MINISTÉRIO DAS COMUNICAÇÕES

TERMO DE REFERÊNCIA

Solução Antivírus

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

1 – OBJETO DA CONTRATAÇÃO

1.1 Registro de Preços para eventual aquisição de solução de next generation antimalware, com gerenciamento centralizado, análise forense, detecção e respostas a incidentes, para atender às necessidades do Ministério das Comunicações – MCOM.

2 – DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1 Contratação de empresa para a aquisição de solução de next generation antimalware, com gerenciamento centralizado, análise forense, detecção e respostas a incidentes.

2.2 A solução que se pretende adquirir deve ser moderna e capaz de identificar e combater ameaças avançadas no nível de estações de trabalho e servidores de rede, além de possibilitar controle granular e visibilidade no tráfego da rede corporativa. Desta forma, sendo possível agir de forma proativa, ao invés de reativa, bloqueando ataques de ameaças do dia zero, ransomwares, dentre outros.

2.3 A contratação deverá englobar instalação da solução, com configuração e repasse de conhecimento, além do serviço de gerenciamento e suporte da solução, sendo os dois últimos por um período de 36 (trinta e seis) meses.

2.4 Bens e serviços que compõem a solução

GRUPO	ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE PREVISTA
1	1	Solução de Next Generation Antimalware com gerenciamento centralizado, análise forense, detecção e respostas a incidentes	Licenças	1.300
	2	Instalação e configuração	Serviços	1.300
	3	Serviço de instalação do gerenciamento centralizado e repasse de conhecimento	Serviços	1
	4	Serviço de gerenciamento e suporte da solução por 36 meses	Serviços Mensal	36

3 – JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

3.1.1 A partir da publicação da Medida Provisória nº 980, de 10 de junho de 2020, o Ministério das Comunicações – MCOM foi criado e o então Ministério da Ciência, Tecnologia, Inovações e Comunicações – MCTIC, extinto. As competências do MCOM abrangem as seguintes áreas:

I - política nacional de telecomunicações;

II - política nacional de radiodifusão;

III- serviços postais, telecomunicações e radiodifusão;

IV-política de comunicação e divulgação do Governo Federal;

V- relacionamento do Governo Federal com a imprensa regional, nacional e internacional;

VI - convocação de redes obrigatórias de rádio e televisão;

VII- pesquisa de opinião pública; e

VIII- sistema brasileiro de televisão pública.

3.1.2 O **Decreto nº 10.747, de 13 de julho de 2021** aprovou a estrutura regimental do MCOM, sendo este composto pelas seguintes Secretarias:

a) Secretaria de Radiodifusão - SERAD;

b) Secretaria de Telecomunicações - SETEL;

c) Secretaria Especial de Comunicação Social – SECOM;

c.1) Secretaria de Publicidade e Promoção - SEPUP;

c.2) Secretaria de Comunicação Institucional - SECOM; e

d) Secretaria Executiva - SEXEC.

3.1.3 A aquisição de licenças de solução corporativa de antivírus possui como intuito previnir a contaminação por vírus, malwares e suas variantes nos computadores e servidores do MCOM, que podem colocar em risco o sigilo, a integridade e a disponibilidade das informações.

3.1.4 Devido aos ataques cada vez mais sofisticados e a grande utilização de e-mails e acessos "online", bem como a infinidade de aplicativos web ou remotos, a aquisição de software de antimalware passa a ser indispensável para fornecer segurança à infraestrutura de rede e dados do MCOM, sendo este licenciamento imprescindível para o seu bom funcionamento.

3.1.5 Esta aquisição garante a segurança dos sistemas de informação do MCOM, evitando problemas que possam prejudicar a disponibilidade e integridade dos serviços prestados à sociedade e garante o desempenho das estações de trabalho e servidores de rede, disponibilizando melhores condições aos usuários para a realização de suas atividades.

3.1.6 Desta forma, a aquisição da solução tem por finalidade suprir, de forma integrada, a carência de recursos computacionais de segurança para proteção contra ataques e ameaças da nova geração a que o MCOM e demais órgãos estão expostos. Essa situação se torna mais crítica quando levamos em consideração as necessidades de manutenção e entrega de conteúdos referentes aos sistemas e programas de governo, que possuem um papel crucial e único para a sociedade.

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

3.2.1 Alinhamento aos Planos Estratégicos

3.2.1.1 Objetivos Estratégicos

OBJETIVO ESTRATÉGICO	REFERÊNCIA
Garantir recursos materiais e infraestrutura de TIC necessários ao desempenho das atribuições institucionais	Mapa Estratégico MCOM 2021-2023
OE11 - Garantia da segurança das plataformas de governo digital e de missão crítica	Estratégia de Governo Digital - 2020-2022
OE16 - Otimização das infraestruturas de tecnologia da informação	

3.2.1.2 Alinhamento ao PDTIC MCOM (2020 - 2022)

ID	NECESSIDADE	AÇÃO	ID	META
N4	Prover segurança no armazenamento e disponibilidade da informação	Aquisição de licenciamento para uso de solução de software antivírus corporativo com suporte de garantia	**M7**	Prover serviços de firewall

3.2.1.3 Alinhamento ao PAC MCOM (2021-2022)

Nº ITEM	SUBITEM	CÓDIGO DO ITEM	DESCRIÇÃO
408	Serviços de TIC	27472	Licenciamento de direitos permanentes de uso de outros softwares programas de computador
409	Materiais de TIC	350949	Software

3.2.2 Registramos que a contratação está em consonância com os documentos estratégicos elencados no art. 6º da IN SGD/ME nº 1/2019, citados acima.

3.3. Estimativa da demanda

3.3.1 Atualmente o MCom possui 850 (oitocentos e cinquenta) equipamentos a serem protegidos entre estações de trabalho e servidores de rede. Entretanto, existe expectativa de crescimento com limite superior estimado de até 1.300 (mil e trezentos) equipamentos em 12 meses. Desta forma, estima-se:

GRUPO	ITEM	DESCRIÇÃO	CÓDIGO CATSER/CATMAT	UNIDADE DE MEDIDA	QUANTIDADE PREVISTA
1	1	Solução de Next Generation Antimalware com gerenciamento centralizado, análise forense, detecção e respostas a incidentes	27472	Licenças	1.300
	2	Instalação e configuração	27260	Serviços	1.300
	3	Serviço de instalação do gerenciamento centralizado e repasse de conhecimento	27260	Serviços	1
	4	Serviço de gerenciamento e suporte da solução por 36 meses	27260	Serviços Mensal	36

3.4. Parcelamento da Solução de TIC

3.4.1 A contratação do objeto petendido se refere à "bens e serviços" comuns, de caráter continuado e sem fornecimento de mão de obra em regime de dedicação exclusiva, a ser contratado mediante licitação, por meio do Sistema de Registro de Preços, na modalidade pregão, em sua forma eletrônica, com julgamento pelo critério de **MENOR PREÇO GLOBAL**, com vistas à aquisição de solução de *next generation antimalware* (antivírus), com gerenciamento centralizado, análise forense, detecção e respostas a incidentes.

3.4.2 Os itens do objeto deverão ser licitados e adjudicados por grupo, considerando a indivisibilidade dos mesmos, pois as soluções e os serviços são de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia.

3.4.3 O fornecimento de itens por meio de CONTRATADAS distintas trariam enormes riscos ao projeto. Um grande risco viria da necessidade contínua de comunicação entre os diferentes fornecedores, o que, historicamente, não ocorre com fluidez nem de forma satisfatória, sendo a parte mais lesada o CONTRATANTE. Além disso, há necessidade de ocorrer perfeita integração técnica entre os itens do objeto. Dessa forma, o fornecimento parcial dos itens por diferentes fornecedores traria não apenas maior complexidade, como maiores custos de integração e riscos de não execução adequada.

3.4.4 A licitação por item poderia causar prejuízo para o conjunto da licitação (questões técnicas) ou para a economia de escala (questões econômicas), e tornaria inviável e prejudicial o bom desempenho da solução, por se tratar de serviços complementares. Por outro lado, a contratação dessa solução por grupo deverá gerar benefícios como a redução do valor final do contrato. Além disso, esse modelo elimina o problema de ter de gerenciar múltiplos fornecedores

para soluções de conectividade.

3.4.5 Nesse sentido, por se tratar de uma solução de serviços integrados, é fundamental para a garantia da qualidade do serviço, que sejam executados por um mesmo fornecedor, dada a impossibilidade de segregação do objeto sem que haja prejuízo ao conjunto, objetivando alcançar produtividade, economicidade e eficiência na realização dos serviços.

3.4.6 Desta forma, o agrupamento de elementos que compõem a mesma solução compõe a melhor estratégia da Administração, quando a adjudicação de itens isolados onera o "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", vide o ACÓRDÃO Nº 5301/2013 – TCU – 2ª Câmara.

3.5. Resultados e Benefícios a Serem Alcançados

3.5.1 Garantir um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;

3.5.2 Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo a estações de trabalho e notebooks comprometidos;

3.5.3 Evitar, mitigar e conter a propagação de pragas digitais facilitando o tratamento destes incidentes (vírus/malwares/spywares, spam, entre outros) com a administração centralizada da solução de proteção;

3.5.4 Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;

3.5.5 Possibilitar análise pormenorizada de arquivos, discos rígidos, unidades móveis, mensagens de e-mail e anexos, viabilizando detecção de ameaças, com intento de salvaguardar a estrutura tecnológica de ataques com teor e objetivo malicioso;

3.5.6 Possibilitar o controle de acesso e trafego de informações aos dispositivos e serviços operacionais na rede, através de gerenciamento centralizado, o que vem a complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;

3.5.7 Aprimorar a segurança de TIC do Ministério das Comunicações frente a ameaças sofisticadas.

4 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1 Aquisição de licenciamento do software antivírus corporativo, com suporte e garantia, em atendimento à solicitação da Coordenação-Geral de Tecnologia da Informação (CGTI) contida no Documento de Oficialização de Demanda (DOD) Sei nº 7927965.

4.1.2 Garantir o perfeito funcionamento da infraestrutura de rede do MCOM.

4.1.3 Garantir a segurança das informações do negócio e continuidade dos serviços de TIC;

4.1.4 Manter atualizada a solução de proteção antivírus contra novas ameaças.

4.2. Requisitos de Capacitação

4.2.1 Os requisitos de capacitação estão relacionados a "transferência de conhecimento" em que a futura prestadora dos serviços transmitirá exclusivamente aos servidores e/ou a sua equipe técnica do MCOM os conhecimentos teóricos e práticos da solução.

4.2.2 A prestadora dos serviços será responsável por disponibilizar todas as condições para a transferência de conhecimento ao MCOM, conforme especificado no item.

4.2.3 Para a implantação dos itens a serem contratados, deverá ser provido pela empresa contratada a transferência de conhecimentos dos procedimentos operacionais que serão realizados.

4.2.4 A transferência deverá contemplar os seguintes itens:

a) Apresentação da solução a ser implementada;

b) Plano de instalação da solução, que contemple todas as atividades a serem realizadas para garantir o menor impacto possível aos ambientes de produção da rede de dados do MCOM;

c) Operação e Administração da solução;

d) Descrição e uso das funcionalidades da solução;

e) Resolução de problemas;

f) Procedimentos de manutenção (atualizações de software).

4.2.5 A CONTRATADA e o MCOM elaborarão em conjunto um cronograma contendo as datas e horários para realização do repasse de conhecimento da solução, que deverá também atender às seguintes exigências:

a) A solução e todos os seus elementos deverão ser instalados, configurados, migrados, integrados e otimizados, segundo as melhores práticas do fabricante em termos de desempenho, disponibilidade e segurança, por técnico certificado por este, de modo a garantir total interoperabilidade no ambiente computacional do MCOM;

b) Concluídos os serviços de instalação e configuração, deverão ser realizados testes de operação com todas as tecnologias envolvidas na solução, durante o período de até 5 (cinco) dias corridos seguintes à instalação, de modo a garantir total interoperabilidade no ambiente computacional do MCOM objetivando a comprovação dos itens fornecidos e suas respectivas funcionalidades. Os resultados dos testes deverão ser incluídos na documentação a ser entregue.

4.3. Requisitos Legais

4.3.1 Na elaboração deste documento foram observadas as seguintes fontes legais e normativas:

4.3.1.1 Lei Federal nº 8.666/1993: institui normas gerais para licitações e contratos na Administração Pública e dá outras providências;

4.3.1.2 Lei Federal nº 10.520/2002: institui a modalidade de licitação denominada pregão eletrônico para aquisição de bens e serviços comuns e dá outras providências;

4.3.1.3 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;

4.3.1.4 Lei Complementar nº 123/2006 de 14 de dezembro de 2006, alterada pela Lei Complementar nº 147, de 7 de agosto de 2014: Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte; altera dispositivos das Leis nºs 8.212 e 8.213, ambas de 24 de julho de 1991, da Consolidação das Leis do Trabalho – CLT, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, da Lei nº 10.189, de 14 de fevereiro de 2001, da Lei Complementar nº 63, de 11 de janeiro de 1990; e revoga as Leis nºs 9.317, de 5 de dezembro de 1996, e 9.841, de 5 de outubro de 1999;

4.3.1.5 Decreto-Lei nº 200/67: Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências;

4.3.1.6 Decreto nº 2.271/1997: Dispõe sobre a contratação de serviços pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências;

4.3.1.7 Decreto nº 3.505/2000: Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

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

4.3.1.9 Decreto nº 7.579/2011: dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal;

4.3.1.10 Decreto nº 7.746/2012: regulamenta o art. 3º da Lei nº 8.666, de 21 de junho de 1993, para estabelecer critérios e práticas para a promoção do desenvolvimento nacional sustentável nas contratações realizadas pela administração pública federal direta, autárquica e fundacional e pelas empresas estatais dependentes, e institui a Comissão Interministerial de Sustentabilidade na Administração Pública – CISAP;

4.3.1.11 Decreto nº 8.420/2015: regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira e dá outras providências;

4.3.1.12 Decreto nº 10.024/2019: regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal;

4.3.1.13 Decreto nº 10.332, de 28 de abril de 2020: Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências

4.3.1.14 Instrução Normativa SEGES/MP nº 05, 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;

4.3.1.15 Instrução Normativa nº 03, de 26 de abril de 2018: dispõe sobre regras de funcionamento do Sistema de Cadastramento Unificado de Fornecedores – SICAF, no âmbito do Poder Executivo Federal;

4.3.1.16 Instrução Normativa SEGES/ME nº 01, de 10 de janeiro de 2019: dispõe sobre Plano Anual de Contratações de bens, serviços, obras e soluções de tecnologia da informação e comunicações no âmbito da Administração Pública federal direta, autárquica e fundacional e sobre o Sistema de Planejamento e Gerenciamento de Contratações;

4.3.1.17 Instrução Normativa SGD/ME nº 01, de 4 de abril de 2019, e alterações da Instrução Normativa SGD/ME nº 202, de 18 de setembro 2019 e Instrução Normativa SGD/ME nº 31, de 23 de março de 2021: dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

4.3.1.18 Instrução Normativa SEGES nº 73, de 05 de agosto de 2020: dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional;

4.3.1.19 Instrução Normativa nº 40, de 22 de maio de 2020: Dispõe sobre a elaboração dos Estudos Técnicos Preliminares - ETP - para a aquisição de bens e a contratação de serviços e obras, no âmbito da Administração Pública federal direta, autárquica e fundacional, e sobre o Sistema ETP digital;

4.3.1.20 Instrução Normativa SGD/ME nº 5, de 11 de janeiro de 2021: Regulamenta os requisitos e procedimentos para aprovação de contratações ou de formação de atas de registro de preços, a serem efetuados por órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, relativos a bens e serviços de tecnologia da informação e comunicação - TIC;

4.3.1.21 Portaria MPDG nº 20, de 14 de junho de 2016, que dispõe sobre orientações para contratação de soluções de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional e dá outras providências; e

4.3.1.22 Guia Nacional de Sustentabilidade da AGU, 3ª edição, Abr/2020.

4.3.2 O objeto da pretendida contratação NÃO incide nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD/ME nº 1/2019, transcritos abaixo:

> *"Art. 3º Não poderão ser objeto de contratação:*
>
> *I - mais de uma solução de TIC em um único contrato, devendo o órgão ou entidade observar o disposto nos §§ 2º e 3º do art. 12; e*
>
> *II - o disposto no art. 3º do Decreto nº 9.507, de 2018, inclusive gestão de processos de TIC e gestão de segurança da informação.*
>
> *Parágrafo único. O apoio técnico aos processos de gestão, de planejamento e de avaliação da qualidade das soluções de TIC poderá ser objeto de contratação, desde que sob supervisão exclusiva de servidores do órgão ou entidade.*
>
> *Art. 4º Nos casos em que a avaliação, mensuração ou apoio à fiscalização da solução de TIC seja objeto de contratação, a contratada que provê a solução de TIC não poderá ser a mesma que a avalia, mensura ou apoia a fiscalização."*

4.3.3 Cabe também registrar que o presente Termo de Referência foi elaborado a partir da observação dos guias, manuais e modelos publicados pelo órgão central do SISP em consonância com o §2° do art. 8° da Instrução Normativa n° 01/2019/SGD/ME, o qual estabelece:

"§ 2º As contratações de soluções de TIC devem atender às normas específicas dispostas no ANEXO e observar os guias, manuais e modelos publicados pelo Órgão Central do SISP."

4.4. Requisitos de Manutenção

4.4.1 A CONTRATADA deverá sanar todos os vícios e defeitos da solução.

4.4.2 A garantia técnica deverá ser realizada, durante todo o período, pelo próprio fabricante ou por Assistência Técnica Autorizada, localizada em Brasília-DF, a fim de que sejam mantidos válidos todos os direitos oriundos da garantia, excluindo-se a possibilidade de falta de cobertura por manutenções realizadas sem a habilidade técnica necessária.

4.4.3 Nos casos em que a garantia técnica for prestada por meio de Assistência Técnica Autorizada, deverão ser divulgados, pelo fabricante, inclusive por meio de sítio na internet, para fins de identificação, o nome e o telefone da(s) Assistência(s) que prestará(ão) atendimento, bem como declaração do fabricante.

4.4.4 Todo software utilizado para o perfeito desempenho das funções dos produtos deverá ser assegurado durante todo o período de garantia, com correção de todas as possíveis falhas apresentadas e atualizações nas versões dos softwares, ocorridas no período, sem acarretar ônus para o MCOM.

4.4.5 O direito de atualização de versão do software será fornecido durante o período de vigência da prestação do serviço de suporte técnico, da seguinte forma:

4.4.5.1 No período de 36 meses, a contratante deverá fornecer atualizações ou novas versões das licenças de softwares adquiridas, nas seguintes condições:

a) A atualização de versão deve contemplar o fornecimento de todas as novas versões do software; e

b) A cada nova liberação de versão, deverá ser fornecida em seu sítio de suporte técnico nota informativa com a descrição das novas funcionalidades e correções implementadas, bem como as atualizações de manuais e demais documentos técnicos, em até 30 (trinta) dias do seu lançamento. A versão deverá estar disponível para download também neste prazo.

4.5. Requisitos Temporais

4.5.1 A CONTRATADA deverá:

4.5.1.1 Entregar as licenças e os certificados de garantia adquiridos no prazo máximo de 45 (quarenta e cinco) dias corridos no MCOM, localizado na Esplanada dos Ministérios, Bloco “R”, Anexo, Térreo, Brasília/DF, a contar da data de assinatura do contrato. Deve estar incluída a documentação técnica atualizada, drivers e outros programas necessários ao funcionamento dos equipamentos, os quais serão armazenados em mídia eletrônica.

4.5.1.2 Se, após o recebimento provisório, constatar-se que as licenças ou os certificados de garantia foram entregues em desacordo com o solicitado, fora da especificação ou incompletas, a CONTRATADA será notificada e deverá sanar as pendências em até 30 (trinta) dias corridos. A despesas referentes a troca de licenças, inclusive frete, correrá às expensas da CONTRATADA.

4.5.2 A CONTRATADA deverá fornecer os produtos e prestar os serviços descritos no objeto nos prazos abaixo:

ID	DESCRIÇÃO	PRAZO
1	Solução de Next Generation Antimalware com gerenciamento centralizado, análise forense, detecção e respostas a incidentes	Em até 45 dias corridos após assinatura do contrato
2	Instalação e configuração	Em até 15 dias corridos após a entrega dos produtos
3	Serviço de instalação do gerenciamento centralizado e repasse de conhecimento	Em até 15 dias corridos após a entrega dos produtos
4	Serviço de gerenciamento e suporte da solução por 36 meses	Contados a partir da data de assinatura do Termo de Recebimento Definitivo

4.5.3 O prazo de vigência da Ata de Registro de Preços será de 12 (doze) meses contados a partir da data de assinatura do contrato.

4.5.4 O serviço de gerenciamento e suporte técnico será mensal com uma vigência de 36 (trinta e seis) meses, a contar da data de emissão do TERMO DE RECEBIMENTO DEFINITIVO em conformidade com o estabelecido neste Termo de Referência;

4.5.5 A vigência do contrato será de 36 (trinta e seis) meses contados a partir da data de sua assinatura;

4.5.6 O licenciamento da solução terá vigência de 36 (trinta e seis) meses e o CONTRATANTE terá direito a toda e qualquer nova atualização do software, seja versões, patchs, hotfixes ou assinaturas e subscrições de segurança que fizerem parte da solução durante esse período.

4.6. Requisitos de Segurança

4.6.1 A CONTRATADA deverá atender ao disposto no art. 31, I, "b" da IN-SGD 01/2019 (entrega dos termos de Compromisso e de Ciência) no prazo estabelecido no presente Termo de Referência.

4.6.2 A CONTRATADA e seus profissionais envolvidos na solução deverão seguir os seguintes procedimentos e premissas de segurança envolvidos na prestação dos serviços:

4.6.2.1 Manter sigilo sobre todo e qualquer assunto de interesse do MCOM ou de terceiros de que tomar conhecimento em razão da execução dos serviços contratados, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa;

4.6.2.2 Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos pelo MCOM;

4.6.2.3 Manter sigilo de todas as informações a que tiveram acesso inclusive após o término da vigência contratual ou eventual rescisão;

4.6.2.4 Assinar Termo de Compromisso e de Manutenção do Sigilo, constante no **ANEXO D e E**.

4.7. Requisitos Sociais, Ambientais e Culturais

4.7.1 A CONTRATADA deverá atender no que couber, os critérios de sustentabilidade ambiental. Destaca-se, as recomendações contidas no Capítulo III, DOS BENS E SERVIÇOS, com ênfase no art. 5º da Instrução Normativa nº 01/2010 STI/MPOG, bem como, o Decreto nº 7.746/2012 que estabelece critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável e a Lei nº 12.305/2010 que institui a política de resíduos sólidos, no que couber.

4.7.2 É dever da CONTRATADA observar entre outras: o menor impacto sobre recursos naturais como flora, fauna, ar, solo e água; preferência para materiais, tecnologias e matérias-primas de origem local; maior eficiência na utilização de recursos naturais como água e energia; maior geração de empregos, preferencialmente com mão de obra local; maior vida útil e menor custo de manutenção do bem e da obra; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens, serviços e obras.

4.7.3 A CONTRATADA deverá assinar Declaração de Sustentabilidade Ambiental, conforme **ANEXO C** deste Termo de Referência.

4.7.4 A execução do objeto será realizada de acordo com os critérios de sustentabilidade ambiental contidos no Art. 5º da Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Governo Digital do Ministério da Economia e no Decreto nº 7.746, de 05 de junho de 2012, da Casa Civil da Presidência da República, no que couber.

4.7.5 A abertura de chamados técnicos e encaminhamentos de demandas deverão ser realizados, preferencialmente, sob a forma eletrônica, evitando-se a impressão de papel. Além disso, as configurações de hardware e software deverão ser realizadas visando alto desempenho com a utilização racional de energia.

4.8. Requisitos de Arquitetura Tecnológica

4.8.1 A solução deve oferecer console de gerência Web ou console do próprio fabricante.

4.8.2 Caso a console seja Web, deve ser compatível com pelo menos dois dos seguintes navegadores: Microsoft Edge 41 ou superior; Google Chrome 70 ou superior; Mozilla Firefox 60 ou superior.

4.8.3 A console deve funcionar plenamente sem requerer a instalação de plug-ins, drivers, java e flash player.

4.8.4 A solução deve manter log de auditoria com registro das configurações realizadas por qualquer usuário ou administrador do sistema.

4.9. Requisitos de Projeto e de Implementação

4.9.1 A CONTRATADA deverá cumprir os prazos determinados para fornecimento dos itens licitados, instalação das licenças, instalação da solução de segurança e execução dos repasses de conhecimento.

4.9.2 A CONTRATADA deverá manter responsáveis pelo acompanhamento da implantação da solução no MCOM, a fim de tratar das questões técnicas e administrativas.

4.9.3 A CONTRATADA terá até 45 (quarenta e cinco) dias a contar da data de assinatura do contrato para entrega dos produtos relativos ao objeto.

4.9.4 Os itens serão recebidos:

4.9.4.1 Provisoriamente, ocorrerá em até 5 (cinco) dias úteis a contar da entrega dos itens do objeto, para posterior verificação da conformidade e quantidade com as especificações técnicas.;

4.9.4.2 Definitivamente, no prazo máximo de 10 (dez) dias úteis, depois de concluída a verificação de conformidade e quantidades, ocasião em que será emitido o respectivo TERMO DE RECEBIMENTO DEFINITIVO.

4.9.5 Após entrega da solução, iniciar-se-á a etapa de verificação que compreenderá o seguinte procedimento:

4.9.5.1 A CONTRATADA procederá com a instalação da solução para a realização dos testes de funcionamento, na presença e supervisão de técnicos do CONTRATANTE, sendo posteriormente aferido e testado o seu perfeito funcionamento.

4.9.6 Qualquer produto será recusado inteiramente nas seguintes condições:

4.9.6.1 Caso seja entregue em desconformidade com as especificações técnicas constantes neste Temo de Referência e da proposta vencedora;

4.9.6.2 Caso apresente defeitos, em qualquer de suas partes ou componentes, durante os testes de conformidade e verificação;

4.9.6.3 Nos casos de recusa do produto, a CONTRATADA terá o prazo de 30 (trinta) dias corridos para providenciar a sua substituição, contados a partir da comunicação oficial feita pelo CONTRATANTE.

4.10. Requisitos de Implantação

4.10.1 A solução deverá ser fornecida, instalada, otimizada, testada e documentada mediante instruções e aprovação da equipe técnica da CONTRATANTE.

4.10.2 São atividades inerentes a implantação, as quais devem ser executadas pela CONTRATADA:

4.10.2.1 Instalação da solução de segurança;

4.10.2.2 Elaboração da documentação, contendo no mínimo os seguintes itens:

4.10.2.2.1 Cronograma;

4.10.2.2.2 Levantamento de informações sobre o ambiente atual;

4.10.2.2.3 Mapa de rede contendo a topologia a ser implantada ou atualizada;

4.10.2.2.4 Definição dos parâmetros de configuração básicos e avançados a serem implantados;

4.10.2.2.5 Projeto contendo, no mínimo: fases, escopo, riscos, plano de execução, planos de recuperação, resultados esperados.

4.10.2.3 Definição, em conjunto com a CONTRATANTE, em relação a arquitetura de rede e diretrizes de segurança que serão utilizados na implantação da solução de Next-Generation Antimalware no ambiente corporativo do Ministério das Comunicações.

4.10.2.4 Definição, em conjunto com a CONTRATANTE, dos parâmetros de configuração em relação a rede e segurança da solução de Next-Generation Antimalware a ser implantada no ambiente corporativo do Ministério das Comunicações.

4.10.2.5 Instalação Física dos equipamentos, caso houver, em local a ser definido pelo CONTRATANTE, incluindo os componentes necessários: cabeamento, braços, conectores SFP+/XFP, etc;

4.10.2.6 Configuração de solução segundo arquitetura de rede, segurança e parâmetros de configuração definidos pelo CONTRATANTE;

4.10.2.7 Configuração de alarmes e notificações automatizadas via SNMP e/ou SMTP e/ou SMS;

4.10.2.8 Teste e homologação da solução implantada;

4.10.2.9 Elaboração de documentação contendo planejamento, relatório de instalação, configuração adotada, indicando os testes realizados e seus resultados;

4.10.2.10 Elaboração dos planos de recuperação de desastres, bem como a execução de testes para validação do plano;

4.10.2.11 Repasse de tecnologia a equipe técnica, realizado in loco e no ambiente implantado, com o objetivo de prover informações suficientes para supervisão e gestão do ambiente.

4.11. Requisitos de Garantia

4.11.1 Garantia Técnica

4.11.1.1 A CONTRATADA deverá oferecer garantia do fabricante por 36 (trinta e seis) meses para os itens adquiridos, contados a partir da data de emissão do TERMO DE RECEBIMENTO DEFINITIVO;

4.11.1.2 A garantia deverá ser do fabricante;

4.11.1.3 Deve ser fornecida garantia de atualização de softwares para um período de validade de 36 (trinta e seis) meses;

4.11.1.4 Deve ser fornecida garantia de reposição de hardware, caso houver, por um prazo de 36 (trinta e seis) meses, para situações em que sejam identificados problemas no hardware da solução contratada;

4.11.1.5 Em caso de falha no hardware, a CONTRATADA deve disponibilizar um hardware reserva, que irá permanecer em ambiente de produção da CONTRATANTE até o retorno do hardware original reparado, ou novo, em substituição, a critério do CONTRATANTE;

4.11.1.6 A CONTRATADA deverá assegurar que o hardware substituto, em qualquer caso, seja igual ao contratado inicialmente ou que possua características superiores a este, desde que estejam homologadas pelo fabricante como parte compatível da solução;

4.11.1.7 O serviço de substituição de hardware será prestado na modalidade 24x7, ou seja, estará disponível para acionamento 24 horas por dia, 7 dias por semana;

4.11.1.8 A CONTRATADA deverá substituir quaisquer peças ou componentes defeituosos em um prazo máximo de 48 (quarenta e oito) horas após o primeiro atendimento relativo ao chamado, de acordo com a garantia e sem ônus para o CONTRATANTE;

4.11.1.9 A substituição de qualquer componente defeituoso, em qualquer caso, deverá ser feita por item equivalente ou que possua características superiores a estas, desde que estejam homologadas pelo fabricante como parte compatível da solução;

4.11.1.10 As peças de substituição devem ser novas, não sendo aceitas peças usadas ou recondicionadas;

4.11.1.11 A CONTRATADA deverá substituir, caso necessário, todo o equipamento, dentro dos prazos estabelecidos;

4.11.1.12 A substituição do hardware será considerada consumada no momento em que a solução voltar ao seu funcionamento normal e for aceita formalmente pela equipe técnica do CONTRATANTE.

4.11.2 Garantia de Execução

4.11.2.1 O adjudicatário prestará garantia de execução do contrato, nos moldes do art. 56, da Lei nº 8.666, de 1993, com validade durante a execução do contrato, em valor correspondente a 3% (três por cento) do valor total do contrato.

4.11.2.2 No prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério da CONTRATANTE, contados da assinatura do contrato, a contratada deverá apresentar comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

4.11.2.3 A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento). O atraso superior a 30 (trinta) dias autoriza o CONTRATANTE a promover a rescisão do CONTRATO por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n. 8.666 de 1993.]

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

4.11.2.3.2 O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666 de 1993.

4.11.2.4 A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 (noventa) dias após o término da vigência contratual, conforme item 3.1 do Anexo VII-F da IN SEGES/MPDG nº 5/2017.

4.11.2.5 A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

a) Prejuízos advindos do não cumprimento do objeto do CONTRATO;

b) Prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do CONTRATO;

c) Multas moratórias e punitivas aplicadas pela Administração à CONTRATADA.

d) Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela contratada, quando couber.

4.11.2.5 A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

4.11.2.6 A garantia em dinheiro deverá ser efetuada em favor do Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

4.11.2.7 Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

4.11.2.8 No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

4.11.2.9 No caso de alteração do valor do contrato prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

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

4.11.2.11 O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

4.11.2.12 Será considerada extinta a garantia:

4.11.2.12.1 Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato.

4.11.2.13 O garantidor não é parte legítima para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA (cfe. IN nº 05/2017).

4.11.2.14 A CONTRATADA autoriza o contratante a reter, a qualquer tempo, a garantia, na forma prevista no neste Termo de Referência e no contrato.

4.12. Requisitos de Experiência Profissional

4.12.1 Os serviços deverão ser executados por profissionais qualificados e com a capacidade técnica necessária para o objeto de contratação.

4.13. Requisitos de Formação da Equipe

4.13.1 O serviço de suporte técnico deverá ser prestado por profissionais especializados e certificados pelo fabricante da solução, devidamente capacitados.

4.14. Requisitos de Metodologia de Trabalho

4.14.1 Na execução das demandas, a CONTRATADA deve zelar pela observância às políticas, diretrizes, procedimentos, padrões e modelos para as atividades de gestão e fiscalização de contratos e planejamento de contratações. No que couber, quando não especificado de outra forma, o processo de trabalho é aquele descrito no Modelo de Execução e tem como principais referências metodológicas a Instrução Normativa SGD/ME n° 01, de 04 de abril de 2019, e suas atualizações.

4.14.2 A avaliação da qualidade dos serviços prestados ocorrerá através do acompanhamento e avaliação dos atendimentos aos chamados de suporte técnico junto o serviço de gerenciamento da solução, seguindo os termos contratuais definidos neste Termo de Referência e Anexos.

4.15. Outros Requisitos Aplicáveis

4.15.1 Requisito Propriedade, Sigilo e Restrições

4.15.1.1 Toda a documentação gerada durante a vigência do contrato deve ser repassada ao CONTRATANTE com todos os direitos de propriedade.

4.15.1.2 O CONTRATANTE deverá ser o único proprietário dos documentos e manuais gerados durante a vigência do contrato, devendo, para tanto, a CONTRATADA ceder ao CONTRATANTE, mediante cláusula contratual.

4.15.1.3 A CONTRATADA não poderá repassar a terceiros, em nenhuma hipótese, os códigos-fontes desenvolvidos especificamente para o CONTRATANTE, bem como qualquer informação sobre a arquitetura, documentação, assim como dados trafegados no sistema, produtos desenvolvidos e entregues, ficando responsável juntamente com o CONTRATANTE por manter a integridade dos dados e códigos durante a execução das atividades e também após o término da execução dos serviços.

4.15.2 Requisitos do Repasse de Conhecimentos

4.15.2.1 Para a implantação dos itens a serem contratados, deverá ser provido pela empresa contratada a transferência de conhecimentos dos procedimentos operacionais que serão realizados.

4.15.2.2 A transferência deverá contemplar os seguintes itens:

a) Apresentação da solução a ser implementada;

b) Plano de instalação da solução, que contemple todas as atividades a serem realizadas para garantir o menor impacto possível aos ambientes de produção da rede de dados do MCOM;

c) Operação e Administração da solução;

d) Descrição e uso das funcionalidades da solução;

e) Resolução de problemas;

f) Procedimentos de manutenção (atualizações de software).

4.15.2.3 A CONTRATADA e o MCOM elaborarão em conjunto um cronograma contendo as datas e horários para realização do repasse de conhecimento da solução, que deverá também atender às seguintes exigências:

a) A solução e todos os seus elementos deverão ser instalados, configurados, migrados, integrados e otimizados, segundo as melhores práticas do fabricante em termos de desempenho, disponibilidade e segurança, por técnico certificado por este, de modo a garantir total interoperabilidade no ambiente computacional do MCOM;

b) Concluídos os serviços de instalação e configuração, deverão ser realizados testes de operação com todas as tecnologias envolvidas na solução, durante o período de até 5 (cinco) dias corridos seguintes à instalação, de modo a garantir total interoperabilidade no ambiente computacional do MCOM objetivando a comprovação dos itens fornecidos e suas respectivas funcionalidades. Os resultados dos testes deverão ser incluídos na documentação a

ser entregue.

4.15.3 Requisitos Técnicos

4.15.3.1 As especificações técnicas estão previstas no Anexo A , deste Termo de Referência.

5 – RESPONSABILIDADES

5.1. Deveres e responsabilidades da CONTRATANTE

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

5.1.2 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;

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

5.1.4 Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis;

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

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

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

5.1.9 Aplicar as penalidades cabíveis;

5.1.10 Permitir que somente pessoas autorizadas pela CONTRATADA prestem o suporte técnico especializado e realizem a operação assistida;

5.1.11 Disponibilizar todos os meios necessários para a execução dos serviços contratados.

5.2. Deveres e responsabilidades da CONTRATADA

5.2.1 Além de garantir a fiel execução dos serviços contratados de acordo com os termos contratuais, são responsabilidades da CONTRATADA:

5.2.1.1 Executar os serviços conforme as especificações do Contrato, deste Termo de Referência e de sua proposta;

5.2.1.2 Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão CONTRATANTE, nos termos do artigo 7° do Decreto n° 7.203, de 2010;

5.2.1.3 Reparar, refazer, corrigir, remover ou substituir, às suas expensas, no todo ou em parte, no prazo fixado pelo gestor do CONTRATO, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados – ressalvada a aplicação de glosas e sanções pelo não cumprimento dos critérios de qualidade e/ou não atendimento a orientações do CONTRATANTE;

5.2.1.4 Garantir o cumprimento, durante toda a vigência contratual, dos requisitos mínimos relacionados à perfis profissionais de sua equipe técnica diretamente envolvida na execução do objeto, de acordo com as obrigações contratuais e em conformidade com as normas e determinações em vigor;

5.2.1.5 Apresentar ao CONTRATANTE, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço – instruindo-os quanto à necessidade de acatar as normas internas deste;

5.2.1.6 Arcar com todos os custos administrativos de sua responsabilidade relacionados ao objeto e à execução do contrato, responsabilizando-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade ao CONTRATANTE;

5.2.1.7 Indicar e manter preposto apto a representá-la junto ao CONTRATANTE, que deverá responder pela fiel execução do contrato, de acordo com os requisitos definidos;

5.2.1.8 Atender prontamente quaisquer orientações e exigências do gestor do contrato, inerentes à execução do objeto contratual;

5.2.1.9 Informar prontamente ao CONTRATANTE sobre fatos e/ou situações relacionadas à prestação dos serviços contratados que representem risco ao êxito da contratação ou o cumprimento de prazos exigidos, além de responsabilizar-se pelo conteúdo e veracidade das informações prestadas - sob pena de incorrer em situações de dolo ou omissão – comunicando o GESTOR do Contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços;

5.2.1.10 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;

5.2.1.11 Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução dos serviços, durante a vigência do contrato

5.2.1.12 Reparar quaisquer danos diretamente causados ao 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 pelo CONTRATANTE;

5.2.1.13 Submeter previamente, por escrito, ao CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações da metodologia de trabalho;

5.2.1.14 Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à União ou à entidade federal, devendo ressarcir imediatamente a Administração em sua integralidade, ficando o CONTRATANTE autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos;

5.2.1.15 Propiciar todos os meios e facilidades necessárias à fiscalização da Solução de Tecnologia da Informação pelo CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;

5.2.1.16 Manter, durante toda a execução do CONTRATO, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação – assim como deve zelar pelo cumprimento de suas obrigações legais, fiscais e trabalhistas;

5.2.1.17 Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a empresa CONTRATADA deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:

5.2.1.17.1 Prova de regularidade relativa à Seguridade Social;

5.2.1.17.2 Certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;

5.2.1.17.3 Certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado;

5.2.1.17.4 Certidão de Regularidade do FGTS – CRF; e

5.2.1.17.5 Certidão Negativa de Débitos Trabalhistas – CNDT, conforme alínea "c" do item 10.2 do Anexo VIII-B da IN SEGES/MP n. 5/2017.

5.2.1.18 Ceder os direitos de propriedade intelectual e direitos autorais sobre os diversos artefatos e produtos produzidos ao longo do CONTRATO, incluindo a documentação, os modelos de dados e as bases de dados ao CONTRATANTE, nos termos da legislação vigente;

5.2.1.19 Aceitar, nas mesmas condições contratuais, os acréscimos ou as supressões que se fizerem no objeto contratual, até o limite legal de 25% (vinte e cinco por cento) do seu valor total;

5.2.1.20 Zelar pelo cumprimento de leis e normas relativas à segurança e medicina do trabalho durante a execução de quaisquer serviços de sua responsabilidade nas instalações do CONTRATANTE. Assim como cumprir as normas do CONTRATANTE aplicáveis em suas instalações funcionais, inclusive regras de acesso e controles de segurança;

5.2.1.21 Não permitir a utilização de qualquer trabalho do menor de 16 (dezesseis) anos, exceto na condição de aprendiz para os maiores de 14 (quatorze anos); nem permitir a utilização do trabalho do menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre;

5.2.1.22 Manter o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações que a ela venham a ser confiados ou que venha a ter acesso em razão da execução dos serviços, não podendo, sob qualquer pretexto, revelá-los, divulgá-los, reproduzi-los ou deles dar conhecimento a quaisquer terceiros;

5.2.1.23 Em nenhuma hipótese veicular publicidade ou qualquer outra informação acerca do objeto deste Termo de Referência, sem prévia autorização do CONTRATANTE;

5.2.1.24 Retirar, após o término do contrato, qualquer bem de que seja proprietária e que, eventualmente, esteja no espaço do CONTRATANTE;

5.2.1.25 Assinar Termo de Compromisso conforme ANEXO D - TERMO DE COMPROMISSO DE MANUTENÇÃO DO SIGILO.

5.3. Deveres e responsabilidades do órgão gerenciador.

5.3.1 Não se aplica.

6 – MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de Execução

6.1.1 Reunião Inicial

6.1.1.1 O CONTRATANTE, por intermédio do Gestor do Contrato, convocará a CONTRATADA, imediatamente após a assinatura do contrato, para reunião de alinhamento de entendimentos e expectativas, ora denominada reunião inicial, com o objetivo de:

a) Alinhar a forma de comunicação entre as partes, que deverá ocorrer preferencialmente entre o CONTRATANTE e o Preposto da CONTRATADA;

b) Definir as providências necessárias para inserção da CONTRATADA no ambiente de prestação dos serviços;

c) Definir as providências de implantação dos serviços;

d) Alinhar entendimento quanto aos modelos de execução e de gestão do contrato.

6.1.1.2 Na Reunião Inicial a CONTRATADA deverá:

a) Apresentar seu PREPOSTO;

b) Havendo necessidade outros assuntos de comum interesse, poderão ser tratados na reunião inicial, além dos anteriormente previstos. Todas as atas de reuniões e as comunicações entre o CONTRATANTE e a CONTRATADA, assim como todas as demais intercorrências contratuais, positivas ou negativas, serão arquivadas em processo próprio para fins de manutenção do histórico de gestão do CONTRATO.

6.1.2 Suporte Técnico

6.1.2.1 A contratação do objeto dar-se-á por meio de Pregão Eletrônico para Registro de Preços do tipo Menor Preço por grupo;

6.1.2.2 O serviço de suporte técnico consiste em manutenção preventiva e manutenção corretiva de todos os itens do objeto;

6.1.2.3 A execução do serviço de suporte técnico e de atualização de versões deverá ser realizada por profissional certificado pelo fabricante da solução, sem custos adicionais para o CONTRATANTE, durante o período de licenciamento, suporte técnico e garanta, sendo indispensável a apresentação de documentação original do fabricante que comprove a validade da certificação enquanto durar o vínculo contratual, podendo ser solicitada a qualquer momento;

6.1.2.4 O serviço de suporte técnico deverá ser realizado em regime de 24 (vinte e quatro) horas por 7 (sete) dias por semana, todos os dias do ano, no idioma português, devendo a empresa possuir uma central de atendimento sem custos para o CONTRATANTE e atender aos chamados da equipe técnica nos prazos estipulados;

6.1.2.5 Se o problema não for resolvido em no máximo 20 (vinte) dias, a partir do registro do chamado, a solução deverá ser integralmente substituída, sem ônus adicional para o CONTRATANTE, no prazo máximo de 10(dez) dias úteis subsequentes;

6.1.2.6 Durante o período de vigência do suporte técnico e garantia, quando for o caso, todos os firmwares e softwares deverão ser atualizados a cada nova versão ou correção, sem nenhum custo adicional para o CONTRATANTE;

6.1.2.7 O serviço de suporte técnico poderá ser atendido através de contato telefônico 0800, por e-mail ou nas dependências do CONTRATANTE, sendo este critério decidido pela equipe técnica do CONTRATANTE;

6.1.2.8 A CONTRATADA deverá possuir sistema de abertura de chamados para que o CONTRATANTE possa receber um identificador único para cada solicitação de atendimento e que tenha recurso(s) (e-mail, página web, central telefônica ou etc.) que possa manter a equipe técnica do CONTRATANTE informada sobre o andamento de cada chamado, esteja ele aberto, em andamento ou fechado.

6.1.3 Prestação do Serviço

6.1.3.1 Administrar, suportar, manter, gerenciar e Monitorar 24x7x365 o Ambiente da solução de Next Generation AntiMalware;

6.1.3.2 O serviço terá a participação e cooperação da Área de TI do CONTRATANTE durante toda a duração do contrato;

6.1.3.3 A CONTRATADA irá prestar auxílio à equipe de Segurança da Informação do CONTRATANTE no suporte direto às Estações de Trabalho, Servidores e Laptops do ambiente de TI, além de outros Hosts que possuam interação com o serviço da solução de segurança e não estejam descriminados nesse item;

6.1.3.4 A CONTRATADA deverá disponibilizar VPN Site-to-Site para conexão ao CONTRATANTE, a fim de gerenciar remotamente via VPN, a solução de Next Generation AntiMalware.

6.1.3.5 O atendimento pode ser remoto ou local (on-site), a depender da necessidade de atendimento identificada pelo CONTRATANTE ou CONTRATADA, de acordo com o SLA contratado.

6.1.3.6 Manutenção Preventiva

6.1.3.6.1 A manutenção preventiva será destinada a atualizar os componentes do software e a realizar quaisquer operações que evitem uma parada parcial ou total da solução;

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

6.1.3.7 Manutenção Corretiva

6.1.3.7.1 A manutenção corretiva será destinada a remover os defeitos apresentados pelos componentes de software e hardware de toda solução objeto do contrato, compreendendo também a atualização de versões e correções dos componentes de software e hardware que se fizerem necessários.

6.1.3.7.2 A manutenção corretiva será realizada sempre que a solução apresentar falha que impeça o seu funcionamento regular e requeira uma intervenção técnica especializada ou mesmo a substituição de seus componentes.

6.1.3.7.3 A manutenção corretiva pode ser solicitada a qualquer momento em que o sistema apresente pane, deficiência ou dificuldade de operação.

6.1.3.7.4 As visitas para prestação do serviço de manutenção preventiva e corretiva, independentemente da quantidade necessária, não implicarão em custos adicionais para o CONTRATANTE e deverão estar inclusas no custo mensal proposto do suporte técnico especializado.

6.1.4 Serviços de Gerenciamento

6.1.4.1 O serviço de gerenciamento da solução deverá proteger a rede corporativa do CONTRATANTE e seus usuários contra vírus, malwares, phishing e outras ameaças indesejáveis, através de análise de artefatos, filtragem e limpeza dos arquivos recebidos, enviados ou transferidos, por qualquer meio, garantindo que nem a rede e nem as atividades dos usuários sejam interrompidos.

6.1.4.2 Com o gerenciamento centralizado, deverá ser possível realizar a emissão de relatórios e gráficos informativos, com a visão geral da segurança da rede quanto às ameaças protegidas. Os relatórios deverão ser gerados semanalmente pela CONTRATADA para servirem como apoio para as tomadas de decisões em relação aos riscos operacionais da rede corporativa do CONTRATANTE, mitigação dos mesmos e aumento do nível de segurança da solução.

6.1.4.3 Ação:

a) Identificação e bloqueio de ataques, invasões e sabotagens em tempo real;

b) Atuar de acordo com as melhores práticas e recomendações das organizações de segurança;

c) Proteção dos servidores de rede, notebooks e estações de trabalho;

d) Configurações e ajustes necessários no ambiente;

e) Monitoramento 24x7x365 de forma ininterrupta;

f) Tratativa de Outbreak de infecção;

g) Proteção contra Ransonware, Zero Day e demais ameaças avançadas;

h) Gestão de tratamento e resposta a incidente;

i) Redução dos índices de contaminação por vírus e pragas virtuais;

j) Constante identificação dos principais pontos de fragilidade e riscos;

k) Aderência a padrões e normas internacionais, como ISO 27001.

6.2. Quantidade mínima de bens ou serviços para comparação e controle

6.2.1 Conforme item 2.4 deste Termo de Referência.

6.3 Rescisão Contratual

6.3.1 A inexecução total ou parcial do contrato enseja a sua rescisão, conforme disposto nos arts. 77 a 80 da Lei nº 8.666/93:

6.3.1.1 Os casos de rescisão contratual deverão ser formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

6.3.2 A rescisão do contrato poderá ser:

6.3.2.1 Determinada por ato unilateral e escrito do CONTRATANTE, nos casos enumerados nos incisos I a XII, XVII e XVIII, do art. 78 da Lei nº 8.666/93;

6.3.2.2 Amigável, por acordo entre as partes, desde que haja conveniência para o CONTRATANTE;

6.3.2.3 Judicial, nos termos da legislação vigente sobre a matéria;

6.3.2.4 A rescisão administrativa ou amigável será precedida de autorização escrita e fundamentada da autoridade competente.

6.4. Mecanismos formais de comunicação

6.4.1 São definidos como mecanismos formais de comunicação, entre a CONTRATANTE e a CONTRATADA, os seguintes:

a) Ordem de Serviço;

b) Ata de Reunião;

c) Ofício;

d) Sistema de abertura de chamados;

e) E-mails.

6.5. Manutenção de Sigilo e Normas de Segurança

6.5.1 A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.5.2 O **Termo de Compromisso**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e **Termo de Ciência**, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos **ANEXOS D** e **E.**

7 – MODELO DE GESTÃO DO CONTRATO

7.1 Para cumprir as atividades de gestão e fiscalização do CONTRATO, o CONTRATANTE designará servidores (titulares e substitutos) para executar os seguintes papéis:

a) Gestor do Contrato: servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente;

b) Fiscal Técnico: servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato;

c) Fiscal Requisitante: servidor representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista funcional da Solução de Tecnologia da Informação; e

d) Fiscal administrativo: servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos.

7.2. Critérios de Aceitação

7.2.1 O objeto contratado será recebido, como parte do processo de monitoramento da execução, de forma provisória e definitiva, conforme prevê o artigo 73 da Lei nº 8.666/93 e o art. 33 da Instrução Normativa n° 01/2019/SGD/ME, observando o disposto a seguir:

7.2.1.1 Recebimento Provisório

7.2.1.1.1 O recebimento provisório será realizado pelo Fiscal Técnico do contrato quando da entrega do objeto resultante de cada ordem de serviço e consiste na emissão do Termo de Recebimento Provisório que, por sua vez, consiste na “declaração formal de que os serviços foram prestados ou os bens foram entregues, para posterior análise das conformidades e qualidades baseadas nos requisitos e nos critérios de aceitação, de acordo com a alínea "a" do inciso I, e alínea "a" do inciso II do art. 73 da Lei nº 8.666, de 1993” (inc XXI do art. 2° da IN-01/2019/SGD/ME).

7.2.1.1.2 O recebimento provisório ocorrerá em até 5 (cinco) dias úteis a contar da entrega dos itens do objeto, para posterior verificação da conformidade e quantidade com as especificações técnicas.

7.2.1.2 Recebimento Definitivo

7.2.1.2.1 Concluída a avaliação da qualidade e da conformidade dos serviços entregues, o gestor do contrato efetuará o recebimento definitivo dos serviços através da confecção e assinatura do Termo de Recebimento Definitivo, com base nas informações da etapa de avaliação da qualidade e contendo a autorização para emissão de Nota(s) Fiscal(is), a ser encaminhado ao Preposto da CONTRATADA.

7.2.1.2.2 Observando de forma complementar o disposto na alínea "c" do inciso II do art. 50 da IN n° 05/SEGES/MPDG, de 26/05/2017, quando houver glosa parcial dos serviços, o Gestor deverá comunicar a empresa para que emita a(s) Nota(s) Fiscal(is) com o valor exato dimensionado, evitando, assim, efeitos tributários sobre valor glosado pela Administração.

7.2.1.2.3 O recebimento definitivo ocorrerá em até 10 (dez) dias úteis depois de concluída a verificação de conformidade e quantidades, ocasião em que será emitido o respectivo TERMO DE RECEBIMENTO DEFINITIVO.

7.2.1.2.4 Será rejeitado, no todo ou em parte, o entregável fornecido em desacordo com as especificações constantes deste Termo de Referência e seus encartes. Ainda, conforme o art. 69 da Lei nº 8.666/1993, a CONTRATADA é obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

7.2.1.2.5 Só haverá o Recebimento definitivo após a análise da qualidade dos serviços, em face da aplicação dos critérios de qualidade e da verificação dos níveis mínimos de serviço, resguardando-se ao CONTRATANTE o direito de não receber o objeto cuja qualidade seja comprovadamente baixa – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no Contrato. Quando for caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

7.3. Procedimentos de Teste e Inspeção

7.3.1 Não se aplica ao objeto de contratação.

7.4. Níveis Mínimos de Serviço Exigidos

7.4.1 Os níveis de serviços seguirão os padrões descritos na tabela abaixo:

Serviço para Solução	Tempo de Resposta Máximo	
Gerenciamento de Configurações: Alteração e inclusão de regras e configurações (após abertura de chamado, exceto quando for necessária uma janela de manutenção)	**Alta**	3 horas
	Média	4 horas
	Baixa	6 horas
Atualização, implementação de patches e fixes (após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA, além da liberação de janela pelo CONTRATANTE)	96 h Chamado de Prioridade Relativa	
Início de atuação remota (VPN ou Telefone) para resolução de problemas (após abertura de chamado ou detecção pela CONTRATADA)	60 min Chamado de Alta prioridade	
Início de atuação remota (VPN ou Telefone) para troubleshooting após queda definitiva do serviço da solução (Indisponibilidade da solução)	45 min Chamado de Alta Prioridade	
Implementação de novos serviços e features de software remotamente (após abertura de chamado na CONTRATADA, exceto quando for necessária uma janela de manutenção)	96 h Chamado de Baixa Prioridade	
RELATÓRIO TÉCNICO: Relatórios da ferramenta com o resumo semanal do serviço	Semana	
RELATÓRIO EXECUTIVO: Relatório com informações gerenciais das correlações e resultados obtidos no mês	Mensal 01 Relatório	
RELATÓRIO EMERGENCIAL: Tratamento de problemas, incidentes e mudanças com a causa raiz ou de mudança emergencial, desde que seja solicitado pelo CONTRATANTE	16 h	

7.4.2 Nível de serviço para atendimento local (on-site)

7.4.2.1 Em no máximo 04 (quatro) horas para suporte no local, após a solicitação de correção de problemas.

7.4.3 Início do atendimento:

7.4.3.1 Hora da abertura do chamado técnico.

7.4.4 Término do chamado:

7.4.4.1 Momento em que o(s) equipamento(s) torna-se operacional e com todas as funcionalidades disponíveis para uso, com ateste do responsável técnico do CONTRATANTE.

7.5 Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

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

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

7.5.1.2 não assinar a ata de registro de preços, quando cabível;

7.5.1.3 apresentar documentação falsa;

7.5.1.4 deixar de entregar os documentos exigidos no certame;

7.5.1.5 ensejar o retardamento da execução do objeto;

7.5.1.6 não mantiver a proposta;

7.5.1.7 cometer fraude fiscal;

7.5.1.8 comportar-se de modo inidôneo.

7.5.2 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

7.5.3 O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

7.5.3.1 Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação, conforme item 7.5.12;

7.5.3.2 Multa, nos percentuais descritos no item 7.5.12;

7.5.3.3 Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

7.5.3.4 Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;

7.5.3.5 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir o Contratante pelos prejuízos causados.

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

7.5.5 Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

7.5.6 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

7.5.7 O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

7.5.8 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

7.5.9 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

7.5.10 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

7.5.11 As penalidades serão obrigatoriamente registradas no SICAF.

7.5.12 Em casos de inconformidade na prestação dos serviços, a CONTRATADA estará sujeita à aplicação das seguintes sanções:

ID	EVENTO	SANÇÃO/MULTA
1	Atraso no fornecimento dos produtos e/ou licenças adquiridos superior ao prazo inicial estipulado de 45 (quarenta e cinco) dias	Multa de 1% (um por cento) por dia sobre o valor do fornecimento com atraso, quando a CONTRATADA deixar de cumprir, dentro do prazo estabelecido, a obrigação assumida. A partir do décimo dia de atraso, essa multa será aplicada em dobro
2	Atraso superior a 20 (vinte) dias no fornecimento dos produtos e/ou licenças adquiridos passados o prazo inicial	Multa de 10% (dez por cento) por dia sobre o valor do contrato, quando a CONTRATADA deixar de cumprir a obrigação assumida
3	Atraso superior a 30 (trinta) dias no fornecimento dos produtos e/ou licenças adquiridos passados o prazo inicial	Será declarada inexecução do contrato
4	Atraso na resolução de atendimento de chamado	Notificação alertando sobre as questões contratuais que devem ser cumpridas e sobre a possibilidade de multa, conforme prazos estipulados nos níveis de serviços
5	Atraso na resolução do atendimento de chamado	Multa de 1% (um por cento) por dia sobre o valor do suporte mensal, quando a CONTRATADA deixar de cumprir, dentro do prazo estabelecido, a obrigação assumida. A partir do décimo dia de atraso, essa multa será aplicada em dobro, conforme prazos estipulados nos níveis de serviços
6	Atraso na resolução de atendimento de chamado superior a 10 (dez) dias.	Multa de 10% (dez por cento) por dia sobre o valor do suporte mensal, quando a CONTRATADA deixar de cumprir a obrigação assumida
7	Atraso na resolução de atendimento de chamado superior a 30 (trinta) dias	Será declarada inexecução do contrato por não cumprimento das cláusulas contratuais
8	Na segunda ocorrência de recusa do produto entregue	Multa de 5% (cinco por cento) sobre o valor do produto e prazo de 5 (cinco) dias para troca do produto entregue. A partir do décimo dia de atraso, essa multa será aplicada em dobro, conforme prazos estipulados nos níveis de serviços
9	Na terceira ocorrência de recusa do produto entregue	Multa de 10% (dez por cento) sobre o valor do produto e prazo de 5 (cinco) dias para troca do produto entregue
10	Após a terceira ocorrência de recusa do produto entregue	Será declarada inexecução do contrato por não cumprimento das cláusulas contratuais

11	Atraso na troca do equipamento e/ou peças defeituosas	Multa de 5% (cinco por cento) sobre o valor do produto por dia
12	Atraso de mais de 2 (dois) dias do prazo estipulado no contrato para troca do equipamento e/ou peças defeituosas	Multa de 10% (dez por cento) sobre o valor do produto por dia
13	Na terceira ocorrência de atraso na troca do equipamento e/ou peças defeituosas	Será declarada inexecução do contrato por não cumprimento das cláusulas contratuais
14	Não informar o nome e o contato dos responsáveis pelo atendimento ao CONTRATANTE	Notificação alertando sobre as questões contratuais que devem ser cumpridas e sobre a possibilidade de multa de 10% (dez por cento) sobre o valor do suporte mensal, por dia de atraso no cumprimento
15	Não utilizar mão de obra qualificada e tecnicamente habilitada para atendimento ao CONTRATANTE	Notificação alertando sobre as questões contratuais que devem ser cumpridas e sobre a possibilidade de multa de 10% (dez por cento) sobre o valor do suporte mensal, por dia até que pessoa qualificada passe a atender às solicitações do CONTRATANTE
16	Deixar de comunicar qualquer anormalidade técnica de caráter urgente para o CONTRATANTE	Notificação alertando sobre as questões contratuais que devem ser cumpridas e sobre a possibilidade de multa de 10% (dez por cento) sobre o valor do suporte mensal, por dia de atraso no cumprimento
17	Deixar de atualizar os softwares necessários para o perfeito funcionamento da solução	Notificação alertando sobre as questões contratuais que devem ser cumpridas e sobre a possibilidade de multa de 10% (dez por cento) sobre o valor do suporte mensal, por dia de atraso no cumprimento
18	Primeira ocorrência de descumprimento dos níveis de serviços estabelecidos	Notificação alertando sobre as questões contratuais que devem ser cumpridas e sobre a possibilidade de multa, conforme prazos estipulados nos níveis de serviços
19	Segunda ocorrência de descumprimento dos níveis de serviços estabelecidos	Multa de 1% (um por cento) por dia sobre o valor do serviço total contratado, quando a CONTRATADA deixar de cumprir, dentro do prazo estabelecido, a obrigação assumida
20	Terceira ocorrência de descumprimento dos níveis de serviços estabelecidos	Multa de 10% (dez por cento) por dia sobre o valor do serviço total contratado, quando a CONTRATADA deixar de cumprir a obrigação assumida
21	Inexecução parcial ou total do contrato, por não cumprimento de cláusulas contratuais	Suspensão temporária de participar em licitação e impedimento de contratar com a Administração, pelo prazo não superior a 2 (dois) anos mais multa de 10% (dez por cento) sobre o valor global do contrato

7.6. Do Pagamento

7.6.1 Os pagamentos dos itens 1 e 2 do objeto ocorrerão em parcela única, após a emissão do Termo de Recebimento Definitivo. O prazo para pagamento será de até 30 (trinta) dias, contados do recebimento da respectiva Nota Fiscal/Fatura;

7.6.2 O pagamento do item 3 do objeto, Serviço de instalação do gerenciamento centralizado e repasse de conhecimento ocorrerá em parcela única, após a efetiva realização dos procedimentos necessários com objetivo de disponibilizar a solução de segurança em produção. O prazo para pagamento será de até 30 (trinta) dias contados do recebimento da respectiva Nota Fiscal/Fatura;

7.6.3 O pagamento do item 4 do objeto, serviço de gerenciamento e suporte técnico para toda a solução será pago mensalmente. O prazo para pagamento será de até 30 (trinta) dias, contados do recebimento da respectiva Nota Fiscal/Fatura e do relatório mensal da manutenção preventiva, devidamente assinado por representante da equipe técnica do CONTRATANTE e da CONTRATADA, sendo obrigatória a sua apresentação;

7.6.3.1 O pagamento do item 4 do objeto, serviço de gerenciamento e suporte terá seu valor reajustado seguindo o índice ICTI (Índice de Custo da Tecnologia da Informação).

7.6.4 A apresentação da Nota Fiscal/Fatura deverá ocorrer no prazo de 10 (dez) dias, contado da data final do período de adimplemento da parcela da contratação a que aquela se referir;

7.6.5 O pagamento somente será autorizado depois de efetuado o "atesto" pelo servidor competente, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação aos serviços efetivamente prestados e aos materiais empregados;

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

7.6.7 Nos termos do artigo 36, § 6°, da Instrução Normativa SLTI/MPOG n° 02, de 2008, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

7.6.7.1 Não produziu os resultados acordados;

7.6.7.2 Deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

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

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

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

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

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

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

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

6.7.14 Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante, não será rescindido o contrato em execução com a contratada inadimplente no SICAF;

6.7.15 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável;

6.7.16 A contratada regularmente optante pelo Simples Nacional não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar;

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

EM = I x N x VP, sendo:

EM = Encargos moratórios

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

VP = Valor da parcela a ser paga

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

I = (TX)	I = (6/100)/365	I = 0,00016438 TX = Percentual da Taxa Anual = 6%

8 – ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1 A estimativa de custo total para a aquisição de licenciamento do software antivírus corporativo com suporte e garantia, de acordo com as necessidades do MCOM, é de R$ 820.745,00 (oitocentos e vinte mil e setecentos e quarenta e cinco reais), pelo período de 36 (trinta e seis) meses.

8.2 A metodologia utilizada para definição do valor estimado foi a mediana**,** uma vez que nas comparações de modo geral, representa melhor o valor típico da amostra, pois não é distorcida por valores extremamente altos ou baixos.

8.3 Diante do valor da estimativa de preço não atrai a necessidade de sua aprovação pelo Órgão Central do SISP (art. 1º, §2º, da IN SGD/ME nº 1/2019).

GRUPO	ITEM	DESCRIÇÃO	CÓDIGO CATSER/CATMAT	UNIDADE DE MEDIDA	QUANTIDADE PREVISTA	VALOR UNITÁRIO	VALOR TOTAL
1	1	Solução de Next Generation Antimalware com gerenciamento centralizado, análise forense, detecção e respostas a incidentes	27472	Licenças	1.300	R$375,00	R$487.500,00
	2	Instalação e configuração	27260	Serviços	1.300	R$46,15	R$59.995,00
	3	Serviço de instalação do gerenciamento centralizado e repasse de conhecimento	27260	Serviços	1	R$21.250,00	R$21.250,00
	4	Serviço de gerenciamento e suporte da solução por 36 meses.	27260	Serviços Mensal	36	R$7.000,00	R$252.000,00
						VALOR GLOBAL	**R$820.745,00**

9 – ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA DE EXECUÇÃO FÍSICO-FINANCEIRA

9.1 Os recursos orçamentários, para fazer frente às despesas desta contratação serão definidos de acordo com o art. 7° § 2° do Decreto nº 7.892/2013, *in verbis:*

> "Na licitação para registro de preços não é necessário indicar a dotação orçamentária, que somente será exigida para a formalização do contrato ou outro instrumento hábil".

9.2 As despesas estão programadas em dotação orçamentária própria, e correrão dos recursos orçamentários constantes do Orçamento Geral da União, aprovado pela Lei Orçamentária Anual - LOA para o exercício de 2021.

9.3 A adoção do Sistema de Registro de Preços – SRP, conforme Orientação Normativa AGU nº, de 1º de abril de 2009 ("Na Licitação para Registro de Preços, a indicação da dotação orçamentária é exigível apenas antes da assinatura do contrato").

9.4 A seguir, estima-se o cronograma de execução físico-financeira:

CRONOGRAMA DE EXECUÇÃO				PREVISÃO DE DESEMBOLSO		
ITEM	DESCRIÇÃO	QUANTIDADE PREVISTA	DATA	1º ANO	2º ANO	3º AI
1	Solução de Next Generation Antimalware com gerenciamento centralizado, análise forense, detecção e respostas a incidentes e repasse de conhecimento	1.300	Até 45 (quarenta e cinco) dias após a assinatura do Contrato e após a emissão do Termo de Recebimento Definitivo	R$ 487.500,00	-	-
2	Instalação e configuração	1.300	Até 15 (quinze) dias a partir do Termo de Recebimento Definitivo e após a	R$59.995,00	-	-

			Instalação, configuração e repasse de conhecimento			
3	Serviço de instalação do gerenciamento centralizado e repasse de conhecimento	1	Até 15 (quinze) dias a partir do Termo de Recebimento Definitivo e após a Instalação, configuração e repasse de conhecimento	R$21.250,00	-	-
4	Serviço de gerenciamento e suporte da solução por 36 meses	36	Após a execução do item 2 e 3 do objeto. Pagamento mensal	R$84.000,00	R$84.000,00	R$84.0
			VALOR TOTAL	R$652.745,00	R$84.000,00	R$84.0
			VALOR GLOBAL	**R$820.745,00**		

10 – DA VIGÊNCIA DO CONTRATO

10.1. O prazo de vigência contratual é de **36 (trinta e seis) meses**, a contar da data de sua assinatura, podendo, no interesse da administração, ser prorrogado pelo período de 12 (doze) meses mediante Termo Aditivo, observado o limite máximo de 60 (sessenta) meses, desde que mantida a obtenção de preços e condições mais vantajosas para a Administração, nos termos do art. 57, inciso II, da Lei nº 8.666/93, com suas posteriores alterações.

10.2. A prorrogação do contrato dependerá da verificação da manutenção da necessidade, economicidade e oportunidade da contratação, acompanhada de a realização de pesquisa de mercado que demonstre a vantajosidade dos preços contratados para a Administração.

11 – DO REAJUSTE DE PREÇOS (quando aplicável)

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

11.2 Após o interregno de um ano, e independentemente de pedido da CONTRATADA, os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, do índice ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA, <Acesso em: http://www.ipea.gov.br/cartadeconjuntura/index.php/tag/icti/>, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, com base na seguinte fórmula (art. 5º do Decreto n.º 1.054, de 1994):

R = V (I – Iº) / Iº, onde:

R = Valor do reajuste procurado;

V = Valor contratual a ser reajustado;

Iº = índice inicial - refere-se ao índice de custos ou de preços correspondente à data fixada para entrega da proposta na licitação;

I = Índice relativo ao mês do reajustamento;

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

11.4.No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

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

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

11.7 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.

11.8 O reajuste será realizado por apostilamento.

12 – DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. Regime, Tipo e Modalidade da Licitação

12.1.1 A contratação do objeto petendido se refere à "bens e serviços" comuns, de caráter continuado e sem fornecimento de mão de obra em regime de dedicação exclusiva, a ser contratado mediante licitação, por meio do Sistema de Registro de Preços, na modalidade pregão, em sua forma eletrônica, com julgamento pelo critério de **MENOR PREÇO GLOBAL**, com vistas à aquisição de solução de *next generation antimalware* (antivírus), com gerenciamento centralizado, análise forense, detecção e respostas a incidentes.

12.1.2 A licitação será composta por um 1 (um) grupo, formado por 4 (quatro) itens.

12.2 Adoção do Sistema de Registro de Preços (se aplicável)

12.2.1 À luz do princípio da eficiência, o SRP tem por escopo instrumentalizar meios para aquisição parcelada de bens e serviços na Administração Pública, sendo, portanto, compatível com a Lei do Pregão nº 10.520/02.

12.2.2 Desta forma, a adoção do SRP, enquadra-se nas hipóteses previstas no Decreto nº 7.892/2013:

"Art. 3- O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:

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

II – quando o for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;

III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo: ou

IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração."(griffos nossos)

12.2.3 Posto isto, em função dos aspectos técnicos e requisitos que envolvem a execução dos serviços e considerando o grau de interação do conjunto de serviço técnico descrito no presente Termo de Referência, natureza específica, caráter contínuo, características de especificidade, aliada a criticidade e complexidade que envolve a prestação de serviço desta contratação, justifica-se a adoção do SRP pelo fato do MCOM ser um órgão novo e podem ocorrer demandas ao longo dos 12 meses de vigência da Ata, bem como por não ser possível definir previamente o quantitativo exato a ser demandado pela Administração.

12.3 Adesão a Ata de Registro de Preços por órgãos ou entidades

12.3.1 O setor técnico optou pela não divulgação da Intenção de Registro de Preços - IRP, em virtude da ausência de estrutura administrativa satisfatória para fins de gerenciamento de demandas advindas de outros órgãos interessados na contratação, bem como pela necessidade de realização e conclusão célere deste procedimento licitatório, evidencia-se ser inviável para o MCOM. Outrossim, caso o quantitativo e as especificações técnicas sejam alteradas para adequar a demanda de eventuais partícipes, a pesquisa de preços teria que ser atualizada e a contratação certamente seria atrasada.

12.3.2 Por tais razões, justifica-se a dispensa da divulgação da intenção de registro de preços.

12.4 Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência

12.4.1 Em atenção ao Acórdão 1352/2018 – TCU – Plenário, orienta-se aos órgãos integrantes do Sistema de Serviços Gerais (Sisg), quando da contratação de serviços de tecnologia da informação associados ao fornecimento ou locação de bens, devem ser aplicadas as regras de preferência dispostas no Decreto nº 7.174, de 12 de maio de 2010.

12.4.2 Entretanto, não se aplica ao objeto desta contratação devido aos itens serem agrupados em um único lote.

12.5 Critérios de Qualificação Técnica para a Habilitação

12.5.1 As empresas deverão comprovar a aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, nos termos definidos a seguir:

12.5.1.1 A licitante deve ter executado, por no mínimo 12 meses, em contrato único ou separado, serviços de entrega, instalação, configuração e suporte técnico de solução de segurança de Next Generation Altimalware em pelo menos 50% (cinquenta por cento) do quantitativo estimado, por este Termo de Referência.

12.5.2 A(s) Licitante(s) deverá(ão) apresentar:

a) atestado(s) que se refiram a contratos já concluídos ou já decorrido no mínimo um ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior devendo ser comprovado por meio do contrato;

b) atestado(s) que se refiram a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

12.5.3 No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente.

12.5.4 Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente empresas controladas ou controladoras da empresa proponente ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

12.5.5 A comprovação será realizada por qualquer processo de cópia reprográfica, ou por servidor da Administração, desde que conferido(s) com o original, ou publicação em órgão da imprensa oficial.

12.5.6 A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, consoante o disposto no item 10.10 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

12.5.7 É facultada a instauração de diligência destinada a esclarecer ou a confirmar a veracidade das informações prestadas pela licitante constantes de sua Comprovação de Capacidade Técnica, Proposta de Preços e de eventuais documentos anexados.

12.6 Participação de consórcios

12.6.1 É vedada a participação de empresas em consórcio ou cooperativas; qualquer que sua forma de constituição, considerando as características específicas da contratação dos serviços a serem fornecidos, que não pressupõem multiplicidade de atividades empresariais distintas para execução do objeto.

12.7 Da subcontratação

12.7.1 Não será permitida a subcontratação em parte ou total do objeto licitado.

13 – DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

13.1 A Equipe de Planejamento da Contratação foi instituída pela **Portaria nº 3990/2021/SEI-MCOM, de 3 de novembro 2021 (SEI nº 8356968).**

13.2 Certificamos que as diretrizes estabelecidas no termo de referência são as adequadas ao atendimento do interesse público envolvido, estando compatíveis com o estudo técnico preliminar da contratação. Além disso, o instrumento contém todos os elementos necessários para a caracterização da contratação, conforme disposição do art. 3º, inciso XI do Decreto nº 10.024, de 2019.

13.3 Certificamos, ainda, que as especificações técnicas previstas neste Termo de Referência atendem às premissas contidas no o art. 16 da IN SGD/ME nº 01, de 2019.

13.4 Foram observados, neste Termo de Referência, os guias, manuais e modelos publicados pelo Órgão Central do SISP (art. 8º, §2, da IN SGD/ME nº 1/2019).

13.5 Conforme o §6º do art. 12 da IN SGD/ME nº 01, de 2019, o Termo de Referência ou Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

13.6 São partes integrantes deste Termo de Referência os seguintes anexos:

13.6.1 ANEXO A - ESPECIFICAÇÃO TÉCNICA;

13.6.2 ANEXO B - MODELO DE PROPOSTA DE PREÇOS;

13.6.3 ANEXO C - DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL;

13.6.4 ANEXO D - TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO;

13.6.5 ANEXO E - TERMO DE CIÊNCIA;

13.6.6 ANEXO F - MODELO DE ORDEM DE SERVIÇO;

13.6.7 ANEXO G - TERMO DE RECEBIMENTO PROVISÓRIO;

13.6.8 ANEXO H - TERMO DE RECEBIMENTO DEFINITIVO.

Integrante Requisitante	**Integrante Técnico**	**Integrante Administrativo**
Daniele Meira Borges Coordenadora de Governança de TI Matrícula/SIAPE: 1793595 *(assinado eletronicamente)*	**Filipe Carneiro Guimarães** Coordenador de Infraestrutura e Serviços de TI Matrícula/SIAPE: 1443304 *(assinado eletronicamente)*	**Kelma Regina Batista e Silva Araújo** Chefe de Serviço de Licitações Matrícula/SIAPE: 1354569 *(assinado eletronicamente)*

Autoridade Máxima da Área de TIC
Wanessa Queiroz de Souza Oliveira Subsecretária de Planejamento e Tecnologia da Informação Matrícula/SIAPE: 1905250 *(assinado eletronicamente)*

Aprovo,

Autoridade Competente
Ivancir Gonçalves da Rocha Castro Filho Coordenador Geral de Recursos Logísticos *(assinado eletronicamente)*

ANEXOS

A - ESPECIFICAÇÃO TÉCNICA

1. Características Técnicas

1.1 Toda solução de segurança proposta deverá ser fornecida por um único fabricante, de modo que, tanto o suporte à solução quanto as funcionalidades, sejam inteiramente integradas e gerenciadas através de uma única console de gerenciamento;

1.2 A solução de proteção para endpoint deve prover identificação positiva e proteção contra ameaças em programas maliciosos conhecidos e desconhecidos. As ameaças devem ser identificadas e neutralizadas, incluindo o código executável, scripts e exploits.

2. Solução para estações de trabalho e servidores

2.1 Suporte total para os seguintes sistemas operacionais:

- Windows Server 2016 (64 bits);
- Mac OS X 10.9 (Mavericks);
- Mac OS X 10.10 (Yosemite);
- Mac OS Sierra;
- Red Hat Enterprise Linux 6.6 - 64-bit;
- Red Hat Enterprise Linux 6.7 - 64-bit;
- Red Hat Enterprise Linux 6.8 - 64-bit;
- Red Hat Enterprise Linux 7.0 - 64-bit;
- Red Hat Enterprise Linux 7.1 - 64-bit;
- Red Hat Enterprise Linux 7.2 - 64-bit;
- Red Hat Enterprise Linux 7.3 - 64-bit.

2.1.1 A instalação da solução de Next Generation Antimalware deve aceitar parâmetros de configuração e distribuição, como instalação silenciosa e definição de diretório de instalação;

2.1.2 Deve permitir a utilização de senha para prevenir a desinstalação do produto nas estações/servidores;

2.1.3 Deve possuir serviço de proteção contra finalização (kill) do processo da ferramenta. Também deve impedir que outros aplicativos efetuem a finalização do serviço;

2.1.4 Todas as funcionalidades desta ferramenta devem ser ativadas por um único produto, facilitando a instalação, a configuração e o gerenciamento;

2.1.5 O funcionamento da solução deve operar analisando a execução da ameaça em potencial, nas camadas do Sistema Operacional (O/S), Memória e prevenindo a entrada de códigos maliciosos;

2.1.6 Capacidade de análise automática do código do arquivo, identificando suas características antes da sua capacidade de execução;

2.1.7 A solução deve aplicar análise baseada em algoritmo matemático, para identificar programas maliciosos antes da sua execução;

2.1.8 Caso seja identificado um programa malicioso, a sua execução não deve ser permitida;

2.1.9 A solução deve identificar e bloquear a execução de códigos executáveis (binários), scripts ou comandos;

2.1.10 A solução de endpoint deve detectar e prevenir qualquer alteração oriunda de código malicioso ou não-autorizado em programas que estejam sendo executados em memória;

2.1.11 Deve utilizar a tecnologia de “Machine Learning” para identificar qualquer ameaça nos arquivos potencialmente perigosos;

2.1.12 A análise do malware deve ocorrer em pré-execução, ou seja, o código malicioso deve ser bloqueado antes de executar e infectar a máquina.

2.1.12.1 No processo de detecção e bloqueio em pré execução, não serão aceitas tecnologias que fazem uso de análise de hashing do arquivo ou verificação do arquivo em nuvem.

2.1.13 Identificar ameaças avançadas (APTs), chamadas de zero day, e ransomwares sem a necessidade de base de assinaturas, detecção por heurística, detecção por hashing, detecção por comportamento ou sandboxing. Todas as detecções devem ser feitas em tempo real;

2.1.14 Deve permitir controlar dispositivos de armazenamento conectados via USB, permitindo bloquear o acesso ou liberar. Adicionalmente, deve ser possível a criação de exceções na política, pelo número de série, identificador do fabricante e tipo de dispositivo;

2.1.15 O controle do acesso via USB deve ter a capacidade mínima de controlar os seguintes dispositivos:

2.1.15.1 Dispositivos Android;

2.1.15.2 Dispositivos Apple IOS;

2.1.15.3 Dispositivos Still Image como câmeras e Scanners;

2.1.15.4 Dispositivos de armazenamento CD, DVD RW;

2.1.15.5 Dispositivos USB Drive (Pen Drive);

2.1.15.6 Dispositivos VMWARE USB Passthrough;

2.1.15.7 Dispositivos portáteis Windows.

2.1.16 A solução não deve depender de base de assinaturas e hashes para identificação de qualquer ameaça;

2.1.17 Capacidade de extrair características dos arquivos potencialmente perigosos e aplicar algoritmos de análise para determinar sua intenção;

2.1.18 Prover proteção em tempo real, independente do estado de conexão da máquina, sendo:

2.1.18.1 Online – Com conexão com a Internet;

2.1.18.2 Offline – Sem conexão com a Internet.

2.1.19 Os módulos de proteção de memória e controle de execução devem prevenir técnicas de ataques do tipo:

2.1.19.1 Hijacking;

2.1.19.2 File Injection;

2.1.19.3 File Overflow;

2.1.19.4 In-Memory execution;

2.1.19.5 Exploitation - Stack Pivot, Stack protect, Overwrite Code, RAM Scraping e Malicius Payload;

2.1.19.6 Process Injection – Remote Allocation of Memory, Remote Mapping of Memory, Remote Write to Memory, Remote Write PE to Memory, Remote Overwrite Code, Remote Unmap of Memory, Remote Thread Creation, Remote APC Scheduled e DYLD Injection (Apenas para MacOS X);

2.19.7 Escalation – LSASS Read e Zero Allocate.

2.1.20 O módulo de proteção de memoria deve possuir as seguintes ações em caso de violação:

2.1.20.1 Ignorar;

2.1.20.2 Alertar;

2.1.20.3 Bloquear;

2.1.20.4 Terminar.

2.1.21 O módulo de controle e analise de scripts deve ser capaz de analisar no mínimo as seguintes linguagens:

2.1.21.1 PowerShell;

2.1.21.2 Active Scripts – Jscript, WScript, CScript, macros, VBA.

2.1.22 O módulo de controle e analise de scripts deve possuir as seguintes ações em caso de violação:

2.1.22.1 Alertar;

2.1.22.2 Bloquear.

2.1.23 Caso ocorra alguma identificação de código malicioso em scripts, a ferramenta deve agir no interpretador e prevenir sua execução imediata;

2.1.24 Deve ser capaz de finalizar processos e sub processos em execução, caso haja a identificação de algum código malicioso sendo executado nos mesmos;

2.1.25 Possuir funcionalidade para análise contra ameaças em background, permitindo análises periódicas no disco contra ameaças inativas. Esta análise apenas poderá ser feita quando a estação/servidor estiver em modo ocioso, ou seja, com os recursos disponíveis para execução desta ação;

2.1.26 Permitir a verificação de ameaças em apenas novos arquivos;

2.1.27 Deve ser capaz de analisar arquivos compactados, como:

2.1.27.1 ZIP;

2.1.27.2 RAR;

2.1.27.3 GZIP;

2.1.27.4 TAR;

2.1.27.5 JAR;

2.1.27.6 WAR

2.1.28 Deve ser possível a configuração de limite de tamanho para análise de arquivos compactados;

2.1.29 Gerar registro (log) dos eventos de detecção de ameaças em arquivo local, com opção de upload para a console de gerenciamento;

2.1.30 Gerar notificações de eventos de ameaças através de alerta via Syslog ou por email;

2.1.31 Deve possuir um módulo integrado de AntiExploit, permitindo identificar e bloquear a execução de Exploits na máquina em memória. Este módulo deve permitir, no mínimo, a proteção contra ferramentas de injeção de código malicioso, como por exemplo o Shelter, além de detectar e evitar a execução de backdoors;

2.1.32 Deve possuir módulo integrado de bloqueio de Exploits e não deve ser baseado em assinaturas. Deve ser capaz de bloquear estas ameaças utilizando o próprio engine de inteligência artificial e machine learning;

2.1.33 No modo desconectado, o endpoint deve fazer a detecção e bloqueio usando unicamente o algoritmo matemático. Não serão permitidas soluções hibridas que utilizem assinaturas, hashes ou consultas na Internet (Cloud Lookups) para a detecção neste cenário;

2.1.34 O endpoint deve ser certificado pela Microsoft como uma ferramenta de Antivírus. Sendo assim, nas plataformas Windows, a ferramenta deve ser identificado como solução de Antivírus.

2.2 Módulo de Análise Forense e detecção e respostas (EDR)

2.2.1 O módulo de análise forense e detecção e respostas (EDR) deve permitir a monitoração contínua dos eventos, captura e gravação em modo seguro. Este módulo deve permitir analisar o comportamento do usuário ou do malware no endpoint;

2.2.2 Este módulo deve obrigatoriamente estar integrado ao agente do Next Generation Antimalware, não sendo permitida a adição de agentes adicionais;

2.2.3 O módulo deve ter a capacidade de coletar informações dos processos em execução da máquina e o motivo para a terminação dos processos;

2.2.4 O módulo deve permitir visualizar através da console web uma linha do tempo gráfica, contendo toda a sequência de eventos que ocorreram durante a execução do malware, sendo possível ainda expandir os detalhes de cada informação;

2.2.5 O módulo deve identificar processos que tenham sido suspensos;

2.2.6 Devem ser fornecidas na console, informações do identificador do processo (Process ID), nome do processo, a linha de comando de execução, o usuário logado que executou o processo, o caminho do executável, e quando disponível o hash MD5 do processo;

2.2.7 O módulo deve reportar eventos maliciosos em memória sendo que devem ser fornecidas no log do evento, os grupos, SID, e quantas vezes o código malicioso tentou executar em memória;

2.2.8 O módulo deve detectar a injeção de ameaças em funções e módulos do programa (aplicativo) executado;

2.2.9 Deve identificar processos suspeitos que executam em localidades não comuns, como diretórios de dados e lixeira;

2.2.10 Deve identificar processos que estabelecem conexões de rede externas e suspeitas (call back);

2.2.11 Quanto as conexões de redes externas e suspeitas devem ser reportadas no log, a origem da conexão, o destino, o tempo de início e/ou término da conexão;

2.2.12 Deve identificar alterações não comuns em áreas do registro da máquina;

2.2.13 Deve monitorar alterações em tarefas agendadas na máquina;

2.2.14 Deve monitorar tentativas de escalação de privilégios;

2.2.15 Deve possuir a capacidade de armazenar toda a informação forense de forma criptografada na própria estação;

2.2.16 O administrador da console de gerenciamento pode solicitar o envio destas informações para a gerência;

2.2.17 Deve possuir a capacidade de realizar busca de ameaças na rede (IOC hunting) por arquivos, hashes, processos, alterações de chaves de registros e conexões de rede;

2.2.18 Deve permitir realizar um isolamento completo da máquina que foi identificada a ameaça, este isolamento evita a propagação da mesma pela rede;

2.2.19 O agente deve ter a capacidade de fazer o isolamento da máquina por si só, sem necessitar de nenhuma integração com outros softwares ou dispositivos de rede para isso;

2.2.20 Este isolamento pode ser realizado por um tempo específico não inferior a 5 minutos, onde deve ser possível ao administrador fornecer uma chave para realizar a liberação da máquina isolada. Durante o período de isolamento, a máquina não poderá realizar nenhuma conexão de rede, ficando completamente sem acesso à rede de dados;

2.2.21 Deve ter a capacidade de realizar, através da solução, o envio do arquivo da ameaça ao sistema de gerenciamento em cloud, para análise posterior. O módulo de análise forense ou EDR deve possuir a capacidade de identificação automática de comportamentos maliciosos executados no EndPoint através de um conjunto mínimo de 20 regras;

2.2.22 As regras devem apresentar três níveis de criticidade: alto, médio e baixo;

2.2.23 As regras devem identificar pelo menos os seguintes conjuntos de ações:

2.2.23.1 Tentativas de mascarar ou matar os processos no NGAM;

2.2.23.2 Detecção de Fileless Powershell malware;

2.2.23.3 Detecção da execução de comandos maliciosos em Powershell, como comandos que ocultam a execução do Powershell;

2.2.23.4 Invocação maliciosa de JavaScritps com Rundll;

2.2.23.5 Processos de Sistema Operacional iniciados por usuários que não são SYSTEM;

2.2.23.6 Executáveis iniciados do Recycle Bin;

2.2.23.7 Executável criado ou lançado como executável do Windows;

2.2.23.8 Processos do Windows sendo executados em pastas não padrão;

2.2.23.9 Processos criados com nomes confusos (tentando se passar por processos do Windows);

2.2.23.10 Uso do PSEXEC;

2.2.23.11 Modificação de host files;

2.2.23.12 Tentativa de invocação do Remote Shell; Detecção de executável com múltiplas extensões;

2.2.23.13 Tarefas agendadas suspeitas.

2.2.24 Após identificar estes comportamentos o módulo de EDR deve ter a capacidade de realizar uma ação automática (sem a intervenção do operador), entre as ações automáticas customizadas, devem estar incluídas:

2.2.24.1 Apagar arquivos;

2.2.24.2 Realizar Log Off de todos os usuários, ou usuários remotos, ou usuários interativos;

2.2.24.3 Suspender e terminar processos;

2.2.24.4 Gerar log de aplicação.

2.2.25 Através do dashboard deve ser possível requisitar e fazer download dos logs e evidências causa-raiz, os arquivos maliciosos ou adicionar os mesmos a quarentena global.

2.3 Gerenciamento da solução de segurança

2.3.1 Possuir gerência centralizada e integrada, a partir de uma única console, para as todas as ferramentas integradas de segurança em estações de trabalho e servidores, de onde seja possível manter a proteção atualizada, gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

2.3.2 Deve ser possível o gerenciamento de no mínimo 1.300 máquinas;

2.3.3 Deve permitir o acesso a console de gerenciamento Web, com acesso através de protocolo seguro (HTTPS);

2.3.4 Deve possuir relatórios na console WEB, estes relatórios devem permitir serem exportados em formato PDF;

2.3.5 Deve possuir relatórios que permitam no mínimo: ter um sumário das ameaças identificadas, identificar ameaças que são Anti-VM, identificar ameaças que possam ter comprometido credenciais, apresentem um sumário de proteção de memória, dos processos maliciosos e um sumário dos dispositivos, identificando qual a versão do agente está instalado em cada um deles;

2.3.6 Possuir comunicação segura padrão SSL entre os servidores e as consoles de gerenciamento da solução de segurança;

2.3.7 Permitir o gerenciamento através de console Web compatível com Mozilla Firefox e Google Chrome;

2.3.8 Deve permitir a definição de níveis diferentes de administração, onde administradores gerenciem, com diferentes níveis de privilégios, grupos de máquinas em diferentes partes do ambiente, havendo, contudo, um grupo de administradores que poderá ter uma visão completa de todo o ambiente instalado;

2.3.9 Deve permitir integração com diferentes ferramentas de SIEM, com opção de configurar qual informação será repassada, como:

2.3.9.1 Log de Auditoria;

2.3.9.2 Dispositivos;

2.3.9.3 Proteção de Memória;

2.3.9.4 Script Control;

2.3.9.5 Ameaças;

2.3.9.6 Classificação de Ameaças;

2.3.9.7 Controle de Aplicação.

2.3.10 Deve permitir a atualização automática dos agentes, com possibilidade de permitir a homologação da atualização em zona específica e, posteriormente, para o ambiente de produção;

2.3.11 Deve suportar a inclusão de certificados digitais para que arquivos assinados com estes certificados estejam dentro de uma lista segura (Safe List) para a execução;

2.3.12 Possuir integração a serviços de diretório LDAP, inclusive Microsoft Active Directory, permitindo a criação de regras para a adição direta das máquinas para os grupos/subgrupos e da console de gerenciamento, da mesma forma que estão nos containers do Active Directory;

2.3.13 Forçar a configuração determinada no servidor para os clientes;

2.3.14 Através do console da ferramenta deve ser exibido à lista dos clientes (servidores e estações), online e offline, que possuem o endpoint instalado, contendo as informações necessárias de rede a respeito deles.

2.3.15 Ferramenta deve prover indicadores a partir do seu console único para monitoramento do ambiente.

2.3.16 Capacidade de exportar os indicadores para o formato CSV;

2.3.17 Possibilitar a verificação no site “Vírus Total”, através de link pré-definido no resultado de uma detecção; Possuir módulo que registre em arquivo de log todas as atividades efetuadas pelos administradores permitindo execução de analises em nível de auditoria;

2.3.18 Possuir um painel de controle contendo em tempo real, os indicadores que os administradores da solução julguem necessários para monitorar o ambiente.

B - Modelo de Proposta de Preços

PREGÃO:	**Pregão Eletrônico SRP n° ____/20XX**
UASG:	
OBJETO	

Grupo	Item	Descrição	Quantidade	UNIDADE DE MEDIDA	Valor unitário (R$)	Valor total (R$)
1	1	Solução de Next Generation Antimalware com gerenciamento centralizado, análise forense, detecção e respostas a incidentes	1.300	LICENÇAS		
	2	Instalação, configuração e repasse de conhecimento	1.300	SERVIÇOS		
	3	Serviço de instalação do gerenciamento centralizado e repasse de conhecimento	1	SERVIÇOS		
	4	Serviço de gerenciamento e suporte da solução por 36 meses	36	SERVIÇOS MENSAL		
VALOR TOTAL						

IDENTIFICAÇÃO DA EMPRESA LICITANTE:		
Razão Social:		
CNPJ:		
Endereço Completo		
CEP:	Fone/Fax:	E-mail:
DADOS BANCÁRIOS:		
Agência:	Conta Corrente:	Banco:
IDENTIFICAÇÃO DO RESPONSÁVEL PELA ASSINATURA DO CONTRATO:		
Nome Completo (sem abreviaturas):		
CPF:	IDENTIDADE / ÓRGÃO EXPEDITOR:	
Cargo / Função:		
Endereço Completo:		
Cidade / UF:	CEP:	

Demais condições:

1. Ao efetuar essa proposta, esta empresa proponente declara ter tomado pleno conhecimento do Edital, do Termo de Referência e dos demais documentos integrantes da presente licitação estando ciente das obrigações das partes e das condições de prestação dos serviços.
2. Esta empresa proponente declara atender aos requisitos de capacidade técnica adequada para execução do objeto.
3. Esta empresa proponente declara que todas as despesas diretas e indiretas envolvidas no provimento dos serviços estão incluídas nos valores desta proposta de preços e que esses preços são exequíveis.
4. Esta empresa atesta a não aplicação da prática do "registro de oportunidade" para o objeto ofertado na presente proposta comercial, conforme disposto na Lei 8.666/1993, art. 3º, caput e nos termos do Acórdão-TCU 928/2020-Plenário.

Local e data: _____, _____ de _____de 20xx.

_____
Razão Social e CNPJ da Empresa Proponente

_____
Identificação e Assinatura do Representante Legal da Empresa Proponente

Prazo de validade da proposta: ..... (.....) dias, contados da data limite estipulada para a apresentação.

INSTRUÇÕES:

1. A descrição e a disposição de itens da proposta de preços devem obedecer ao padrão proposto. Os valores correspondentes a cada item devem ser informados em separado, considerando seus preços unitários e totais (por item).

3. Para a fase de habilitação técnica, anexo à proposta, devem ser apresentados os documentos necessários e suficientes para a comprovação do atendimento aos critérios técnicos de habilitação, conforme definido no item xx do TERMO DE REFERÊNCIA.

4. Conforme súmula TCU 254/2010 o Imposto de Renda Pessoa Jurídica (IRPJ) e a Contribuição Social Sobre o Lucro Líquido (CSLL) não devem constar da composição de preços da proposta.

5. À proposta é necessário juntar cópia dos principais documentos da empresa (alteração contratual ou procuração) e do responsável (documento de identidade, CPF ou CNH).

6. A proposta deve ter validade de, no mínimo, 90 (noventa) dias

C - Declaração de Sustentabilidade Ambiental

Declaração de Sustentabilidade	
PROPONENTE:	
CNPJ/RFB:	
ENDEREÇO:	
Declaro, sob as penas da Lei nº 6.938/1981, na qualidade de proponente do procedimento licitatório, sob a modalidade Pregão Eletrônico nº ____/_____, instaurado pelo Processo de nº _____, que atendemos aos critérios de qualidade ambiental e sustentabilidade socioambiental, respeitando as normas de proteção do meio ambiente. Estou ciente de que todos os resíduos sólidos gerados pelos produtos fornecidos que necessitam de destinação ambientalmente adequada (incluindo embalagens vazias) deverão ter seu descarte adequado, obedecendo aos procedimentos de logística reversa, em atendimento à LEI Nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos, em especial a responsabilidade compartilhada pelo ciclo de vida do produto, me comprometendo a aplicar o disposto nos artigos de 31 a 33 da Lei nº 12.305/2010 e nos artigos 13 a 18 do Decreto nº 7.404/2010, principalmente, no que diz respeito à LOGÍSTICA REVERSA. Estou ciente da obrigatoriedade da apresentação das declarações e certidões pertinentes dos órgãos competentes quando solicitadas como requisito para habilitação e da obrigatoriedade do cumprimento integral ao que estabelece o art. 6º e seus incisos, da Instrução Normativa nº 01, de 19 de janeiro de 2010, do Ministério do Planejamento, Orçamento e Gestão – MPOG e Decreto nº 7746 de 5 de junho de 2012, que estabelece critérios, práticas e diretrizes para a	

promoção do desenvolvimento nacional sustentável.

Estou ciente da obrigatoriedade da apresentação do registro no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais caso minha empresa exerça uma das atividades constantes no Anexo II da Instrução Normativa nº 31, de 03 de dezembro de 2009, do IBAMA.

Por ser a expressão da verdade, firmamos a presente DECLARAÇÃO.

_____ de _____ de _____.

_____

Nome:

RG/CPF:

Cargo:

D - Termo de Compromisso de Manutenção do Sigilo

Este TERMO DE COMPROMISSO ("TERMO") é celebrado entre:

1. CONTRATANTE Ministério XXXX, Endereço: _____, CEP _____, Brasília/DF, inscrito no CNPJ/MF _____, neste ato representado pelo Gestor do Contrato xx/xxxx, e
2. CONTRATADA xxxxxxxx, Endereço xxxxxxxx, inscrita no CNPJ/MF xxxxxx, personificação xxxxxx, neste ato representada por seus respectivos procuradores abaixo assinados, na forma de seus respectivos Contratos Sociais.

A CONTRATANTE e a CONTRATADA podem ser referidas individualmente como PARTE e coletivamente como PARTES, onde o contexto assim o exigir.

CONSIDERANDO QUE as PARTES estabeleceram ou estão considerando estabelecer uma relação de negócio que inclui o XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX;

CONSIDERANDO QUE as PARTES podem divulgar entre si INFORMAÇÕES CONFIDENCIAIS, conforme definido abaixo neste instrumento, sobre aspectos de seus respectivos negócios, e em consideração da divulgação destas INFORMAÇÕES CONFIDENCIAIS;

CONSIDERANDO QUE as PARTES desejam ajustar as condições de revelação das INFORMAÇÕES CONFIDENCIAIS, bem como definir as regras relativas ao seu uso e proteção;

RESOLVEM as PARTES celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, o qual se regerá pelas considerações acima, bem como pelas cláusulas e condições a seguir:

1. Para a finalidade deste Termo, "INFORMAÇÕES CONFIDENCIAIS" significarão todas e quaisquer informações divulgadas por uma PARTE (de acordo com este instrumento, a "Parte Divulgadora") à outra PARTE (de acordo com este instrumento, a "Parte Recebedora"), em forma escrita ou verbal, tangível ou intangível, patenteada ou não, de natureza técnica, operacional, comercial, jurídica, a qual esteja claramente marcada como CONFIDENCIAL, incluindo, entre outras, mas não se limitando a, segredos comerciais, know-how, patentes, pesquisas, planos de negócio, informações de marketing, informações de usuários, situação financeira, métodos de contabilidade, técnicas e experiências acumuladas, e qualquer outra informação técnica, comercial e/ou financeira, seja expressa em notas, cartas, fax, memorandos, acordos, termos, análises, relatórios, atas, documentos, manuais, compilações, código de software, e-mail, estudos, especificações, desenhos, cópias, diagramas, modelos, amostras, fluxogramas, programas de computador, discos, disquetes, fitas, pareceres e pesquisas, ou divulgadas verbalmente e identificadas como confidenciais por ocasião da divulgação.

2. Não serão incluídas nas INFORMAÇÕES CONFIDENCIAIS quaisquer informações que: (i) sejam geralmente conhecidas, ou subsequentemente se tornem disponíveis ao comércio ou ao público; (ii) estejam na posse legal da Parte Recebedora antes da divulgação pela Parte Divulgadora; ou (iii) sejam legalmente recebidas pela Parte Recebedora de um terceiro, desde que essas informações não tenham chegado ao conhecimento da Parte Recebedora através do referido terceiro, direta ou indiretamente, a partir da Parte Divulgadora numa base confidencial.

3. Quando a divulgação de INFORMAÇÕES CONFIDENCIAIS for necessária para estrito atendimento de ordem judicial ou agência governamental, o mesmo se procederá da seguinte maneira: (i) a Parte Recebedora fica obrigada a comunicar o teor da determinação judicial à Parte Divulgadora no prazo de 2 (dois) dias úteis a contar do recebimento da ordem, no caso de se tratar de determinação para cumprimento em prazo máximo de 5 (cinco) dias; ou no prazo de uma hora a contar do recebimento, no caso de se tratar de ordem judicial para cumprimento no prazo máxima de até 48 (quarenta e oito) horas; e (ii) fica a Parte Recebedora obrigada também a enviar à Parte Divulgadora cópia da resposta dada à determinação judicial ou administrativa concomitantemente ao atendimento da mesma. A Parte Recebedora cooperará com a Parte Divulgadora para possibilitar que a Parte Divulgadora procure uma liminar ou outra medida de proteção para impedir ou limitar a divulgação dessas Informações Confidenciais.

4. A Parte Recebedora não divulgará nenhuma INFORMAÇÃO CONFIDENCIAL da Parte Divulgadora a nenhum terceiro, exceto para a finalidade do cumprimento deste Termo e com o consentimento prévio por escrito da Parte Divulgadora. Além disso:

1. A Parte Recebedora, (i) não usará as INFORMAÇÕES CONFIDENCIAIS para interferir, direta ou indiretamente, com nenhum negócio real ou potencial da Parte Divulgadora, e (ii) não usará as Informações Confidenciais para nenhuma finalidade, exceto avaliar uma possível relação estratégica entre as Partes.
2. As Partes deverão proteger as INFORMAÇÕES CONFIDENCIAIS que lhe forem divulgadas, usando o mesmo grau de cuidado utilizado para proteger suas próprias INFORMAÇÕES CONFIDENCIAIS.

3. A Parte Recebedora não revelará, divulgará, transferirá, cederá, licenciará ou concederá acesso a essas INFORMAÇÕES CONFIDENCIAIS, direta ou indiretamente, a nenhum terceiro, sem o prévio consentimento por escrito da Parte Divulgadora, estando este terceiro, condicionado à assinatura de um Termo de Compromisso de Manutenção de Sigilo prevendo as mesmas condições e obrigações estipuladas neste Termo.
4. A Parte Recebedora informará imediatamente à Parte Divulgadora de qualquer divulgação ou uso não autorizado das Informações Confidenciais da Parte Divulgadora por qualquer pessoa, e tomará todas as medidas necessárias e apropriadas para aplicar o cumprimento das obrigações com a não divulgação e uso limitado das obrigações das empreiteiras e agentes da Parte Recebedora.
5. A Parte Recebedora deverá manter procedimentos administrativos adequados à prevenção de extravio ou perda de quaisquer documentos ou INFORMAÇÕES CONFIDENCIAIS, devendo comunicar à Parte Divulgadora, imediatamente, a ocorrência de incidentes desta natureza, o que não excluirá sua responsabilidade.
6. A Parte Recebedora obrigará seu pessoal que possa ter acesso às INFORMAÇÕES CONFIDENCIAIS que cumpram tais obrigações de sigilo, assinando o TERMO DE CIÊNCIA.

5. As Partes se comprometem e se obrigam a tomar todas as medidas necessárias à proteção da informação confidencial da outra Parte, bem como para evitar e prevenir revelação a terceiros, exceto se devidamente autorizado por escrito pela Parte Divulgadora. De qualquer forma, a revelação é permitida para empresas coligadas, assim consideradas as empresas que direta ou indiretamente controlem ou sejam controladas pela Parte neste Termo. Além disso, cada Parte terá direito de revelar a informação a seus funcionários que precisem conhecê-la, para os fins deste Termo; tais funcionários deverão estar devidamente avisados acerca da natureza confidencial de tal informação, e estarão vinculados aos termos e condições do presente Termo de Compromisso de Manutenção de Sigilo independentemente de terem sido avisados do caráter confidencial da informação, ficando a Parte Recebedora responsável perante a Parte Divulgadora por eventual descumprimento do Termo.

6. O intercâmbio de informações nos termos deste instrumento não será interpretado de maneira a constituir uma obrigação de uma das Partes para celebrar qualquer Termo ou acordo de negócio, nem obrigarão a comprar quaisquer produtos ou serviços da outra ou oferecer para a venda quaisquer produtos ou serviços usando ou incorporando as Informações Confidenciais.

7. Cada Parte reconhece que em nenhuma hipótese este Termo será interpretado como forma de transferência de propriedade ou qualquer tipo de direito subsistido nas Informações Confidenciais da parte Divulgadora para a parte Recebedora, exceto o direito limitado para utilizar as Informações Confidenciais conforme estipulado neste Termo.

8. Este TERMO entrará em vigor por ocasião da assinatura pelas Partes. Os compromissos deste instrumento também serão obrigatórios às coligadas, subsidiárias ou sucessoras das Partes e continuará a ser obrigatório a elas até a ocasião em que a substância das Informações Confidenciais tenha caído no domínio público sem nenhum descumprimento ou negligência por parte da Parte Recebedora, ou até que a permissão para liberar essas Informações seja especificamente concedida por escrito pela Parte Divulgadora.

9. A omissão ou atraso em aplicar qualquer disposição deste Termo não constituirá uma renúncia de qualquer aplicação futura dessa disposição ou de quaisquer de seus termos. Se qualquer disposição deste Termo, ou sua aplicação, por qualquer razão e em qualquer medida for considerada inválida ou inexequível, o restante deste Termo e a aplicação de tal disposição a outras pessoas e/ou circunstâncias serão interpretados da melhor maneira possível para atingir a intenção das Partes signatárias.

10. As PARTES concordam que a violação do presente Termo, pelo uso de qualquer Informação Confidencial pertencente à Parte Divulgadora, sem sua devida autorização, causar-lhe-á danos e prejuízos irreparáveis, para os quais não existe remédio na lei. Desta forma, a Parte Divulgadora poderá, imediatamente, tomar todas as medidas extrajudiciais e judiciais, inclusive de caráter cautelar, como antecipação de tutela jurisdicional, que julgar cabíveis à defesa de seus direitos.

11. A Parte Recebedora deverá devolver, íntegros e integralmente, todos os documentos a ela fornecidos, inclusive as cópias porventura necessárias, na data estipulada pela Parte Reveladora para entrega, ou quando não mais for necessária a manutenção das Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades previstas neste Termo.

12. A Parte Recebedora deverá destruir quaisquer documentos por ela produzidos que contenham Informações Confidenciais da Parte Divulgadora, quando não mais for necessária a manutenção dessas Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades previstas neste Termo.

13. A inobservância de quaisquer das disposições de confidencialidade estabelecidas neste Termo sujeitará a Parte infratora, como também o agente causador ou facilitador, por ação ou omissão ou qualquer daqueles relacionados neste TERMO, ao pagamento, recomposição, de todas as perdas e danos, comprovadamente suportados ou demonstrados pela outra Parte, bem como as de responsabilidade civil e criminal respectivas, as quais serão apuradas em regular processo.

14. As obrigações de confidencialidade decorrentes do presente Termo, tanto quanto as responsabilidades e obrigações outras derivadas do presente Termo, vigorarão durante o período de 5 (cinco) anos após a divulgação de cada Informação Confidencial à Parte Recebedora.

15. O não exercício por qualquer uma das Partes de direitos assegurados neste instrumento não importará em renúncia aos mesmos, sendo tal ato considerado como mera tolerância para todos os efeitos de direito.

16. Alterações do número, natureza e quantidade das Informações Confidenciais disponibilizadas para a Parte Recebedora não descaracterizarão ou reduzirão o compromisso ou as obrigações pactuadas neste Termo de Compromisso de Manutenção de Sigilo, que permanecerá válido e com todos os efeitos legais em qualquer das situações especificadas neste Termo.

17. O acréscimo, complementação, substituição ou esclarecimento de qualquer das Informações Confidenciais disponibilizadas para a Parte Recebedora, em razão do presente objeto, serão incorporadas 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, não sendo necessário, nessas hipóteses, assinatura ou formalização de Termo Aditivo.

18. Este instrumento não deve ser interpretado como criação ou envolvimento das Partes, ou suas Afiliadas, nem em obrigação de divulgar informações confidenciais para a outra Parte.

19. O fornecimento de INFORMAÇÕES CONFIDENCIAIS pela Parte Divulgadora ou por uma de suas Afiliadas não implica em renúncia, cessão a qualquer título, autorização de uso, alienação ou transferência de nenhum direito, já obtido ou potencial, associado a tais informações, que permanecem como propriedade da Parte Divulgadora ou de suas Afiliadas, para os fins que lhe aprouver.

20. Nenhum direito, licença, direito de exploração de marcas, invenções, direitos autorais, patentes ou direito de propriedade intelectual estão aqui implícitos, incluídos ou concedidos por meio do presente Termo, ou ainda, pela transmissão de Informações Confidenciais entre as Partes.

21. A CONTRATADA declara conhecer todas as Normas, Políticas e Procedimentos de Segurança estabelecidos pela Contratante para execução do CONTRATO, tanto nas dependências da Contratante como externamente.

22. A CONTRATADA responsabilizar-se-á integralmente e solidariamente, pelos atos de seus empregados praticados nas dependências da Contratante, ou mesmo fora dele, que venham a causar danos ou colocar em risco o patrimônio da CONTRATANTE.

23. Este TERMO contém o acordo integral de confidencialidade entre as PARTES com relação ao seu objeto. Quaisquer outros acordos, declarações, garantias anteriores ou contemporâneos com relação à proteção das Informações Confidenciais, verbais ou por escrito, serão substituídos por este Termo. Este Termo será aditado somente firmado pelos representantes autorizados de ambas as Partes.

24. Quaisquer controvérsias em decorrência deste Termo serão solucionadas de modo amistoso através do representante legal das PARTES, baseando-se nas leis da República Federativa do Brasil. E por estarem assim justas e contratadas, as Partes firmam o presente Instrumento em 03 (três) vias de igual teor e forma, na presença das testemunhas abaixo indicadas.

Brasília, ___ de _____ de _____.

DE ACORDO

_____ CONTRATANTE	_____ CONTRATADA	_____ TESTEMUNHA	_____ TESTEMUNHA

E - Termo de Ciência

TERMO DE CIÊNCIA INDIVIDUAL – SIGILO E SEGURANÇA DA INFORMAÇÃO	
IDENTIFICAÇÃO DO CONTRATO	
N° do Contrato:	
Empresa Contratada:	
CNPJ:	
Objeto Resumido:	
Vigência Contratual:	
TERMOS	
O(s) funcionário(s) abaixo qualificado(s) declara(m) ter pleno conhecimento de sua(s) responsabilidade(s) no que concerne ao sigilo que deve ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito do Contrato Administrativo n° / , bem como sobre todas as informações que eventualmente ou por força de sua(s) função(ões) venha(m) a tomar conhecimento, comprometendo-se a guardar o sigilo necessário nos termos da legislação vigente e a prestar total obediência às normas de segurança da informação vigentes no ambiente do CONTRATANTE ou que venham a ser implantadas a qualquer tempo por este; em conformidade com o TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO firmado entre as partes.	
OBSERVAÇÕES	
Digite observações, se houver.	
DE ACORDO	
E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE CIÊNCIA é assinado pela(s) parte(s) declarante(s) em 02 (duas) vias de igual teor e um só efeito.	
Brasília (DF), / / .	
IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)	
Nome: Identidade: CPF:	Assinatura:

Função:	

Observação: Este termo deve ser impresso em papel timbrado da empresa CONTRATADA.

F - Modelo de Ordem de Serviço

ORDEM DE SERVIÇO **Art. 32 da Instrução Normativa SGD/ME nº 01/2019**			
1. IDENTIFICAÇÃO			
N° IDENTIFICADOR DA OSFB			
N° CONTRATO			
EMPRESA CONTRATADA / CNPJ:			
OBJETO DO CONTRATO:			
GESTOR DO CONTRATO: [*caput* art. 32 da IN 01/2019/SGD]	NOME:		
	E-MAIL:	TELFONE:	MATRÍCULA:
REQUISITANTE: [Inc. IV do art. 32 da IN 01/2019/SGD]	NOME:		
	E-MAIL:	TELFONE:	MATRÍCULA:

2. ESPECIFICAÇÃO DOS SERVIÇOS (Inc. I e II do art. 32 da IN 01/2019/SGD)					
ITEM/GRUPO:					
ID	DESCRIÇÃO	UND	QTDE/VOLUME	VL UNITÁRIO	VL TOTAL ITEM
VALOR TOTAL ESTIMADO:					

3. CRONOGRAMA (Inc. III do art. 32 da IN 01/2019/SGD)			
GRUPO/ITEM/ID	PRAZO (EM DIAS)	DATA INÍCIO	DATA ENTREGA

ORDEM DE SERVIÇO **Art. 32 da Instrução Normativa SGD/ME nº 01/2019**			
1. IDENTIFICAÇÃO			
4. INFORMAÇÃOES COMPLEMENTARES			
5. CIÊNCIA DA CONTRATADA			
PREPOSTO DA CONTRATADA: [art. 32 da IN 01/2019/SGD]	NOME:		
	E-MAIL:	TELEFONE:	CPF:
Brasília/DF, xx de xxxx de xxxx.			

(*) Modelo meramente exemplificativo

G - Modelo de Termo de Recebimento Provisório

TERMO DE RECEBIMENTO PROVISÓRIO

Identificação

Contrato:		**N° da OS / OFB:**	
Objeto:			
Contratante:			
Contratada:			

Por este instrumento, atestamos que os serviços (ou bens), relacionados na O.S. acima identificada, foram recebidos nesta data e serão objeto de avaliação quanto à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos pela Contratante.

Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até xx dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência correspondente ao Contrato supracitado.

De Acordo

CONTRATANTE	**CONTRATADA**
Fiscal Técnico do Contrato	**Preposto**

_____ *<Nome>* **Matrícula: *<Matr.>***	_____ *<Nome>* ***<Qualificação>***

_____, _____ de _____ de 20_____.

H - Modelo de Termo de Recebimento Definitivo

TERMO DE RECEBIMENTO DEFINITIVO

Identificação

Contrato Número:		**N° da OS / OFB:**	
Objeto:			
Gestor do Contrato:			
Fiscal Requisitante do Contrato:			

Por este instrumento, os servidores acima identificados atestam que o(s) serviço(s) ou bem(ns) integrantes da Ordem de Serviço ou de Fornecimento de Bens acima identificada possui(em) qualidade compatível com a especificada no Termo de Referência / Projeto Básico do Contrato supracitado.

De Acordo

Gestor do Contrato	Fiscal Requisitante do Contrato
_____ *<Nome>* **Matrícula: *<Matr.>***	_____ *<Nome>* ***<Qualificação>***

_____, _____ de _____ de 20_____.

Documento assinado eletronicamente por **Daniele Meira Borges**, **Coordenadora de Governança de Tecnologia da Informação**, em 11/01/2022, às 13:55 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Kelma Regina Batista E Silva**, **Chefe do Serviço de Licitações**, em 12/01/2022, às 09:24 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Wanessa Queiroz de Souza Oliveira**, **Subsecretária de Planejamento e Tecnologia da Informação**, em 12/01/2022, às 14:15 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Filipe Carneiro Guimarães**, **Integrante Técnico**, em 12/01/2022, às 14:51 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site http://sei.mctic.gov.br/verifica.html, informando o código verificador **8983996** e o código CRC **E0FD5C72**.

Referência: Processo nº 53115.019835/2021-45 SEI nº 8983996