Estudo Técnico Preliminar 7/2022

1. Informações Básicas

Número do processo: 53115.028776/2021-04

2. Introdução

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Referência: Art. 11 da IN SGD/ME nº 1/2019.

3. Descrição da necessidade

Solução de segurança de perímetro

4. Área requisitante

Área Requisitante	Responsável
Coordenação-Geral de Tecnologia da Informação e Comunicação (CGTI)	Luiz Fernando Bastos Coura

5. Necessidades de Negócio

- Aquisição de solução de segurança de perímetro contemplando o hardware, software, licenciamento, implantação, configuração, treinamento, garantia, atualizações e suporte técnico, em atendimento à solicitação da Coordenação-Geral de Tecnologia da Informação e Comunicação (CGTI) contida no Documento de Oficialização de Demanda Sei nº 8204972.
- Garantir o perfeito funcionamento da infraestrutura de rede do MCOM e;
- Garantir a segurança das informações do negócio e continuidade dos serviços de TIC.

6. Necessidades Tecnológicas

- Estão incluídos todos os softwares e suas licenças de uso, gerenciamento centralizado, serviços de implantação, garantia a de atualização contínua e suporte técnico durante o período de garantia com repasse de conhecimento da solução a fim de atender as necessidades do MCOM.
- Prover soluções tecnológicas integradas, seguras e de alto desempenho.
- Providenciar suporte técnico e garantia ao Firewall de Próxima Geração, aumentando a segurança da rede do MCOM;
- Disponibilizar treinamento técnico aos servidores do MCOM, permitindo o domínio da solução contratada;

- Transferir as regras do Firewall atual (Palo Alto Networks 5020) para a nova solução contratada;
- Gerar relatórios para rápida análise de informações sobre todo o tráfego da rede, incluindo tentativas de invasão, arquivos maliciosos, aplicações suspeitas e etc.
- Permitir Alta Disponibilidade;
- Possuir pelo menos 3 Gbps de *throughput* com todas as funcionalidades de inspeção ativas simultaneamente para análise do tráfego;
- Proteção do Ambiente de rede contra ameaças através da detecção e proteção em tempo real contra ameaças (IDS/IPS);
- Permitir a decriptografia do tráfego SSL para inspeção de conteúdo;
- Permitir inspeção em camada 7 (nível de aplicação);
- Permitir que os logs sejam armazenados pelo período mínimo de 01 ano e;
- Permitir pelo menos 70.000 novas conexões por segundo.

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

7.1 Requisitos de Sustentabilidade Ambiental

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.

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.

7.2 Requisitos dos Direitos de Propriedade Intelectual e Direitos Autorais da Solução de Tecnologia da Informação

Em conformidade com a IN n° 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:

- 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;
- Destaca-se que o MCOM pretende adquirir hardware e software prontos, nos quais não se aplicará o direito de propriedade intelectual;
- Se aplicará direito de propriedade intelectual ao MCOM sobre toda e qualquer documentação fruto da execução dos serviços prestados.

7.3. Alinhamento estratégico

7.3.1 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	

OE16 - Otimização das infraestruturas de tecnologia da informação	Estratégia de Governo Digital - 2020-2022

7.3.2 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

7.3.3 Alinhamento ao PAC MCOM (2022)

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

7.4. A contratação pretendida NÃO pode ser integrada à Plataforma de Cidadania Digital, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016, pois não está relacionada à oferta digital de serviços públicos.

8. Estimativa da demanda - quantidade de bens e serviços

A quantidade estimada da presente contratação, cujo objeto é a aquisição de solução de proteção de rede Next Generation Firewall(NGFW), em cluster, contemplando o hardware, software de gerenciamento, licenciamento, implantação, configuração e treinamento, incluindo, garantia, atualizações e suporte técnico, por 60 (sessenta) meses, consta especificada na tabela abaixo:

Lote	Item	Descrição Equipamento/Software	Código Catser /Catmat	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 com serviço de suporte técnico remoto por igual período	150100	02 unidades

	2	PLATAFORMA DE GESTÃO E MONITORAMENTO CENTRALIZADO, COM ARMAZENAMENTO DE LOGS, INCLUINDO SUPORTE E GARANTIA POR 60 MESES.	27472	01 unidade
	3	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL NGFW	27014	02 unidades
	4	TREINAMENTO - Serviço de treinamento solução adquirida, com carga horária mínima de 20 horas, ministrado por profissional certificado pelo fabricante	16837	05 capacitações

A Infraestrutura de Rede do Ministério das Comunicações (MCOM) dispõe, atualmente, de dois Firewalls, marca Palo Alto, Modelo 5020, atuando em modo ativo-passivo, os quais foram doados pelo Ministério da Ciência, Tecnologia e Inovação (MCTI) e estão sem garantia e sem suporte técnico especializado, sujeitando-se a riscos e falhas que podem expor a rede à invasões e malwares.

Além disso, dispor de um Firewall sem suporte técnico e garantia do fabricante pode comprometer a segurança de toda a rede do MCOM, pois, em caso de falha geral deste equipamento, ocorrerá a inoperância de toda a intranet do Ministério, paralisando também o acesso da VPN dos servidores que encontram-se em teletrabalho.

Para resolver esse problema, o presente Estudo Técnico Preliminar visa adquirir duas novas unidades de NGFW, provendo, dessa forma, a Alta Disponibilidade da rede. Esse termo, também conhecido como High Availability (HA), em inglês, é uma implantação na qual dois firewalls são colocados em um grupo e sua configuração é sincronizada para evitar um único ponto de falha em sua rede. Uma conexão vital entre os pares de firewall garante um *failover* contínuo, ou seja, no caso de um equipamento ficar inativo o outro assume a gerência da conexão de rede. A configuração de dois firewalls em um par de alta disponibilidade fornece redundância e permite garantir a continuidade dos negócios.

Não obstante, a equipe de planejamento está embasando essa contratação em soluções de fabricantes recomendados no estudo "Critical Capabilities for Network Firewalls", publicado em janeiro de 2022 pela Gartner, a maior empresa de consultoria do mundo da área de tecnologia. O referido estudo relaciona os pontos positivos e negativos de todas as principais fabricantes de NGFW do mundo. Portanto, embasado nisso, a equipe de planejamento da contratação buscou equipamentos de empresas com excelência, provendo assim, um equipamento de segurança que irá proteger o MCOM do maior número possível de ameaças e incidentes oriundos da internet.

- **Item 1: Firewall com suporte, garantia e licenças de proteção com vigência de 60 meses**

Conforme já mencionado, a Alta Disponibilidade é essencial ao funcionamento da rede interna do MCOM. Para isso, um equipamento deve atuar em modo ativo, enquanto o segundo equipamento pode ser visto como um espelho do primeiro, mas operando de forma passiva. Ou seja, no caso de um firewall, o equipamento que opera em modo passivo possui todas as regras e políticas configuradas no equipamento ativo. Isso é realizado através da sincronização entre eles. Se o equipamento ativo apresentar alguma falha, o equipamento passivo passa a atuar de forma ativa, garantindo assim, a disponibilidade da rede e dos serviços.

Em relação às exigências técnicas mínimas, **o subitem 13.2** deste documento busca descrevê-las em detalhes.

- **Item 2: Plataforma de gestão centralizada e armazenamento de logs**

A utilização de um software de gerenciamento centralizado facilita as tarefas de gestão 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.

Dessa forma, o processo de obtenção de informações e geração de relatórios é facilitando, tornando esses processos mais rápidos e eficientes.

Outro fator que deve ser considerado é a capacidade de armazenamento. Quando não se tem um software de gerenciamento e de armazenamento de logs, a capacidade de armazenamento está relacionada ao espaço em disco que o equipamento possui. Com base no Marco Civil da Internet é necessário que os registros sejam armazenados pelo período mínimo de seis meses e alguns tipos de registros, por um período de 12 meses. Dessa forma, um firewall necessita ter um grande espaço em disco. Realizando a integração do firewall ao software de armazenamento, que geralmente são implementados em máquina virtual, pode-se solucionar uma possível falta de espaço em disco com a alocação de mais espaço de armazenamento dedicado ao VM. Essa solução se torna mais rápida e com menor custo do que fazer a aquisição de um disco maior para um appliance. Vale ressaltar que um appliance com um disco menor tem seu valor de aquisição menor. Portanto, a aquisição do software de gerenciamento centralizado e armazenamento de logs é visto como uma alternativa viável e mais vantajosa para a instituição.

Por fim, ressalta-se que, o software de gerenciamento deve atender aos requisitos mínimos elencados **no subitem 13.2** deste documento.

- **Item 3: Serviço de instalação de firewall**

O serviço de instalação de firewall deve considerar a instalação em modo de alta disponibilidade, ou seja, dois equipamentos (um em modo ativo e outro em modo passivo). Para realizar a instalação devem ser realizadas reuniões para planejar e definir datas e eventuais necessidades, como por exemplo: avaliação e/ou manutenção do datacenter e também, a análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados.

A instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos deverá ocorrer no local determinado pela equipe responsável pelo projeto por parte da contratante na cidade de Brasília-DF.

Além disso, as configurações do Firewall PA-5020 que o MCOM dispõe atualmente devem ser inteiramente migradas pela contratada para o novo firewall adquirido.

Outrossim, o serviço de VPN disponibilizado pela solução de Firewall atual deve ser migrado e colocado em funcionamento na nova solução contratada, sob total responsabilidade da CONTRATADA, permitindo que todos os acessos e regras existentes continuem em funcionamento.

Os detalhes técnicos podem ser encontrados no subitem 13.2.

- **Item 4: Treinamento oficial de firewall**

Considerando que se trata da aquisição de uma solução para a qual a equipe da Coordenação de Infraestrutura (COINS) pode não dispor de conhecimento técnico suficiente para manter em operação, deve ser fornecido o treinamento específico da solução, com carga horária mínima de 20 horas, para o gerenciamento da aplicação do Firewall, conduzido pelo próprio fabricante ou por um parceiro certificado e autorizado pelo fabricante a ministrar treinamentos oficiais.

Os detalhes sobre esse item estão expostos no subitem 6.2 deste estudo.

O número de 05 treinamentos foi pensado com base na equipe técnica atual da COINS/CGTI, com o intuito do conhecimento ser disseminado em toda a coordenação.

9. Levantamento de soluções

Durante o levantamento de possíveis soluções, foram identificadas 3 (três) possíveis soluções:

1. Solução Livre de Softwares Livres Gratuitos;
2. Licitação para aquisição de uma solução de proteção de rede Next Generation Firewall(NGFW) de maior capacidade, garantia e suporte;
3. Adesão a Ata de Registro de Preços para aquisição de uma solução de proteção de rede Next Generation Firewall(NGFW)de maior capacidade garantia e suporte.

9.1. Identificação das Soluções (ou Cenários)

- **Solução 1 - Solução livre de Softwares Livres Gratuitos:**

Não há disponibilidade de solução de software livre capaz de atender aos requisitos técnicos nesse contexto. Os firewalls baseados em código aberto ou livre possuem limitações em funcionalidades essenciais como controle/identificação de aplicações.

Apresenta alta complexidade, pois necessita de capacitação permanente da equipe de informática, falta de suporte técnico, baixa cobertura para malwares e novos incidentes de segurança. Além dessas dificuldades, o volume de tráfego de rede vem crescendo a cada ano exigindo hardwares dedicados para essa função. Assim, esta opção está aos poucos sendo substituída por ferramentas pagas com suporte, gerenciamento simplificado e garantia de funcionamento.

- **Solução 2 - Licitação para aquisição de uma solução de proteção de rede Next Generation Firewall (NGFW) de maior capacidade, com suporte e garantia:**

Contratação de empresa especializada na solução, para atender aos requisitos previstos na IN. 01/2019 e realizar a aquisição;

Em se tratando de uma solução corporativa de NGFW (firewall de próxima geração), há no mercado diversas soluções que se posicionam como tal. Esse fato torna mais complexa a análise de qual solução (ou conjunto de soluções) seria adequada para atender à demanda do MCOM.

- **Solução 3 - Adesão a Ata de Registro de Preços para aquisição de uma solução de proteção de rede Next Generation Firewall(NGFW)de maior capacidade, com suporte e garantia:**

Esta solução atende aos requisitos previstos na IN. 01/2019 e apresenta uma série de vantagens, dentre as quais destaca-se a agilidade e a economia do processo de contratação.

10. Análise comparativa de soluções

Com relação a **Solução 1 - Solução livre de Softwares Livres Gratuitos**, evidencia-se que essa solução não tem custos com a aquisição do softwares, mas possui custos indiretos de configuração e gestão **altíssimos** , difíceis de mensurar. Desse modo, a solução apresenta aumento significativo no volume de gestão, passíveis de criar alto impacto ao negócio por gestão ineficiente e/ou ineficaz.

No que tange a **Solução 2 - Licitação para aquisição de uma solução de proteção de rede Next Generation Firewall(NGFW) de maior capacidade, com suporte e garantia** e **Solução 3 - Adesão a Ata de Registro de Preços para aquisição de uma solução de proteção de rede Next Generation Firewall(NGFW) de maior capacidade, com suporte e garantia,** ambas apresentam diversos benefícios diretos, em especial no que se refere à solução centralizada de segurança NGFW, não comprometendo a disponibilidade, integridade, confidencialidade e autenticidade da informação, bem como integração e gerenciamento centralizado através de software de gerência e armazenamento de logs.

Em virtude disso, a seguir está disposta a seguinte análise comparativa das soluções:

Características Avaliadas	Solução 1	Solução 2 e 3		
	Software Livre Gratuito	NGFW-CheckPoint	NGFW-Fortinet	NGFW - Pao Alto
Gerenciamento Simplificado	Não	Sim	Sim	Sim
Interface Web de gerência e configuração de toda solução	Sim	Sim	Sim	Sim
Necessidade de instalação,configuração e treinamento	Não	Sim	Sim	Sim
Compatibilidade com software de gerência e análise de log	Não	Sim	Sim	Sim
Suporte 24x7	Não	Sim	Sim	Sim
Garantia de Funcionamento	Não	Sim	Sim	Sim

Dentre as soluções identificadas, foi preenchido o quadro a seguir para validação de quais soluções se encaixam nos seguintes requisitos exigidos pelo SISP:

REQUISITO	ID DA SOLUÇÃO	SIM	NÃO	NÃO SE APLICA
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	Solução 1		x	
	Solução 2	x		
	Solução 3	x		
A Solução está disponível no Portal do Software Público Brasileiro?	Solução 1	x		
	Solução 2		x	
	Solução 3		x	
A Solução é um software livre ou software público?	Solução 1	x		
	Solução 2		x	
	Solução 3		x	

A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING e e-MAG?	Solução 1			x
	Solução 2			x
	Solução 3			x
A Solução é aderente às regulamentações da ICP-Brasil?	Solução 1			x
	Solução 2			x
	Solução 3			x
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do – e-ARQ Brasil?	Solução 1			x
	Solução 2			x
	Solução 3			x

11. Registro de soluções consideradas inviáveis

Dentre as soluções levantadas, foram identificadas duas que são consideradas inviáveis, quais sejam:

- Solução 1 - Solução livre de Softwares Livres Gratuitos, em face do aumento significativo no volume de gestão e o modelo de contratação ser oneroso para a Administração Pública, considera-se inviável.
- Solução 3 - Adesão a Ata de Registro de Preços para aquisição de uma solução de proteção de rede Next Generation Firewall(NGFW) de maior capacidade, mostrou-se inviável, haja vista que não há disponibilidade de atas que atendam aos requisitos mínimos da solução e estejam aptas para a carona.

12. Análise comparativa de custos (TCO)

Para a contratação em tela, baseado nas melhores práticas de mercado e em contratações similares realizadas pela Administração Pública foi identificada uma possível solução:

- Solução 2 - Licitação para aquisição de uma solução de proteção de rede Next Generation Firewall (NGFW) de maior capacidade.

12.1. Cálculo dos Custos Totais de Propriedade

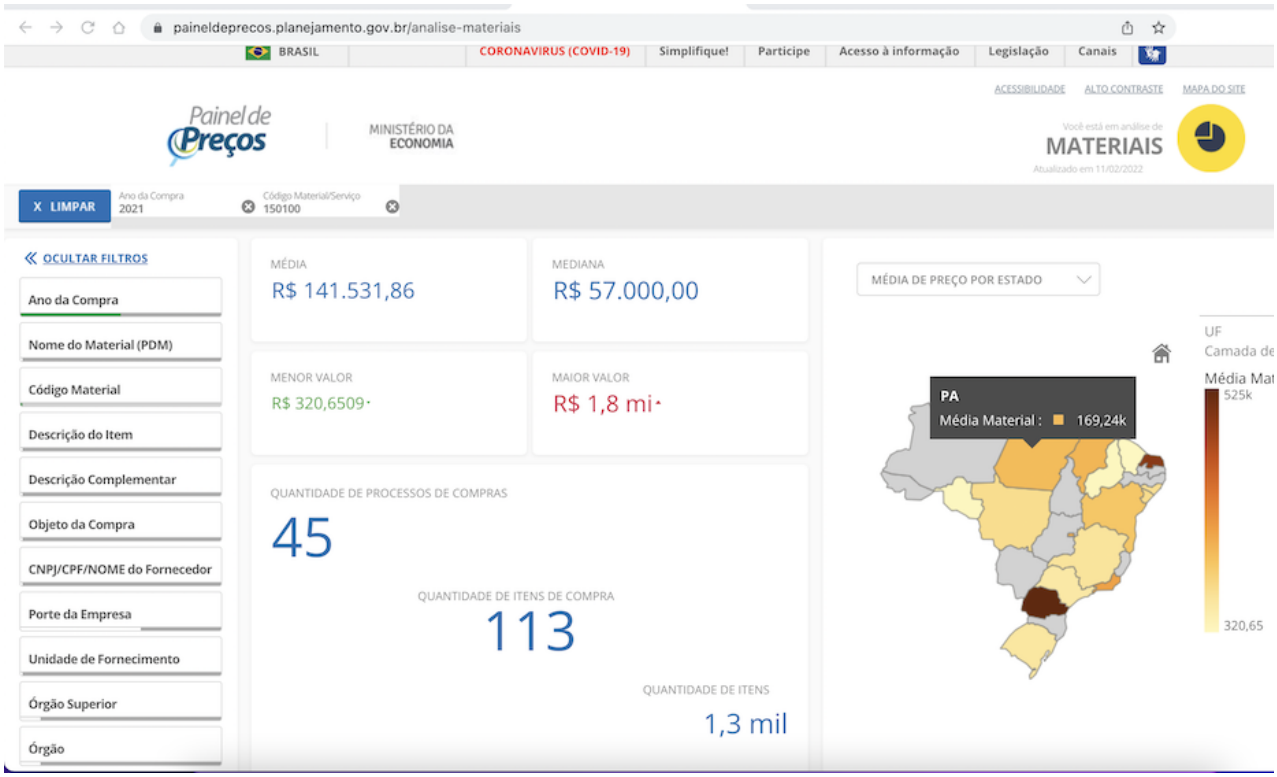
Solução 2 - Licitação para aquisição de uma solução de proteção de rede Next Generation Firewall (NGFW) de maior capacidade, incluindo garantia e suporte técnico.

Uma vez delineado o escopo e os requisitos técnicos mínimos para os equipamentos e softwares que irão compor a solução de firewall de próxima geração, detalhados neste estudo técnico preliminar, a Equipe de planejamento realizou extensa busca no SIASG a procura de atas de registro de preços válidas e com equipamentos compatíveis às demandas elencadas. Para isso, utilizou-se os seguintes filtros:

Ano da compra: **2021**;

Código Material/Serviço: **150100** (Firewall).

Com essa busca foram retornados **45** processos de compras e **113** itens de compra, conforme mostra a figura a seguir:



É importante ressaltar que há no mercado diverso modelos e soluções de firewall, resultando em uma quantidade de possíveis combinações e características relativamente amplas (capacidade de *throughput*, quantidade de sessões novas e simultâneas, quantidade de interfaces). Além das possíveis combinações características de hardware, existem ainda diferentes tipos de licenciamento (período de suporte /garantia, Filtro de URL, Prevenção a ameaças conhecidas ou desconhecidas, Antivírus, Segurança para DNS, etc.). Portanto, entre os processos de compras listados em nossa filtragem, apenas 03 apresentaram compatibilidade aos requisitos buscados neste processo de contratação, conforme tabela 01, mostrada a seguir:

Tabela - Painel de preços do Governo Federal

ID	Identificação da Compra	Unidade de Fornecimento	QTD	Valor Unitário	Órgão	Data d Compr
1	008/2021	UNIDADE	1	729.300,0200	INST.FED.DE EDUC.,CIENC.E TEC.DE BRASILIA	18/09/2(
2	62/2020	UNIDADE	1	734.909,37	Universidade Federal do Rio Grande do Norte	05/10/2(
3	15/2021	UNIDADE	1	632.550	Universidade Federal de Roraima	12/07/2(

Considerando que os itens previstos no presente estudo têm suporte e garantia de cinco anos, então, durante esse período não existirão custos de manutenção. O mesmo vale para custos com licenças, haja vista que são válidas pelo mesmo período.

As licenças deverão ser renovadas no sexto ano, por mais 60 meses (5 anos). Para que, dessa forma, o appliance físico chegue aos 10 anos de uso inteiramente coberto por garantia e suporte.

Os *appliances* físicos, apresentam, em média, uma vida útil de dez anos. Portanto, nos primeiros cinco anos a probabilidade que aconteçam falhas no funcionamento é menor. Após esse período, possíveis problemas devido ao desgaste do hardware que compõem a appliance, como discos e memória RAM, têm maior probabilidade de ocorrer.

Por fim, estima-se o custo total de propriedade na tabela a seguir, levando em consideração os dados expostos no parágrafo anterior:

Item	Descrição Equipamento/Software	QTDE	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 com serviço de suporte técnico remoto por igual período	02 unidades	R$1.190.780,69	R$2.381.561,39
2	PLATAFORMA DE GESTÃO E MONITORAMENTO CENTRALIZADO, COM ARMAZENAMENTO DE LOGS, INCLUINDO SUPORTE E GARANTIA POR 60 MESES.	01 unidade	R$ 126.530,87	R$ 126.530,87
3	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL NGFW	02 unidades	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	05 capacitações	R$ 21.813,11	R$ 109.065,55
			TOTAL	**R$ 2.710.509,78** (dois milhões, setecentos e dez mil quinhentos e nove reais e setenta e oito centavos)

12.2 Mapa Comparativo dos Cálculos Totais de Propriedade (TCO)

Não se aplica ao objeto de contratação.

13. Descrição da solução de TIC a ser contratada

13.1 Descrição da Solução

Após análise comparativa das soluções, a mais viável solução para o MCOM é a **Solução 2** - Licitação para aquisição de uma solução de proteção de rede Next Generation Firewall(NGFW) de maior capacidade, com suporte e garantia**,** pois, além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela equipe CGTI/COINS.

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;

A escolha do agrupamento dos itens em lote 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 contratado 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.

13.2. Registra-se que o objeto da contratação NÃO incide nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD/ME nº 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.*

13.3. Características Técnicas

Item	Descrição
	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 SERVIÇO DE SUPORTE TÉCNICO REMOTO E 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 e 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 de rede 40 Gbps QSFP;

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

1.2.1.11. 01 (uma) interface do tipo console ou similar;

1.2.1.12. 01 (uma) interface dedicada para gerenciamento fora de banda (out-of-band);

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

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

1.2.1.15. 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 atráves 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	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; 1.4.15. 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, 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 SUPORTE E 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;

2	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 serviço de suporte técnico remoto e 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 o armazenamento de logs de forma ilimitada, sem limite de tempo e sem limite de espaço utilizado. Caso seja necessário licenciamento adicional, deverá ser entregue licenciado com a maior capacidade suportada; **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 dever 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 E SUPORTE TÉCNICO** Deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a atualização do software para obter no funcionalidades e correção de bugs. Demais itens referentes a 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	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 de 4 horas 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.
4	**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 c**arga horária mínima de 20 Hora**s; • 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
- 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 se 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 E SUPORTE

- 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 60 (sessenta) 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.***

13.4 Justificativas para o parcelamento ou não da solução

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

O fornecimento de itens por meio de CONTRATADAS distintas trariam enormes riscos ao projeto. Um grande risco viria da necessidade continua 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.

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.

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.

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.

13.5 Contratações correlatas e/ou interdependentes

Não se aplica. A solução pretendida não afeta significativamente outra contratação existente ou pretendida nos artefatos de Planejamento da área (PDTIC; PAC).

14. Estimativa de custo total da contratação

Valor (R$): 2.710.509,78

A estimativa de custo total para a aquisição, 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), pelo período de 60 (sessenta) meses.

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

Tendo em vista a estimativa de preço, destaca-se que o valor não atrai a necessidade de sua aprovação pelo Órgão Central do SISP (art. 1º, §2º, da IN SGD/ME nº 1/2019).

Grupo	Item	Descrição Equipamento /Software	Código Catser /Catmat	QTDE	Unidade de Medida	VALOR UNITÁRIO	VALOR TOTAL
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 com serviço de suporte técnico remoto por igual período	150100	02 unidades	Peças	R$1.190.780,69	R$2.381.561,39
	2	PLATAFORMA DE GESTÃO E MONITORAMENTO CENTRALIZADO, COM ARMAZENAMENTO DE LOGS, INCLUINDO SUPORTE E GARANTIA POR 60 MESES.	27472	01 unidade	Licenças	R$126.530,87	R$126.530,87
	3	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL NGFW	27014	02 unidades	Serviços	R$46.675,99	R$93.351,97
		TREINAMENTO - Serviço de treinamento solução adquirida,					

	4	com carga horária mínima de 20 horas, ministrado por profissional certificado pelo fabricante	16837	05 capacitações	Serviços	R$21.813,11	R$109.065,55

15. Justificativa técnica da escolha da solução

As justificativas técnicas da escolha da solução encontram-se pormenorizadas nos itens 9 e 10.

16. Justificativa econômica da escolha da solução

A justificativa econômica da escolha da solução encontra-se pormenorizada no item 10.

17. Benefícios a serem alcançados com a contratação

Os resultados pretendidos com a presente contratação são:

- Contribuir para garantia de um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;
- Aprimorar a segurança de TIC do Ministério das Comunicações frente a ameaças sofisticadas;
- Possibilitar o controle de acesso e complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;
- Possibilitar o acesso remoto de maneira estável aos colaboradores de forma segura;
- 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.
- Assegurar a sustentabilidade e desempenho dos serviços do Ministério, conforme sua nova topologia e tráfego de rede e;
- Aumento da capacidade de resposta incidentes de segurança.

18. Providências a serem Adotadas

- O Ministério das Comunicações irá designar equipe para fiscalização e gestão do contrato nos moldes do Art. 29 da IN SGD/ME nº 01/2019.
- A Contratada deverá designar preposto para representar a empresa e atuar como principal interlocutor junto ao MCOM.

19. Impactos Ambientais

- Os serviços serão 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.
- Cumprir, no que couber, as exigências do inciso XI, art. 7° da Lei nº 12.305, de 02 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos – PNRS.
- Cumprir, no que couber, as exigências do art. 6° da Instrução Normativa MPOG n° 01, de 19 de janeiro de 2010, que estabelece as práticas de sustentabilidade na execução dos serviços.

20. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

20.1. Justificativa da Viabilidade

O presente ESTUDO TÉCNICO PRELIMINAR, elaborado pelos integrantes TÉCNICO e REQUISITANTE em harmonia com o disposto no art. 11 da Instrução Normativa n° 01/2019/SGD, considerando a análise das alternativas de atendimento das necessidades elencadas pela área requisitante e os demais aspectos normativos, conclui pela VIABILIDADE DA CONTRATAÇÃO, uma vez considerados os seus potenciais benefícios em termos de eficácia, eficiência, efetividade e economicidade, detalhados no item 8 deste documento. Em complemento, os requisitos listados atendem adequadamente às demandas formuladas, os custos previstos são compatíveis e os riscos identificados são administráveis, pelo que RECOMENDAMOS o prosseguimento da pretensa contratação.

21. Responsáveis

VICTOR HUGO DE SOUZA PEÇANHA
INTEGRANTE TÉCNICO

DANIELE MEIRA BORGES
INTEGRANTE REQUISITANTE

Declaro a adequação do conteúdo deste documento às disposições da Instrução Normativa 1/2019-SGD/ME.

WANESSA QUEIROZ DE SOUZA OLIVEIRA
AUTORIDADE MÁXIMA DA ÁREA DE TIC