresa vencedo certame fornecim solução |

### 17.3 Estratégia de continuidade contratual

17.3.1 Para assegurar a continuidade da solução, acionar-se-á as seguintes ações para os eventos apresentados na tabela abaixo.

| Evento | Ação Preventiva | Responsáveis | Ação de Contingência | Responsáve |
|---|---|---|---|---|
| Inexecução do Contrato | Fiscalização adequada dos níveis de serviço | DTI | Acionamento contratual | Gestor do Contrato |
| | Realização de processo | | | |

| | | | | |
|---|---|---|---|---|
| Encerramento ordinário do contrato | de renovação tempestiva. | Gestor do Contrato | Prorrogação do ajuste | DTI |
| Encerramento sem possibilidade de renovação. | Realizar novo planejamento. | DTI | Realizar novo processo de planejamento e contratação dos serviços. | DTI |

## 18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

### 18.1. Justificativa da Viabilidade

Esta equipe de planejamento declara esta contratação

## 19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

**IVANILDO FELICIANO DA SILVA**

Coordenador de T.I

*Assinou eletronicamente em 10/11/2023 às 11:41:25.*