



## MINISTÉRIO DAS COMUNICAÇÕES

### TERMO DE REFERÊNCIA

#### TERMO DE REFERÊNCIA

Solução de segurança de perímetro

**Referência: Arts. 12 a 24 IN SGD/ME N° 1/2019**

#### **1 – OBJETO DA CONTRATAÇÃO**

1.1 Contratação de solução de proteção de rede Next Generation Firewall(NGFW), em cluster, contemplando o hardware, software de gerenciamento, licenciamento, implantação, configuração, treinamento e atualizações, incluindo, garantia por 60 (sessenta) meses, conforme quantidades e exigências estabelecidas neste instrumento e seus anexos.

Grupo	Item	Descrição Equipamento/Software	Código CATSER/ CATMAT	QTDE	Unidade de Medida
1	1	FIREWALL - Solução de Plataforma de Segurança em cluster, composta por Next Generation Firewall (NGFW), licença de uso do sistema de gerenciamento e garantia/suporte 24x7, em português por ASC Authorized Support Center) – Subscrição por 60 meses	484747	02	Unidade
	2	PLATAFORMA DE GESTÃO E MONITORAMENTO CENTRALIZADO, COM ARMAZENAMENTO DE LOGS, INCLUINDO GARANTIA POR 60 MESES.	27472	01	Licença
	3	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL NGFW	27014	02	Serviço
	4	TREINAMENTO - Serviço de treinamento solução adquirida, com carga horária mínima de 20 horas, ministrado por profissional certificado pelo fabricante	16837	01	Capacitação

#### **2 – DESCRIÇÃO DA SOLUÇÃO DE TIC**

2.1 Trata-se de aquisição de solução de proteção de rede Next Generation Firewall (NGFW), em cluster, contemplando o hardware, software de gerenciamento, licenciamento, implantação, configuração, treinamento e atualizações, incluindo, garantia por 60 (sessenta) meses, conforme descrição pormenorizada em Tópico específico do Estudo Técnico Preliminar, anexo a este termo.

2.2 A solução deverá ser constituída dos equipamentos relacionados nos itens, sendo todos de um mesmo fabricante, garantindo a entrega e execução dos serviços por uma única empresa e a total compatibilidade entre eles.

2.3 A escolha do agrupamento dos itens em grupo visa a plena qualificação da empresa fornecedora que prestará os serviços de instalação e configuração, bem como prestará os serviços de suporte durante a vigência do contrato de garantia dos equipamentos, a total compatibilidade entre os equipamentos solicitados, a redução de custos operacionais e de infraestrutura física, a capacidade técnica de manter a solução em operação, os recursos humanos disponíveis para prestarem o devido apoio, treinamento e curva de aprendizagem e o custo total de propriedade.

2.4 **Registra-se que o objeto da contratação NÃO incide nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD/ME n° 1/2019:**

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.

## 2.5 Bens e serviços que compõem a solução

Grupo	Item	Descrição Equipamento/Software	Unidade de Medida	QTDE
1	1	FIREWALL - Solução de Plataforma de Segurança em cluster, composta por Next Generation Firewall (NGFW), licença de uso do sistema de gerenciamento e garantia/suporte 24x7, em português por ASC Authorized Support Center) – Subscrição por 60 meses	Unidade	02
	2	PLATAFORMA DE GESTÃO E MONITORAMENTO CENTRALIZADO, COM ARMAZENAMENTO DE LOGS, INCLUINDO GARANTIA POR 60 MESES.	Licença	01
	3	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL NGFW	Serviço	02
	4	TREINAMENTO - Serviço de treinamento solução adquirida, com carga horária mínima de 20 horas, ministrado por profissional certificado pelo fabricante	Capacitação	01

## 3 – JUSTIFICATIVA PARA A CONTRATAÇÃO

### 3.1. Contextualização e Justificativa da Contratação

3.1.1 Justifica-se a contratação descrita neste Termo de Referência através do Documento de Oficialização de Demandas (Doc. SEI nº 8204972), transcrito abaixo:

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.

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.

O Firewall atualmente em uso pelo Ministério das Comunicações é o appliance Palo Alto Network PA 5020, equipamento concedido pelo Ministério da Ciência, Tecnologia e Inovações, após a extinção do MCTIC. É o responsável pela inspeção do tráfego da rede interna e da Internet, prevenindo intrusões e permitindo o acesso remoto seguro à rede interna do Ministério.

Desta forma, o ativo de TI em questão cumpre o importante papel na confiabilidade e integridade dos ambientes

computacionais, uma vez que as soluções de firewall desempenham papel preponderante no controle de acesso a informações, controle de tráfego de rede e implementação de políticas de segurança de rede nas instituições.

Sobretudo no período compreendido no exercício de 2020, em que a pandemia de SARS-COV-2 determinou que a força de trabalho do Ministério permanesse em isolamento e trabalhando em regime de home-office, o acesso remoto proporcionado por meio deste equipamento, mostrou-se robusto e satisfatório para utilização nos próximos exercícios.

Para os fins previstos no art. 3º do Decreto nº 8.540/2015, identifica-se a necessidade da aquisição de uma nova solução de firewall devido a atual não possuir mais garantia ou suporte técnico. Nesse sentido, uma falha na solução de firewall causa impacto imediato nos serviços do ministério, principalmente levando em consideração que a crescente adoção de processos digitais, cuja disponibilidade é de máxima importância. Dessa forma, pela criticidade do ambiente, é necessário uma solução em alta disponibilidade e que seja possível a migração da atual configuração para uma nova solução, utilizando arquiteturas semelhantes de forma a reduzir os impactos de possíveis migrações.

A manutenção dos equipamentos de segurança de redes em constante atualização é quesito básico para tais fins. Por este motivo, torna-se essencial manter tal solução atualizada, com recepção de suporte contínuo, de maneira a permitir a escalabilidade das soluções de TIC no Ministério.

Diante deste contexto, a aquisição proposta reflete uma necessidade evidente por recursos tecnológicos essenciais aos objetivos do MCOM como medida eficaz, integrada, de ampliação e manutenção capaz de absorver as demandas sempre crescentes de capacidades, desempenho e disponibilidade, internas e externas, promovendo o fornecimento de alta disponibilidade, integridade e confiabilidade nos sistemas de informação e equipamentos computacionais do Ministério.

3.1.2 Conforme demonstrado no Estudo Técnico Preliminar, a solução de firewall atual não suportaria um aumento na banda disponível ou a implementação de novos mecanismos de segurança, pois, atualmente a solução em questão já trabalha com o máximo da sua capacidade. Nesse caso, isso ocasionaria frequentes perdas e necessidade de retransmissão de pacotes, o que reflete em atrasos no tráfego de dados, ou seja, uma lentidão na rede, a qual pode ser percebida pelos usuários em momentos de maior utilização. Além de oferecer um nível maior de segurança à rede, um firewall de próxima geração, possibilita a implementação de novos serviços, como por exemplo, análise do tráfego. Com isso seria possível ter uma visualização detalhada da utilização da rede e das aplicações utilizada, bem como, o processo de identificação de ameaças é facilitado e permite a aplicação de políticas de segurança mais eficientes. Outra funcionalidade importante que pode ser implementada é a identificação de usuários que utilizam a rede e o registro de conexões.

3.1.3 Neste ano, a Lei Geral de Proteção de Dados nº 13.709, de 14 de agosto de 2018, entrou em vigência, ampliando as exigências do Marco Civil da Internet e reforçando a utilização de melhores práticas de mercado no que tange aspectos da Segurança da Informação. Tal Lei, a partir de 2021 passa a aplicar sanções administrativas pesadas para entidades privadas e públicas de até R\$ 50.000.000,00 (cinquenta milhões de reais) por infração. A exemplificar, no caso de vazamento de informações de algum banco de dados de usuários deste Ministério, caracterizaria infração e aplicação de sanção.

3.1.4 Outro motivador desta contratação é o simples fato de que a solução atual não possui qualquer suporte ou garantia de funcionamento. Portanto, pode-se destacar que aquisição de um firewall de próxima geração é um investimento que apresentará grandes benefícios para o Mcom, dentre eles, maior nível de segurança a todos usuários da rede e a todos equipamentos ativos na rede sistemas computacionais disponibilizados pelo Ministério, além de garantir mais eficiência e qualidade para utilizar a Internet.

## 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	Aprimoramento dos processos de Segurança da Informação	Contratação de solução de segurança de perímetro	M7	Prover serviços de firewall

#### 3.2.1.3 Alinhamento ao PAC MCOM (2022)

Nº ITEM	DESCRIÇÃO
228	Equipamento segurança rede
229	Serviços de instalação, transição e configuração parametrização de software
230	Serviços de instalação, transição e configuração parametrização de software

**3.2.1.4 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 Estima-se a aquisição de solução de proteção de rede Next Generation Firewall(NGFW), em cluster, contemplando o hardware, software de gerenciamento, licenciamento, implantação, configuração, treinamento e atualizações, incluindo, garantia por 60 (sessenta) meses.

3.3.2 Quantidade:

Grupo	Item	Descrição Equipamento/Software	Código Catser/Catmat	Unidade de Medida	QTDE
1	1	FIREWALL - Solução de Plataforma de Segurança em cluster, composta por Next Generation Firewall (NGFW), licença de uso do sistema de gerenciamento e garantia/suporte 24x7, em português por ASC Authorized Support Center) – Subscrição por 60 meses	484747	Unidade	02
	2	PLATAFORMA DE GESTÃO E MONITORAMENTO CENTRALIZADO, COM ARMAZENAMENTO DE LOGS, INCLUINDO GARANTIA POR 60 MESES.	27472	Licença	01
	3	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL NGFW	27014	Serviço	02
	4	TREINAMENTO - Serviço de treinamento solução adquirida, com carga horária mínima de 20 horas, ministrado por profissional certificado pelo fabricante	16837	Capacitação	01

**3.4. Parcelamento da Solução de TIC**

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

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 traria 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 Contribuir para garantia de um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;

3.5.2 Aprimorar a segurança de TIC do Ministério das Comunicações frente a ameaças sofisticadas;

3.5.3 Possibilitar o controle de acesso e complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;

3.5.4 Possibilitar o acesso remoto de maneira estável aos colaboradores de forma segura;

3.5.5 Prestar os serviços de TIC mantendo a segurança adequada às informações organizacionais, principalmente quanto à garantia de disponibilidade e integridade dos dados necessários ao pleno funcionamento dos processos administrativos;

3.5.6 Assegurar a sustentabilidade e desempenho dos serviços do Ministério, conforme sua nova topologia e tráfego de rede;

3.5.7 Aumento da capacidade de resposta incidentes de segurança.

## **4 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO**

### **4.1. Requisitos de Negócio**

4.1.1 Garantir o perfeito funcionamento da infraestrutura de rede do MCOM;

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

4.1.3 Melhorar o nível de qualidade e segurança dos serviços das aplicações internas do Ministério.

### **4.2. Requisitos de Capacitação**

4.2.1 Considerando que se trata da aquisição de uma solução para a qual a equipe da CGTI/MCOM pode não ter conhecimento técnico suficiente para manter em operação, deverão fazer parte da aquisição treinamentos específicos que deverão ser conduzidos pelo próprio fabricante ou por um parceiro nacional, capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais.

4.2.2 O treinamento deverá ser ministrado em Língua Portuguesa/Brasil.

4.2.3 Ao término do treinamento será realizada a avaliação do mesmo. Caso o treinamento não tenha sido aprovado pela maioria dos participantes, por falha da CONTRATADA, esta deverá realizar novo treinamento, sem ônus para o CONTRATANTE, com as reformulações que o Ministério julgar necessárias, inclusive com a mudança do(s) instrutor(es), caso necessário.

4.2.4 A capacitação será ministrada para um turma com até 5 (cinco) participantes.

4.2.5. Outros requisitos de capacitação encontram-se definidos na Especificação Técnica, Anexo A deste Termo de Referência.

### **4.3. Requisitos Legais**

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

4.3.2 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;

4.3.3 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;

4.3.4 Lei Complementar nº 123/2006: institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte, e dá outras providências;

4.3.5 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;

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

4.3.7 Decreto 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;

4.3.8 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;

4.3.9 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;

4.3.10 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;

4.3.11 Instrução Normativa SLTI/MP nº 05, de 27 de junho de 2014: dispõe sobre os procedimentos administrativos básicos para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral e suas alterações;

4.3.12 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;

4.3.13 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;

4.3.14 Instrução Normativa SGD/ME nº 01, de 4 de abril de 2019: 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; e

4.3.15 Instrução Normativa SGD/ME nº 02, de 4 de abril de 2019: Regulamenta o art. 9º-A do Decreto nº 7.579, de 11 de outubro de 2011, e o art. 22, § 10 do Decreto nº 7.892, de 23 de janeiro de 2013, e dispõe sobre a composição e as competências do Colegiado Interno de Referencial Técnico;

4.3.16 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;

4.3.17 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;

4.3.18 Os serviços deverão ser prestados 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 Logística e Tecnologia da Informação do Ministério do Planejamento Orçamento e Gestão — SLTI/MPOG e no Decreto nº 7.746/2012, da Casa Civil, da Presidência da República, no que couber.

4.3.19 Deverão ser cumpridas, no que couber, as exigências:

4.3.19.1 Do inciso XI, art. 7º da Lei nº 12.305, de 02 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos — PNRS;

4.3.19.2 Do art. 6º da Instrução Normativa MPOG nº 01, de 19 de janeiro de 2010, que estabelece as práticas de sustentabilidade na execução dos serviços.

4.3.19.3 Da Portaria nº 170, de 10 de abril de 2012 do Instituto Nacional de Metrologia, Qualidade e Tecnologia — INMETRO.

#### **4.4. Requisitos de Manutenção**

4.4.1 Encontram-se definidos na Especificação Técnica, Anexo A deste Termo de Referência.

#### **4.5. Requisitos Temporais**

4.5.1 Encontram-se definidos na Especificação Técnica, Anexo A deste Termo de Referência.

#### **4.6. Requisitos de Segurança**

4.6.1 A Contratada deverá submeter-se aos procedimentos de segurança existentes, ou que possam ser criados durante a vigência do contrato. Os procedimentos deverão ser observados sempre que for necessária a presença nas dependências da Contratante.

4.6.2 A CONTRATADA deverá atender à legislação, principalmente à Instrução Normativa GSI/PR nº 01, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, a qual disciplina a gestão de segurança da Informação e Comunicações na Administração Pública Federal, bem como ao Decreto nº 3505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

#### **4.7. Requisitos Sociais, Ambientais e Culturais**

4.7.1 A documentação e os manuais da solução deverão ser apresentados no idioma Português (Brasil), eventualmente poderão ser apresentados em inglês. Todos os contatos para gerenciamento de chamados e suporte técnico deverão ser realizados em Português (Brasil).

4.7.2 Em conformidade com a IN SLTI/MPOG n. 01/2010, a Contratada deverá cumprir com os seguintes requisitos de sustentabilidade ambiental, quando aplicável:

4.7.2.1 Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2.

4.7.2.2 Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares.

4.7.2.3 Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

4.7.3 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 Encontram-se definidos na Especificação Técnica, Anexo A deste Termo de Referência.

#### **4.9. Requisitos de Projeto e de Implementação**

4.9.1 Encontram-se definidos na Especificação Técnica, Anexo A deste Termo de Referência.

#### **4.10. Requisitos de Implantação**

4.10.1 Encontram-se definidos na Especificação Técnica, Anexo A deste Termo de Referência.

#### **4.11. Requisitos de Garantia**

4.11.1 Encontram-se definidos na Especificação Técnica, Anexo A deste Termo de Referência.

#### **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 durante o período da garantia deverá ser prestado por profissionais especializados e certificados pelo fabricante da solução, devidamente capacitados.

#### **4.14. Requisitos de Metodologia de Trabalho**

4.14.1 A Contratante será a responsável pela verificação da aderência aos padrões de qualidade exigidos dos produtos entregues. A Contratada será responsável pelo fornecimento do software e gestão dos recursos humanos e materiais necessários para a prestação da garantia.

4.14.2 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; maior geração de empregos; maior vida útil e menor custo de manutenção do bem; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens e serviços.

#### **4.15. Requisitos de Segurança da Informação**

4.15.1 A solução contratada deverá observar a Norma Brasileira ABNT NBR ISO/IEC 27002.

4.15.2 A Contratada deverá respeitar a Política de Segurança da Informação e Comunicações (POSIC) o Ministério das Comunicações, bem como demais políticas e normas internas que poderão ser instituídas durante a vigência do contrato.

4.15.3 A Contratada deverá guardar 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.

#### **4.16. Outros Requisitos Aplicáveis**

##### **4.16.1 Requisitos de Sustentabilidade Ambiental**

4.16.1.1 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.

4.16.1.2 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.

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

#### **4.16.2 Requisitos dos Direitos de Propriedade Intelectual e Direitos Autorais da Solução de Tecnologia da Informação**

4.16.2.1 Em conformidade com a IN nº 01/2019 SGD/ME, art. 17, alínea h, define-se a seguir quais serão os direitos a propriedade intelectual pertinente a esta contratação, a saber:

4.16.2.1.1 Não se aplicará direito de propriedade intelectual ao MCOM sobre o código fonte, visto que a execução dos serviços não envolve desenvolvimento de software e/ou aplicativo;

4.16.2.1.2 Destaca-se que o MCOM pretende adquirir hardware e software prontos, onde não se aplicar-se-á o direito de propriedade intelectual;

4.16.2.1.3 Se aplicará direito de propriedade intelectual ao MCOM sobre toda e qualquer documentação fruto da execução dos serviços prestados.

#### **4.16.3 Requisitos Gerais**

4.16.3.1 Para fins de total compatibilidade, gerenciamento unificado e padronização do conhecimento a ser transferido/recebido e dos procedimentos de manutenção e de operação da solução, optou-se por exigir que todos componentes sejam fornecidos em regime de empreitada global.

### **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 ou Projeto Básico;

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, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

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 Não praticar atos de ingerência na administração da CONTRATADA, a exemplo daqueles listados no art. 5º da IN 05/SEGES/MPDG de 26/05/2017;

5.1.8 Aplicar as penalidades cabíveis;

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

5.1.10 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 7º do Decreto nº 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 a 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 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;

5.2.1.18 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;

5.2.1.19 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;

5.2.1.20 Não permitir a utilização de qualquer trabalho do menor de 16 (dezesesseis) 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;

5.2.1.21 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;

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

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

### **5.3. Deveres e responsabilidades do órgão gerenciador da ata de registro de preços**

5.3.1 Não se aplica, tendo em vista que não será admitida a adesão de outros órgãos à presente ata.

## **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 Prazos, horários de fornecimento de bens ou prestação dos serviços**

6.1.2.1 A entrega de todos os produtos deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato.

6.1.2.2 A implantação completa da solução deverá ser concluída em até 30 (trinta) dias corridos após a entrega do objeto.

6.1.2.3 O(s) equipamento(s) deverão ser entregues e instalados em Brasília/DF, Esplanada dos Ministérios, Bloco "R" e Anexo, Térreo, Ministério das Comunicações.

6.1.2.4 A entrega dos equipamentos e instalação deverão ser realizadas nos dias úteis, no horário das 09:00 às 12:00 e das 14:00 às 17:00, e poderá ser agendada em data e hora previamente com a Contratante.

6.1.2.5 O transporte dos equipamentos deverá ser realizado pela CONTRATADA, inclusive os procedimentos de seguro, embalagem e transporte até o espaço alocado pela Contratante para guarda.

6.1.2.6 Caberá à Contratante rejeitar no total ou em parte, os materiais entregues em desacordo com o objeto deste Termo de Referência.

6.1.2.7 O recebimento dos equipamentos será efetivado pela equipe designada pela CONTRATANTE e dar-se-á da forma provisória e definitiva, conforme prazos estabelecidos nos subitens 7.2.1.1. e 7.2.1.1 deste Termo de Referência.

#### **6.1.3 Documentação Mínima Exigida**

6.1.3.1 A Contratada deverá fornecer:

- a) Manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração;
- b) Documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, desenho lógico da implantação, comentários e configurações executadas;
- c) Relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.

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

6.2.1 Conforme item 2.5 - Bens e serviços que compõem a solução, 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) Canal 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, encontra-se no **ANEXO D**.

## 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 conforme disposto na Especificação Técnica, Anexo A deste Termo de Referência, bem como, na parte de monitoramentoda execução, de forma provisóriae definitiva, conforme prevê o artigo 73 da Lei nº 8.666/93 e o art. 33 da Instrução Normativa nº 01/2019/SGD/ME, observando o disposto a seguir:

#### 7.2.1.1 Termo de Recebimento Provisório

- a) O recebimento provisório será realizado pelo Fiscal Técnico do contrato quando daentregado objeto resultante de cada ordem de serviço e consiste na emissão doTermo 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. 2º da IN-01/2019/SGD/ME).
- b) O recebimento provisório ocorrerá em até5(cinco) diasúteisapós o recebimentoe verificação de conformidade de todos os componentes da solução.

#### 7.2.1.2 Termo de Recebimento Definitivo

- a) 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.

b) Observando de forma complementar o disposto na alínea “c” do inciso II do art. 50 da IN nº 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.

c) O recebimento definitivo ocorrerá em até 10 (dez) dias úteis após o recebimento provisório.

d) Será rejeitado, no todo ou em parte, o entregável fornecido em desacordo com as especificações constantes deste Termo de Referência e seus anexos. 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.

e) 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 o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

7.2.2 O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor (Lei nº 10.406, de 2002).

7.2.3 Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

### **7.3 Alteração subjetiva**

7.3.1 É admissível a fusão, cisão ou incorporação da CONTRATADA com/por outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do CONTRATO.

### **7.4 Procedimentos de Teste e Inspeção**

7.4.1 A Metodologia de Avaliação da Qualidade será realizada pela Contratante, de acordo com a avaliação das seguintes condições que deverão ser cumpridas pela Contratada:

7.4.1.1 O cumprimento dos prazos e outras obrigações assumidas pela contratada;

7.4.1.2 Entrega da documentação exigida;

7.4.1.3 Atendimento dos critérios de aceitação;

7.4.1.4 Execução dos procedimentos corretos para que haja o recebimento dos bens e a atestação dos serviços prestados durante a garantia e;

7.4.1.5 A Metodologia de Avaliação da Qualidade dos serviços prestados ocorrerá através do acompanhamento e avaliação dos atendimentos aos chamados de suporte técnico especializado junto com as solicitações de garantia;

7.4.2 Durante a vigência da garantia, a fiscalização técnica do contrato avaliará constantemente a prestação do serviço e usará como indicador a tabela disponível no subitem 7.5 Níveis Mínimos de Serviço Exigidos, deste Termo de Referência.

7.4.3 A CONTRATANTE reserva-se o direito de efetuar inspeções e diligências para sanar quaisquer dúvidas existentes, podendo efetuar-las de maneira presencial ou através de documentação, em qualquer momento da contratação.

### **7.5 Níveis Mínimos de Serviço Exigidos**

7.5.1 Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website ou e-mail. O suporte deverá estar disponível na modalidade de 24x7 (24 horas por dia, 7 dias por semana).

7.5.2 O suporte deverá respeitar os seguintes tempos de resposta para os níveis de severidade:

Nível de Severidade
---------------------

ID	Descrição	Prazo
<b>Crítica</b>	O produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Neste caso o chamado deverá ser aberto via telefone (0800)	Para este nível de severidade o atendimento deverá ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno.
<b>Alta</b>	Impacto moderado no sistema, travamento, ou parada de ambiente parcial.	Para este nível de severidade o tempo de resposta deverá ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno.
<b>Média</b>	Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida.	Para este nível de severidade o tempo de resposta deverá ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno.
<b>Baixa</b>	Dúvidas de configuração ou anomalia de baixo impacto.	Para este nível de severidade o tempo de resposta deverá ser de até 8 (oito) horas, em horário comercial.

## 7.6 Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

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

- 7.6.1.1 não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;
- 7.6.1.2 não assinar a ata de registro de preços, quando cabível;
- 7.6.1.3 apresentar documentação falsa;
- 7.6.1.4 deixar de entregar os documentos exigidos no certame;
- 7.6.1.5 ensejar o retardamento da execução do objeto;
- 7.6.1.6 não manter a proposta;
- 7.6.1.7 cometer fraude fiscal;
- 7.6.1.8 comportar-se de modo inidôneo.

7.6.2 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.

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

- 7.6.3.1 Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação, conforme item 7.6.12;
- 7.6.3.2 Multa, nos percentuais descritos no item 7.6.12;
- 7.6.3.3 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;
- 7.6.3.4 Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;
- 7.6.3.5 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.

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

7.6.5 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.

7.6.6 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.

7.6.7 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.

7.6.8 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.

7.6.9 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.

7.6.10 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.

7.6.11 As penalidades serão obrigatoriamente registradas no SICAF.

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

ID	OCORRÊNCIA	GLOSA/SANÇÃO
1	Não comparecer injustificadamente à Reunião Inicial.	Advertência. Em caso de reincidência, 1% sobre o valor total do Contrato.
2	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A Contratada ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/2002, pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais, e multa de 10% do estimado da contratação.
3	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A Contratada será declarada inidônea para licitar e contratar com a Administração.
4	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual. Aplicação de multa de 10% sobre o valor do contrato.
5	Não executar total ou parcialmente os serviços/materiais previstos no objeto da contratação.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual. Aplicação de multa de 10% sobre o valor do contrato.
6	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por até de 30 dias, sem comunicação formal ao gestor do Contrato.	Multa de 10% sobre o valor total do Contrato. Em caso de reincidência, configura-se inexecução total do Contrato por parte da empresa, ensejando a rescisão contratual unilateral.
7	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por mais de 30 (trinta) dias, sem comunicação formal ao gestor do contrato.	Contratada será declarada impedida de licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual. Aplicação de multa de 5% sobre o valor do contrato.
8	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 8 (oito) horas úteis.	Multa de 0,1% (um décimo por cento) sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela CONTRATANTE, até o limite de 7 dias úteis. Após o limite de 7 dias úteis, aplicar-se-á multa de 1% (cinco por cento) do valor total do Contrato.
9	Provocar intencionalmente a indisponibilidade da prestação dos serviços quanto aos componentes de software (sistemas, portais, funcionalidades, banco de dados, programas, relatórios, consultas, etc.)	A Contratada será declarada impedida de licitar ou contratar com a Administração Pública pelo prazo de 12 (doze) meses, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
10	Permitir intencionalmente o funcionamento dos sistemas de modo adverso ao especificado na fase de levantamento de requisitos e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços.	A Contratada será declarada impedida de licitar ou contratar com a Administração Pública pelo prazo de 12 (doze) meses, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.

11	Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	A Contratada será declarada impedida de licitar ou contratar com a Administração Pública pelo prazo de 12 (doze) meses, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
12	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da contratante.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
13	Atraso na resolução de chamados de suporte técnico durante o período da garantia.	Chamados com severidade Baixa: Advertência.
		Chamados com severidade Média: Multa de 0,11% do valor total do Contrato.
		Chamados com severidade Alta: Multa de 0,30% do valor total do Contrato.
		Chamados com severidade Crítica: Multa de 1% do valor total do Contrato.
14	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 10% do valor total do Contrato.

## 7.7. Do Pagamento

7.7.1 O pagamento ocorrerá em parcela única, após a entrega de todos os itens que compõem o objeto da contratação e emissão do Termo de Recebimento Definitivo. O prazo para pagamento será de até 30 (trinta) dias, contados do recebimento da respectiva Nota Fiscal/Fatura.

7.7.2 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.

7.7.3 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 a entrega dos equipamentos e realização dos serviços de instalação, configuração, atualização e treinamento;

7.7.4 A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

7.7.4.1 Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

7.7.5 O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

7.7.5.1 o prazo de validade;

7.7.5.2 a data da emissão;

7.7.5.3 os dados do contrato e do órgão contratante;

7.7.5.4 o período de prestação dos serviços;

7.7.5.5 o valor a pagar; e

7.7.5.6 eventual destaque do valor de retenções tributárias cabíveis.

7.7.6 Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, 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;

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

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

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

7.7.10 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.

7.7.11 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.

7.7.12 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.

7.7.12.1 Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

7.7.13 Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

7.7.14 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei nº 8.212, de 1993, nos termos do item 6 do Anexo XI da IN SEGES/MP n. 5/2017, quando couber.

7.7.15 É vedado o pagamento, a qualquer título, por serviços prestados, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão contratante, com fundamento na Lei de Diretrizes Orçamentárias vigente.

7.7.16 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:

$EM = I \times N \times VP$ , 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 solução de segurança de perímetro contemplando o hardware, software, licenciamento, implantação, configuração, treinamento, atualizações e garantia por 60 (sessenta) meses, de acordo com as necessidades do MCOM, é de R\$ 2.710.509,78 (dois milhões, setecentos e dez mil e quinhentos e nove reais e setenta e oito centavos).

8.2 A metodologia utilizada para definição do valor estimado foi o valor médio das cotações de preços.

8.3 Considerando o valor estimado para a presente contratação, ressalta-se que não há a necessidade de aprovação pelo Órgão Central do SISP, em conformidade ao disposto no art. 1º, §2º, da IN SGD/ME nº 1/2019.

Grupo	Item	Descrição Equipamento/Software	Código Catser/Catmat	QTDE	Unidade de Medida	VALOR UNITÁRIO	VALOR TOTAL
	1	FIREWALL - Solução de Plataforma de Segurança em cluster, composta por Next Generation Firewall (NGFW), licença de uso do sistema de gerenciamento e garantia/suporte 24x7, em português por ASC Authorized Support Center) – Subscrição por 60 meses	150100	02	Unidade	R\$1.190.780,69	R\$ 2.381.561,39

1	2	PLATAFORMA DE GESTÃO E MONITORAMENTO CENTRALIZADO, COM ARMAZENAMENTO DE LOGS, INCLUINDO GARANTIA POR 60 MESES.	27472	01	Licença	R\$126.530,87	R\$126.530,87
	3	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL NGFW	27014	02	Serviço	R\$46.675,99	R\$93.351,97
	4	TREINAMENTO - Serviço de treinamento solução adquirida, com carga horária mínima de 20 horas, ministrado por profissional certificado pelo fabricante	16837	01	Capacitação	R\$109.065,55	R\$109.065,55
	<b>TOTAL</b>						<b>R\$ 2.710.509,78</b>

## 9 – ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

9.1 Os recursos orçamentários, para fazer frente às despesas desta contratação serão definidos de acordo com o art. 7º § 2º 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 2022.

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:

Grupo	Item	Descrição Equipamento/Software	Código Catser/Catmat	QTDE	Unidade de Medida	PREVISÃO DE DESEMBOLSO				
						1º Ano	2º Ano	3º Ano	4º Ano	5º Ano
1	1	FIREWALL - Solução de Plataforma de Segurança em cluster, composta por Next Generation Firewall (NGFW), licença de uso do sistema de gerenciamento e garantia/suporte 24x7, em português por ASC Authorized Support Center) – Subscrição por 60 meses	484747	02	Unidade	R\$2.381.561,39	-	-	-	-
	2	PLATAFORMA DE GESTÃO E MONITORAMENTO CENTRALIZADO, COM ARMAZENAMENTO DE LOGS, INCLUINDO GARANTIA POR 60 MESES.	27472	01	Licença	R\$126.530,87	-	-	-	-

3	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL NGFW	27014	02	Serviço	R\$93.351,97	-	-	-	-
4	TREINAMENTO - Serviço de treinamento solução adquirida, com carga horária mínima de 20 horas, ministrado por profissional certificado pelo fabricante	16837	01	Capacitação	R\$109.065,55	-	-	-	-
<b>Valor Total</b>					<b>R\$2.710.509,78</b>	-	-	-	-

## 10 – DA VIGÊNCIA DO CONTRATO

10.1. O prazo de vigência contratual é de 12 (doze) meses, contados a partir da data da sua assinatura, nos termos do art. 57, inciso II, da Lei nº 8.666/93, com suas posteriores alterações.

10.2. O prazo de garantia é de 60 (sessenta) meses contados da assinatura do Termo de Recebimento Definitivo da solução.

## 11 – DO REAJUSTE DE PREÇOS (quando aplicável)

11.1 Os preços inicialmente contratados são fixos e irremovíveis 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):

$$R = V (I - I^{\circ}) / I^{\circ}, \text{ onde:}$$

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 presente contratação adotará o regime de execução a Empreitada por Preço Global, do tipo Menor Preço por grupo.

12.1.2 As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no edital.

12.1.3 Os critérios de qualificação econômico-financeira a serem atendidos pelo fornecedor estão previstos no edital.

12.1.4 Nos termos do parágrafo único, do art. 1º, da Lei nº 10.520, de 2002, c/c art. 3º, II do Decreto nº 10.024/2019. Vide arts. 14 a 17 da IN SEGES/MP nº 5/2017, o objeto pretendido trata-se de "bens e serviços" comum, 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.

12.1.5 A adjudicação por preço global se deve ao fato de que todos os equipamentos e serviços estão intrinsecamente relacionados. A execução dos serviços por mais de uma empresa acarretaria elevado custo de administração e uma complexa rede de coordenação entre os projetos e, certamente, comprometeria a qualidade e efetividade dos resultados para o MCOM. A divisão do objeto a ser licitado em itens pode acarretar prejuízos quanto à instalação, configuração e operacionalização de todo o sistema, bem como sua manutenção, uma vez que se exige total compatibilidade entre os equipamentos da solução a ser adquirida, ou seja, a instalação tem que ser uniforme.

12.1.6 Considerando a natureza dos serviços do objeto eo disposto no Parágrafo único do art. 25da Instrução Normativanº 01/2019/SGD/ME,a licitação será realizada por meio do Sistema de Registro de Preços, na modalidade PREGÃO, na forma ELETRÔNICA, do tipo MENOR PREÇO.

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

## **12.2 Adoção do Sistema de Registro de Preços**

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 contratação do objeto enquadra-se nas hipóteses de cabimento do SRP descritas no art. 3º do Decreto nº 7.892, de 23 de janeiro de 2013, in verbis:

*"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."(grifos nossos)*

12.2.3 De acordo com o art. 16 do Decreto nº 7.892/2013, a existência de preços registrados não obriga a Administração Pública a contratar, facultando-se a realização de licitação específica para a aquisição pretendida, assegurada preferência ao fornecedor registrado em igualdade de condições.

12.2.4 Posto isso, a adoção do Sistema de Registros se dá em função dos aspectos técnicos e requisitos que envolvem a execução dos serviços e considerando o grau de interação do conjunto de serviço técnico, natureza específica, características de especificidade, aliada a criticidade e complexidade que envolve a prestação de serviço desta contratação.

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

12.3.1 Nos termos do Decreto Federal nº 7.892/2013, atualizado pelo Decreto nº 9.488/18 e, considerando o Decreto nº 8.250/2014, 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, e considerando a ausência de estrutura administrativa satisfatória para fins de gerenciamento de demandas advindas de outros órgãos interessados na contratação, 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. Não se aplica o disposto no art. 6º do Decreto nº 8.538/2015, que regulamenta a LC nº 123/2006, para fins de exclusividade de participação de microempresas e empresas de pequeno porte, tendo em vista que o valor previsto para a presente licitação excede o valor estipulado no decreto supra.

12.4.2. No tocante aos critérios de desempate previstos na LC nº 123/2006, regulamentada pelo Decreto nº 8.538/2015, estes serão observados e disciplinados no edital.

12.4.3 Em atenção ao Acórdão 1352/2018 – TCU – Plenário, que orienta 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, que devem ser aplicadas as regras de preferência dispostas no Decreto nº 7.174, de 12 de maio de 2010, tais critérios serão observados e disciplinados no edital.

## **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 **Atestado de capacidade técnica-operacional ou a Declaração** emitida pelo fabricante do equipamento, comprovando que a licitante é apta a instalar, configurar, prestar suporte técnico e ministrar treinamentos das soluções referente a esta contratação;

12.5.1.2 **Atestado de capacidade técnica-operacional**, em nome da licitante, expedido por pessoa jurídica de direito público ou privado, que comprovem a execução de no mínimo 12 meses, em contrato único ou separado, serviços de solução de segurança de perímetro contemplando o hardware, software, licenciamento, implantação, configuração, treinamento, garantia, atualizações e suporte técnico, conforme exigências deste Termo de Referência e seus anexos.

12.5.1.3 **Declaração de que possuirá no ato da assinatura do contrato**, no mínimo 1 (um) profissional pertencente ao quadro de funcionários da empresa com certificação técnica oficial do fabricante, compatível com o(s) objeto(s) deste processo.

12.5.1.4 **Declaração de que terá no ato da assinatura do contrato**, disponibilização dos equipamentos, ferramentas e corpo técnico especializado para o fornecimento do objeto, conforme o §6º, do art. 30, da Lei nº 8.333/93.

12.5.2 Os atestados deverão referir-se a contratos já concluídos ou já decorrido no mínimo 1 ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior devendo ser comprovado por meio do contra.

12.5.3 Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

12.5.4 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.

12.5.5 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.

12.5.6 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 Permissão de subcontratação**

12.7.1 É vedada 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 4173/2021/SEI-MCOM, de 26 de novembro de 2021 (SEI nº8731118), publicada no Boletim de Serviços nº 87, de 26 de novembro de 2021 (SEI nº8734185).

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 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 - MODELO DE ORDEM DE SERVIÇO;
- 13.6.6 ANEXO F - TERMO DE RECEBIMENTO PROVISÓRIO;
- 13.6.7 ANEXO G - TERMO DE RECEBIMENTO DEFINITIVO;
- 13.6.8 ANEXO H - ESTUDO TÉCNICO PRELIMINAR.

<b>INTEGRANTE TÉCNICO</b>	<b>INTEGRANTE REQUISITANTE</b>	<b>INTEGRANTE ADMINISTRATIVO</b>
<b>Victor Hugo de Souza Peçanha</b> Assistente de Tecnologia da Informação Matrícula/SIAPE: 2420446 <i>(assinado eletronicamente)</i>	<b>Daniele Meira Borges</b> Coordenadora de Governança de TI Matrícula/SIAPE: 1793595 <i>(assinado eletronicamente)</i>	<b>Cristiane Reis Peixoto Serra</b> Matrícula/SIAPE: 3220162 <i>(assinado eletronicamente)</i>

<b>AUTORIDADE MÁXIMA DA ÁREA DE TIC (OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11)</b>
Declaro a adequação do conteúdo deste documento às disposições da Instrução Normativa 1/2019-SGD/ME.  <b>Wanessa Queiroz de Souza Oliveira</b> Subsecretária de Planejamento e Tecnologia da Informação Matrícula/SIAPE: 1905250 <i>(assinado eletronicamente)</i>

Aprovo,

<b>Autoridade Competente</b>
<i>(assinado eletronicamente)</i> <b>Ivancir Gonçalves da Rocha Castro Filho</b> Coordenador Geral de Recursos Logísticos

## ANEXOS

### A - Especificação Técnica

<b>Item</b>	<b>Descrição</b>
	<b>FIREWALL - SOLUÇÃO DE PLATAFORMA DE SEGURANÇA DE PERÍMETRO EM CLUSTER, COMPOSTA POR NEXT GENERATION FIREWALL (NGFW) E GARANTIA/SUPORTE</b>

## **24X7, EM PORTUGUÊS, POR ASC AUTHORIZED SUPPORT CENTER), INCLUINDO GARANTIA DO EQUIPAMENTO POR 60 MESES**

### **1.1 CARACTERÍSTICAS GERAIS**

### **1.2 CAPACIDADES E QUANTIDADES**

1.2.1. A solução de segurança (NGFW) deve possuir a capacidade e as características abaixo:

1.2.1.1. Throughput de 6 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

1.2.1.2. Throughput de no mínimo, 3 (três) Gbps, com todas as funcionalidades de firewall, controle de aplicação, IPS, anti-malware e prevenção contra ameaças avançadas de dia-zero habilitadas e atuantes;

1.2.1.2.1. O Throughput é a quantidade de tráfego que um único equipamento é capaz de encaminhar, não havendo soma entre os membros do cluster;

1.2.1.3. Suporte a, no mínimo, 2.000.000 (dois milhões) de conexões simultâneas;

1.2.1.4. Suporte a, no mínimo, 70.000 (setenta mil) novas conexões por segundo;

1.2.1.5. Armazenamento com capacidade de, no mínimo, 240 GB SSD ;

1.2.1.6. Deve possuir fontes de alimentação AC 100-240VAC redundantes ou hot-swappable;

1.2.1.7. No mínimo, 08 (oito) interfaces de rede de 1GbE RJ-45;

1.2.1.8. No mínimo, 04 (quatro) interfaces de rede de 10 Gbps SFP+;

1.2.1.9. No mínimo, 02 (duas) interfaces Gigabit para alta disponibilidade ou quantidade suficiente a permitir que a solução contratada trabalhe em Alta Disponibilidade (High Availability);

1.2.1.10. 01 (uma) interface do tipo console ou similar;

1.2.1.11. 01 (uma) interface dedicada para gerenciamento fora de banda (out-of-band);

1.2.1.12. Todas as interfaces requeridas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores do tipo SR;

1.2.1.13. Deve, quando em alta disponibilidade, operar em cluster ativo/passivo e ativo/ativo;

**1.2.1.14. Não serão aceitos appliances virtualizados para este item, somente equipamentos físicos.**

### **1.3 FUNCIONALIDADES DE FIREWALL**

1.3.1. As funcionalidades de firewall devem possuir a capacidade e as características abaixo:

1.3.1.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

1.3.1.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

1.3.1.3. A solução deve estar licenciada para trabalhar em cluster ativo/passivo e ativo/ativo;

1.3.1.4. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.3.1.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

1.3.1.6. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.3.1.6.1. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou

policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;

1.3.1.7. Deve suportar os seguintes tipos de NAT:

1.3.1.7.1. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

1.3.1.8. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing);

1.3.1.9. Deve suportar atuar como proxy reverso para aplicações Web que utilizem protocolos HTTP e HTTPS;

1.3.1.10. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

1.3.1.11. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

1.3.1.12. Deve suportar NAT64;

1.3.1.13. Suportar OSPF graceful restart;

1.3.1.14. Deve estar equipado com ferramenta de monitoração de pacotes de rede tipo sniffer para acompanhamento e visualização de tráfego de rede em tempo real, não sendo aceito soluções que fazem a gravação do tráfego para posterior abertura e análise, inclusive com a capacidade de aplicação de filtros personalizados;

1.3.1.15. O Firewall deve ter a capacidade de operar de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);

1.3.1.16. Deve possuir sistema de monitoramento em tempo real do hardware via interface gráfica, interface Web HTTPS e linha de comando CLI.

#### **1.4. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB**

1.4.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

1.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.4.3. Deve de-criptografar tráfego de entrada e saída;

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

1.4.5. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

1.4.5.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

1.4.5.2. Reconhecer aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

1.4.6. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

1.4.7. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

1.4.8. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

1.4.9. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;

1.4.10. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos

checagem de assinaturas, decodificação de protocolos ou análise heurística;

1.4.11. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

1.4.12. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

1.4.12.1. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.4.12.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

1.4.12.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

1.4.12.4. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

1.4.12.5. Suportar base ou cache de URLs local no appliance, sendo o cache populado conforme as requisições de verificação das URLs no banco de dados central forem sendo realizadas, evitando atrasos de comunicação e validação das URLs.

1.4.12.6. Permitir a customização de página de bloqueio;

1.4.12.7 Permitir o controle e monitoramento de aplicações SaaS;

1.4.13. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

1.4.14. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou syslog, para a identificação de endereços IP e usuários;

1 1.4.15. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal).

## **1.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS**

1.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus, Anti-Malware e Threat Emulation (Sandboxing) integrados no próprio equipamento de firewall;

1.5.2. Possuir capacidade de detecção de, no mínimo, 5.000 (cinco mil) assinaturas de ataques pré-definidos;

1.5.3. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

1.5.4. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

1.5.5. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, IMAP, SMB e FTP;

1.5.6. Suportar bloqueio de arquivos por tipo;

1.5.7. Identificar e bloquear comunicação com botnets;

1.5.8. Deve suportar referência cruzada com CVE;

1.5.9. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos. A identificação deve ser de forma automática, não sendo necessário que o administrador cadastre os domínios considerados maliciosos;

1.5.10. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.5.10.1. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.5.11. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS ou Anti-Malware, através da console de gerência centralizada ou através de 02 (duas) TAPs de rede com interfaces compatíveis com os firewalls a ser entregue junto com os equipamentos;

1.5.12. Os eventos devem identificar o país de onde partiu a ameaça;

1.5.13. Suportar rastreamento de vírus em arquivos pdf;

1.5.14. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

1.5.15. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.5.16. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

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

1.5.18. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

1.5.19. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) mediante análise completa do arquivo no ambiente sandbox.

1.5.20. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL e TLS, nas versões mais recentes.

1.5.21. Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL's conhecidas;

1.5.22. A emulação dos arquivos em sandbox deverá ser realizada em equipamento físico instalado no ambiente on-premise ou na nuvem do fabricante, a qual deve estar hospedada em território brasileiro;

1.5.23. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, entre os quais Windows 10 e posteriores, assim como em sistemas Office;

1.5.24. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

1.5.25. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm;

1.5.26. O relatório das emulações deve conter as informações dos arquivos emulados com o tipo do arquivo e tamanho, assim como todo detalhamento das atividades executadas como a criação ou modificação de arquivos, alteração nos registros, uso de rede e manipulação de processos devendo exibir os resultados e detalhamento das atividades por ambiente emulado onde o arquivo foi analisado;

1.5.27. A solução deve possuir os indicadores abaixo referente a última 1 (uma) hora e as últimas 24 (vinte e quatro) horas ou ao último dia, última semana ou últimos 30 dias:

1.5.28.1. Número de arquivos não maliciosos ou arquivos scaneados;

1.5.28.2. Número de arquivos maliciosos.

## **1.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO**

1.6.1. Suportar a criação de políticas de QoS por:

1.6.1.1. Endereço de origem, endereço de destino e por porta;

1.6.2. O QoS deve possibilitar a definição de classes por:

1.6.2.1. Banda garantida, banda máxima e fila de prioridade;

1.6.2.2. Disponibilizar estatísticas RealTime para classes de QoS.

## **1.7. FUNCIONALIDADES DE VPN**

1.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.7.2. Suportar IPSec VPN;

1.7.3. Suportar SSL VPN;

1.7.4. A VPN IPSEc deve suportar:

1.7.4.1. 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

1.7.5. A VPN SSL:

1.7.5.1. Deve permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

1.7.5.2 Deve estar licenciado para ou suportar sem o uso de licença, 10.000 (dez mil) clientes de **VPN SSL** simultâneos;

1.7.5.3. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

1.7.5.4. Deve ser capaz de informar se a senha do usuário da VPN SSL autenticado via Microsoft Active Directory expirou e permitir que o usuário faça a troca da senha;

1.7.5.5. Atribuição de endereço IP nos clientes remotos de VPN;

1.7.5.6. Atribuição de DNS nos clientes remotos de VPN;

1.7.5.7. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

1.7.5.8. Suportar leitura e verificação de CRL (certificate revocation list);

1.7.5.9. O agente de VPN SSL client-to-site deve ser compatível com Windows 7 e versões posteriores, Mac OSx, Linux e também compatível com dispositivos móveis com sistema operacional Android e iOS;

1.7.5.10. Deve suportar mais de um fator de autenticação para a conexão VPN;

1.7.5.11. Deve permitir a verificação de conformidade do cliente ao se conectar à VPN, permitindo verificar se o firewall do cliente está habilitado e se possui antivírus instalado e ativo;

1.7.6. Deve suportar ZTNA (Zero Trust Network Access);

1.7.7 Devem ser migradas as regras de segurança do Firewall em uso atualmente no MCOM (Palto Alto 5020).

1.7.8 Deve ser criada VPN na solução contratada que permita o acesso à rede interna remotamente, ou então, ser migrada a VPN em uso atualmente, caso seja possível.

1.7.9. Suporte a, no mínimo, 30 (trinta) zonas de segurança;

1.7.10. Estar licenciada para ou suportar sem o uso de licença, no mínimo, 2000 (dois mil) túneis de VPN **IPSEC** simultâneos;

1.7.11 Deve suportar, no mínimo, 10 sistemas virtuais lógicos (Contextos) no firewall Físico;

**1.8 Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos**

**em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos as sanções previstas em lei;**

1.9 Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend ou similar).

## **PLATAFORMA DE GESTÃO E MONITORAMENTO CENTRALIZADO, COM ARMAZENAMENTO DE LOGS, INCLUINDO GARANTIA POR 60 MESES.**

A utilização de um software de gerenciamento centralizado facilita as tarefas de gerenciamentos de regras e políticas em um firewall. Por meio desse gerenciamento centralizado é possível gerenciar diversos appliances por meio de uma única interface. Além disso, é possível acessar registros (logs) de diversos equipamentos.

### **Características técnicas mínimas:**

1. Deve possuir solução de gerenciamento centralizado, funcionando ON PREMISES, e também possibilitando o gerenciamento de diversos equipamentos.
  - 1.1. Suportar validação de regras antes da aplicação;
  - 1.2. Suportar validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing);
2. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
3. O Software de Gestão Centralizada deverá ser homologada e totalmente compatível com o item 1 **“FIREWALL - Solução de Plataforma de Segurança de perímetro em cluster, composta por Next Generation Firewall (NGFW) e garantia/suporte 24x7, em português, por ASC Authorized Support Center), incluindo garantia do equipamento por 60 meses”** especificado neste documento para permitir o gerenciamento dos equipamentos e o armazenamento de logs gerados pelos mesmos;
4. Deve permitir a exportação de logs via SCP ou FTP assim como permitir a exportação para soluções de gerenciamento de logs (exemplo: GrayLog);
5. Controle sobre todos os equipamentos da plataforma de segurança em um único console, com administração de privilégios e funções;
6. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual deve ser compatível com VMware ESXi e VSphere Client;
7. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;
8. Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;
9. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;
10. Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;
11. Deve permitir a criação de objetos e políticas compartilhadas;
12. Deve consolidar logs e relatórios de todos os dispositivos administrados;
13. Deve permitir exportar backup de configuração automaticamente via agendamento;

14. Deve permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;

15. Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

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

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

## 16. GARANTIA

Deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a atualização do software para obter novas funcionalidades e correção de bugs. Demais itens referentes à garantia estão descritos nas "Condições Gerais" deste Termo de Referência.

### SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL NGFW

3.1 A contratada deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:

3.1.1 Reunião de alinhamento para criação do escopo do projeto previamente a instalação;

3.1.2 Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);

3.1.3 Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados;

3.1.4 Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

3.1.5 Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;

3.1.6 Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

3.1.7 Configuração do sistema de firewall, VPN, IPS, Filtro URL, Antivírus e Anti-malware de acordo com as exigências levantadas;

3.2 Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos firewalls afim de garantir a melhor eficiência da solução durante o período de vigência das licenças;

3.3 Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances;

3.4 Repasse de informação das configurações realizadas no formato hands-on para a equipe responsável pelo projeto por parte da contratante após validação da migração;

3.5 A instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos deverá ocorrer no Data Center do Ministério das Comunicações, em Brasília-DF, em horário comercial, acordado previamente com a equipe da Coordenação de Infraestrutura da CGTI.

3.6 Todos os cabos de conexão, acessórios e itens relacionados ao completo funcionamento das soluções adquiridas devem ser fornecidos pela CONTRATADA.

## SERVIÇOS DE TREINAMENTO COM PROFISSIONAL CERTIFICADO PELO FABRICANTE DA SOLUÇÃO

- Devido a pandemia de COVID-19, o repasse de conhecimento deverá ser feito a distância, via webconferência;
- O serviço para atualização de conhecimentos (treinamento) deverá ser ministrado em Português;
- Deverá ter **carga horária mínima de 20 Horas**;
- O material de apoio deverá estar em Português;
- O repasse de conhecimento deverá cobrir conhecimentos necessários, de toda a solução contratada, para instalação, administração, configuração, otimização, resolução de problemas e utilização da solução;
- O treinamento compreenderá a transferência de conhecimento das tecnologias envolvidas na Solução de Segurança contratada, envolvendo, no mínimo, os seguintes itens:
  - Equipamento de Firewall: Funcionalidade de Firewall;
  - Funcionalidade de QoS;
  - Funcionalidade de VPN;
  - Funcionalidade de Prevenção de Intrusão;
  - Funcionalidade de Filtragem WEB;
  - Funcionalidade de Prevenção de Ameaças;
  - Solução de Gerenciamento e Relatórios e suas funcionalidades;
  - Funcionalidade de Prevenção de Ameaças Avançadas (Sandbox) e suas funcionalidades;
  - Funcionalidades de DNS security and IoT security;
  - Repasse de informação das configurações realizadas no formato hands-on para a equipe responsável pelo projeto por parte da contratante após validação da migração.
- O treinamento deve ser realizado em dias úteis, no horário das 08h às 12h e das 14h às 18h;
- A CONTRATANTE deve se responsabilizar por qualquer material físico necessário para a execução dos treinamentos.
- O serviço deverá ser ministrado por profissional certificado na solução de proteção de rede;
- O serviço deverá ser baseado no treinamento oficial da solução contratada;
- O certificado de conclusão deverá ser emitido em português brasileiro.

As aulas deverão ser gravadas e disponibilizadas ao MCOM imediatamente após o fim do treinamento.

## CONDIÇÕES GERAIS

### GARANTIA

- Deve possuir garantia do fabricante ou autorizada no Brasil com validade mínima de 60 (sessenta) meses;
- Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;
- Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução;
- Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição nos

locais especificados neste edital, obedecendo a modalidade NBD (Next Business Day);

- Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana);
- O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo:
  - Crítico: significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno. Neste caso o chamado deverá ser aberto via telefone (0800) ou outra forma de contato imediato pela internet;
  - Alta: impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
  - Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
  - Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas, em horário comercial.
- A equipe técnica da contratante poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao sistema;

#### • **CONDIÇÕES DE ENTREGA**

- O prazo de entrega de produtos deverá ocorrer em até 90 (noventa) dias corridos a partir da data de assinatura do contrato;
- A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada;
- Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local para download do arquivo de instalação;

#### • **PADRONIZAÇÃO**

- Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), os equipamentos e softwares, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante;

#### • **CONDIÇÕES DE ACEITE**

- Somente serão aceitos equipamentos novos e sem uso. Não serão aceitos equipamentos re-manufaturados, NFR (Not For Resale) ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;
- O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente especificação técnica;
- Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital. Em caso de dúvida ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnico certificado na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão (conforme itens 1.1.1 e 1.1.2, TC-006.806/2006-4, Acórdão nº 838/2006-TCU-2ª Câmara);

Na data da proposta nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de *end-of-life*, *end-of-support* e/ou *end-of-sale*.

**B - Modelo de Proposta de Preços**

<b>PREGÃO:</b>	<b>Pregão Eletrônico nº ____/20XX</b>
<b>UASG:</b>	
<b>OBJETO</b>	

<b>Grupo</b>	<b>Item</b>	<b>Descrição Equipamento/Software</b>	<b>Código Catesr/Catmat</b>	<b>QTDE</b>	<b>Unidade de Medida</b>	<b>VALOR UNITÁRIO</b>	<b>VALOR TOTAL</b>
1	1	FIREWALL - Solução de Plataforma de Segurança em cluster, composta por Next Generation Firewall (NGFW), licença de uso do sistema de gerenciamento e garantia/suporte 24x7, em português por ASC Authorized Support Center) – Subscrição por 60 meses	484747	02	Unidade		
	2	PLATAFORMA DE GESTÃO E MONITORAMENTO CENTRALIZADO, COM ARMAZENAMENTO DE LOGS, INCLUINDO GARANTIA POR 60 MESES.	27472	01	Licença		
	3	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL NGFW	27014	02	Serviço		
	4	TREINAMENTO - Serviço de treinamento solução adquirida, com carga horária mínima de 20 horas, ministrado por profissional certificado pelo fabricante	16837	01	Capacitação		

**IDENTIFICAÇÃO DA EMPRESA LICITANTE:**

Razão Social:

CNPJ:

Endereço Completo		
CEP:	Fone/Fax:	E-mail:
<b>DADOS BANCÁRIOS:</b>		
Agência:	Conta Corrente:	Banco:
<b>IDENTIFICAÇÃO DO RESPONSÁVEL PELA ASSINATURA DO CONTRATO:</b>		
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 12.5 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, 60 (sessenta) dias

### C - Declaração de Sustentabilidade Ambiental

Declaração de Sustentabilidade	
PROPONENTE:	
CNPJ/RFB:	
ENDEREÇO:	
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Por ser a expressão da verdade, firmamos a presente DECLARAÇÃO.</p>	

_____ 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 xxxxxxxx, 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 XXX;

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 Receptora”), 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 Receptora antes da divulgação pela Parte Divulgadora; ou (iii) sejam legalmente recebidas pela Parte Receptora de

um terceiro, desde que essas informações não tenham chegado ao conhecimento da Parte Receptora 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 Receptora 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 Receptora obrigada também a enviar à Parte Divulgadora cópia da resposta dada à determinação judicial ou administrativa concomitantemente ao atendimento da mesma. A Parte Receptora 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 Receptora 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 Receptora, (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 Receptora 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 Receptora 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 Receptora.
5. A Parte Receptora 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 Receptora 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 Receptora 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 Receptora, 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 Receptora, 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 inexecutável, 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 Receptora 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 Receptora 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 Receptora.

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 Receptora 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 Receptora, 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 - Modelo de Ordem de Serviço

<b>ORDEM DE SERVIÇO</b> <b>Art. 32 da Instrução Normativa SGD/ME nº 01/2019</b>	
<b>1. IDENTIFICAÇÃO</b>	
Nº IDENTIFICADOR DA OSFB	
Nº CONTRATO	
EMPRESA CONTRATADA / CNPJ:	
OBJETO DO CONTRATO:	
	NOME:

GESTOR DO CONTRATO: [caput art. 32 da IN 01/2019/SGD]		<b>ORDEM DE SERVIÇO</b> <b>Art. 32 da Instrução Normativa SGD/ME nº 01/2019</b>			
		<b>1. IDENTIFICAÇÃO</b>			
		E-MAIL:	TELFONE:	MATRÍCULA:	
REQUISITANTE: [Inc. IV do art. 32 da IN 01/2019/SGD]		NOME:			
		E-MAIL:	TELFONE:	MATRÍCULA:	
<b>2. ESPECIFICAÇÃO DOS SERVIÇOS (Inc. I e II do art. 32 da IN 01/2019/SGD)</b>					
ITEM/GRUPO:					
ID	DESCRIÇÃO	UND	QTDE/VOLUME	VL UNITÁRIO	VL TOTAL ITEM
VALOR TOTAL ESTIMADO:					
<b>3. CRONOGRAMA (Inc. III do art. 32 da IN 01/2019/SGD)</b>					
GRUPO/ITEM/ID	PRAZO (EM DIAS)	DATA INÍCIO	DATA ENTREGA		
<b>4. INFORMAÇÕES COMPLEMENTARES</b>					
<b>5. CIÊNCIA DA CONTRATADA</b>					

**ORDEM DE SERVIÇO**

**Art. 32 da Instrução Normativa SGD/ME nº 01/2019**

**1. IDENTIFICAÇÃO**

PREPOSTO DA CONTRATADA: [art. 32 da IN 01/2019/SGD]	NOME:		
	E-MAIL:	TELFONE:	CPF:
Brasília/DF, xx de xxxx de xxxx.			

(\*) Modelo meramente exemplificativo

**F - Modelo de Termo de Recebimento Provisório**

**TERMO DE RECEBIMENTO PROVISÓRIO**

**Identificação**

<b>Contrato:</b>	<b>Nº da OS / OFB:</b>
<b>Objeto:</b>	
<b>Contratante:</b>	
<b>Contratada:</b>	

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**

--

<b>CONTRATANTE</b>	<b>CONTRATADA</b>
<b>Fiscal Técnico do Contrato</b>	<b>Preposto</b>
<b>&lt;Nome&gt;</b> <b>Matrícula: &lt;Matr.&gt;</b>	<b>&lt;Nome&gt;</b> <b>&lt;Qualificação&gt;</b>

\_\_\_\_\_, \_\_\_\_\_ de \_\_\_\_\_ de 20\_\_\_\_

### G- Modelo de Termo de Recebimento Definitivo

#### TERMO DE RECEBIMENTO DEFINITIVO

##### Identificação

<b>Contrato Número:</b>	<b>Nº da OS / OFB:</b>
<b>Objeto:</b>	
<b>Gestor do Contrato:</b>	
<b>Fiscal Requisitante do Contrato:</b>	

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

<b>Gestor do Contrato</b>	<b>Fiscal Requisitante do Contrato</b>

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

\_\_\_\_\_, \_\_\_\_\_ de \_\_\_\_\_ de 20\_\_\_\_.

## H - Estudo Técnico Preliminar



Documento assinado eletronicamente por **Victor Hugo De Souza Peçanha, Integrante Técnico**, em 28/06/2022, às 15:50 (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 **Daniele Meira Borges, Coordenadora-Geral de Tecnologia da Informação e Comunicação substituta**, em 28/06/2022, às 17:15 (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 **Wanessa Queiroz de Souza Oliveira, Subsecretário de Planejamento e Tecnologia da Informação**, em 28/06/2022, às 23:23 (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 **Ivancir Gonçalves da Rocha Castro Filho, Coordenador-Geral de Recursos Logísticos**, em 01/07/2022, às 16:41 (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 <https://super.mcom.gov.br/sei/verifica>, informando o código verificador **10039126** e o código CRC **F69C4ACE**.