Estudo Técnico Preliminar 29/2023

1. Informações Básicas

Número do processo: 21000.020025/2023-02

2. Introdução

O Estudo Técnico Preliminar – ETP é o documento constitutivo da primeira etapa do planejamento de uma contratação, que caracteriza o interesse público envolvido e a sua melhor solução. Ele serve de base ao Termo de Referência a ser elaborado, caso se conclua pela viabilidade da contratação.

Este estudo técnico preliminar em questão tem o objetivo de identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Formalização da Demanda SEI Nº 27476908, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas. Além disso, também descreve as análises realizadas em relação às condições da contratação em termos de necessidades, requisitos, alternativas, , justificativas técnicas e econômica, comparativo de custos e resultados pretendidos, com o objetivo de fornecer as informações necessárias para subsidiar o respectivo processo de contratação.
Referência: Inciso XI, do artigo 2º e artigo 11 da IN SGD/ME Nº 94/20

2.1 - GLOSSÁRIO

- **Ministério Provedor -** Ministério da Agricultura e Pecuária.
- **Ministérios Demandantes:**
  - Ministério da Aquicultura e Pesca. Ministério da Desenvolvimento Agrário e Agricultura Familiar.
- **NGFW** - Next Generation Firewall.
- **LGDP** - Lei Geral de Proteção de Dados Pessoais.

3. Descrição da necessidade

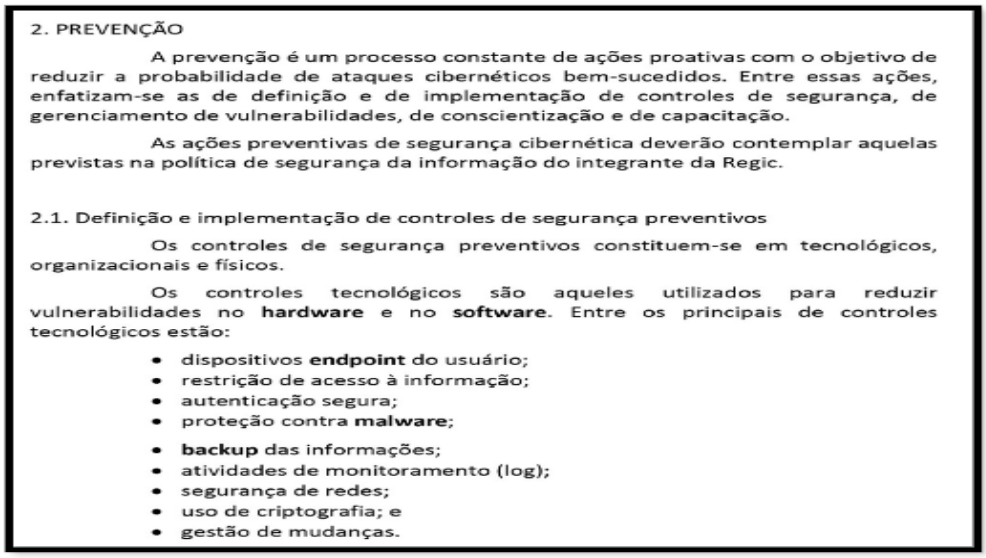
3.1 - CONTEXTUALIZAÇÃO, JUSTIFICATIVA E DESCRIÇÃO DA NECESSIDADE

Os constantes ataques cibernéticos, a necessidade de continuidade do negócio e a evolução de ameaças das mais variadas espécies criam a necessidade de contratação de uma solução eficaz que proteja as informações dos órgãos públicos (MAPA e Ministérios demandantes) e diminua os riscos de acesso indevido às mesmas. Essa crescente disseminação de ataques, em especial à Administração Pública, vem sendo alvo de ações maliciosas com destaque para invasões de sites oficiais, indisponibilidade de recursos e serviços, exposição de vulnerabilidades e consequentes vazamentos de informações, causando assim prejuízos não só ao erário, mas também reflexos negativos no atendimento aos cidadãos , empresas e demais entes envolvidos.

Devido ao aumento significativo dessas ameaças, é imprescindível implementar inteligência e automatização no gerenciamento das soluções de segurança. As ferramentas adotadas para o cenário de outrora tornaram-se insuficientes, uma vez que as tecnologias de mercado evoluíram e o ambiente se expandiu consistentemente. Assim, é prudente acompanhar a evolução e adotar as atualizações tecnológicas necessárias para fornecer serviços adequados e mais seguros. Além disso, em um contexto dinâmico de constante evolução tecnológica e em um curto intervalo de tempo, os equipamentos destinados à segurança da informação podem se tornar obsoletos a tal ponto de não suportarem o aumento do tráfego de internet e dados, o crescimento de novos usuários/novas ameaças e tentativas de invasões das redes corporativas. As tecnologias voltadas à segurança da informação estão em constante evolução, e os fabricantes buscam soluções eficazes para obter o melhor desempenho dos firewalls e ao mesmo tempo prover inteligência proativa, reunindo as mais diversas funcionalidades.

À medida que a dependência do MAPA por sistemas e serviços de informação aumenta, crescem também as ameaças cibernéticas que, muitas vezes, resultam em falhas de segurança críticas que, por sua vez, podem gerar centenas de milhões de reais de prejuízo aos cidadãos, além de causar grandes danos à imagem dos Ministérios (provedor e demandantes).

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) responsável por coordenar as atividades de segurança da informação e das comunicações no governo federal, em sua portaria PORTARIA GSI/PR Nº 120, DE 21 DE DEZEMBRO DE 2022 (https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918) deixa claro as orientações para proteção das entidades publicas do executivo federal, ao qual destacamos:



2. PREVENÇÃO

A prevenção é um processo constante de ações proativas com o objetivo de reduzir a probabilidade de ataques cibernéticos bem-sucedidos. Entre essas ações, enfatizam-se as de definição e de implementação de controles de segurança, de gerenciamento de vulnerabilidades, de conscientização e de capacitação.

As ações preventivas de segurança cibernética deverão contemplar aquelas previstas na política de segurança da informação do integrante da Regic.

2.1. Definição e implementação de controles de segurança preventivos

Os controles de segurança preventivos constituem-se em tecnológicos, organizacionais e físicos.

Os controles tecnológicos são aqueles utilizados para reduzir vulnerabilidades no **hardware** e no **software**. Entre os principais de controles tecnológicos estão:

- dispositivos **endpoint** do usuário;
- restrição de acesso à informação;
- autenticação segura;
- proteção contra **malware**;
- **backup** das informações;
- atividades de monitoramento (log);
- segurança de redes;
- uso de criptografia; e
- gestão de mudanças.

Ainda com relação à portaria citada acima, os controles físicos tem por finalidade prevenir ou evitar o acesso não autorizado à área ou material sensível, bem como os danos e interferências às áreas que contenham informações críticas ou sensíveis. Entre os principais controles físicos estão:

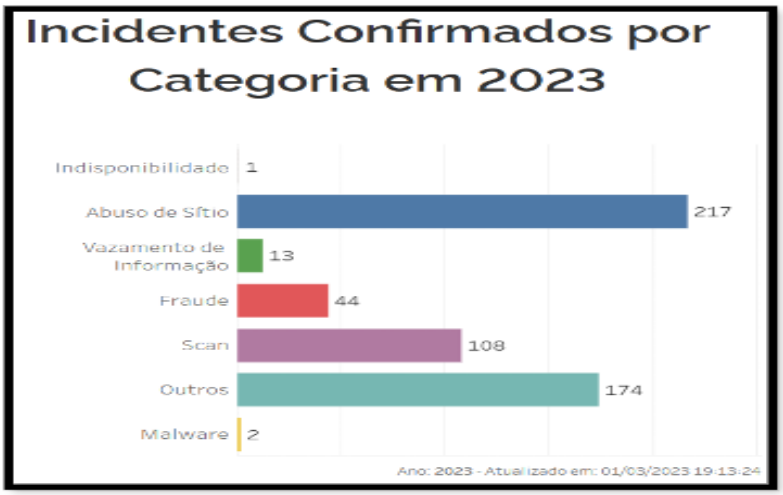
- Definição dos perímetros de segurança física.
- Monitoramento de segurança física.
- Proteção contra ameaças físicas e ambientais.
- Localização e proteção de equipamentos.
- Segurança de ativos fora das instalações da organização e
- Manutenção dos ativos.

Ainda nesta linha o Centro de Prevenção , Tratamento e Resposta a Incidentes Cibernéticos de Governo, entidade que está enquadrada na categoria "CSIRT de responsabilidade nacional de coordenação" publica regularmente relatórios sobre a quantidade de incidentes descobertos (https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/visao-geral) . Vejamos alguns dados importantes:

2019	2020	2021	2022	2023
23.674	24.300	22.298	18.489	3.254
10.716	5.257	4.910	3.786	559
1.201	2.270	3.917	3.189	680

Atualizado em: 01/03/2023 19:13:24

Notificações Incidentes Vulnerabilidades



Percebe-se que a quantidade de incidentes no âmbito do governo federal é extremamente relevante. Em relação à proteção de perímetro, temos que esta é uma das proteções mais importantes em uma instituição, e que se atualizam constantemente por meio de soluções que são conhecidas no mercado como NGFW.

A compra de um Next-Generation Firewall (NGFW) pode trazer vários benefícios para uma organização. Entre elas:

- **Proteção avançada contra ameaças:** Um NGFW oferece recursos de segurança avançados que podem proteger contra ameaças cibernéticas, como malware, phishing, ransomware e ataques de dia zero. Isso inclui recursos como detecção de intrusões, filtragem de URL, antivírus, inspeção de tráfego SSL/TLS e muito mais.

- **Controle de acesso a aplicativos:** Um NGFW permite que uma organização controle o acesso a aplicativos específicos, permitindo ou bloqueando o acesso com base em políticas de segurança definidas. Isso ajuda a proteger contra o uso indevido de aplicativos e reduz o risco de violações de dados.

- **Visibilidade e controle de tráfego:** um NGFW fornece uma visão completa do tráfego de rede, permitindo que as organizações monitorem e controlem o tráfego de entrada e saída. Isso pode ajudar a identificar e mitigar atividades suspeitas e proteger contra vazamentos de dados.

- **Gerenciamento centralizado:** um NGFW pode ser gerenciado de forma centralizada, permitindo que as organizações gerenciem políticas de segurança, implementem atualizações e monitorem o tráfego de rede em vários locais a partir de um único console.

Com a Medida Provisória Nº 1.154, de 1º de janeiro de 2023, o compartilhamento de atividades de administração patrimonial, de material, de gestão de pessoas, de serviços gerais, de orçamento e finanças, de contabilidade, de logística, de contratos, **de tecnologia da informação**, de planejamento governamental e gestão estratégica e de outras atividades de suporte administrativo deve ser realizada por meio de arranjos colaborativos entre **Ministérios ou modelos centralizados**, por isso essa contratação também irá atender, por meio de arranjos colaborativos, os Ministérios da Pesca e Aquicultura e Ministério do Desenvolvimento Agrário e Agricultura Familiar. As despesas executadas para a prestação de serviços administrativos compartilhados serão assumidas pelo Ministério demandante, sem necessidade de celebração de termo de execução descentralizada, nos termos do inciso II do § 3º do art. 3º do Decreto nº 10.426, de 16 de julho de 2020.

Dentro do contexto analisado, a substituição da solução de TIC relacionada ao firewall do MAPA e demais Ministérios demandantes (MPA e MDA) é essencial, uma vez que regula o tráfego de dados entre redes distintas e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede, além de trazer outros inúmeros benefícios que serão detalhados ao longo do estudo técnico preliminar quanto no termo de referência.

3.2 - ALINHAMENTO ESTRATÉGICO

ALINHAMENTO AO PAC

UASG	Nº ITEM	TIPO DE ITEM	SUBITEM	CÓDGIO DO ITEM	DESCRIÇÃO	VALOR TOTAL ESTIMADO R$
130005	274	Soluções de TIC.	Serviço de TIC.	22993	Informática - Suporte Técnico (Software Equipamentos)	R$ 2.800.000,00

ALINHAMENTO AO PDTIC/PLANEJAMENTO ESTRATÉGICO DO MAPA

META 7	NECESSIDADE 5	INDICADOR	OBJETIVO ESTRATÉGICO 23
Tornar as informações, dados e conectividade protegidos e 100% compatível com Normativos de Segurança, incluindo a Lei Geral de Proteção de Dados.	Proteger dados, comunicações e ativos que sejam considerados estratégicos ou identifiquem pessoas físicas e jurídicas.	Aderência à LGPD.	Adequar a capacidade da tecnologia da informação aos novos desafios da transformação digital.

4. Área requisitante

Área Requisitante	Responsável
Coordenadção Geral de Infraestrutura, Cibersegurança e Serviços de TI - CGINFRA	Marco Antônio Bittencourt Sucupira

5. Necessidades de Negócio

A definição dessas características representa o detalhamento do objeto a ser contratado. A seguir, temos alguns requisitos que devem ser cumpridos.

5.1 - REQUISITOS DE NEGÓCIO (NECESSIDADES E ASPECTOS FUNCIONAIS DA SOLUÇÃO DE TIC)

- Aquisição de solução de segurança de perímetro contemplando o hardware, software, licenciamento, implantação, configuração, treinamento, garantia, atualizações e suporte técnico, em atendimento à solicitação (Documento de oficialização de demanda SEI Nº **27476908** da Cooordenação-Geral de Infraestrutura, Cibersegurança e Serviços da Subsecretaria de Tecnologia da Informação do MAPA e demais Ministérios demandantes (Ministério da Aquicultura e Pesca / Ministério da Desenvolvimento Agrário e Agricultura Familiar.)
- Melhorar e garantia o perfeito funcionamento da infraestrutura de rede do Ministério da Agricultura e Pecuária(MAPA) e seus Ministérios demandantes.
- Prover e Garantir a segurança das informações como também a continuidade dos serviços de TIC.
- Assegurar a confidencialidade, disponibilidade e integridades das informações do MAPA e seus Ministérios demandantes em conformidade com a LGPD.
- Melhorar a identificação e o rastreamento das tentativas de invasão às redes.
- Melhoria na implementação de regras e políticas de seguranças relacionados ao uso da rede computacional.
- Melhorar o nível de qualidade e segurança dos serviços e aplicações internas dos Ministérios (Ministério Provedor e demandantes).
- Melhorar a proteção da infraestrutura de TIC de modo a impedir que a rede seja utilizada para outros fins (por exemplo: Mineração de bitcoins, links de internet utilizados para download de conteúdo ilícito , ataques de negação de serviço-DDOS, entre outros).
- Melhoria no reconhecimento e controle da aplicação para detectar e bloquear aplicativos nocivos.
- Melhorar o tempo de resposta aos ataques com automação de segurança.

5.2 - REQUISITOS LEGAIS (NORMAS COM AS QUAIS A SOLUÇÃO DE TIC DEVE ESTAR EM CONFORMIDADE)

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

5.2.1 - LEIS

- Lei Nº 14.133, de 1º de Abril de 2021.
- Lei Nº 13.709, de 14 de Agosto de 2018 e Lei Nº 13.853, de 08 de julho de 2019. (LGPD).

5.2.2 - DECRETOS

- 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.

- Decreto Nº 9.507/2018: Dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;
- 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;
- Decreto-Lei Nº 200, de 25 de fevereiro de 1967 - dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa.
- Decreto Nº10.947, de 25 de Janeiro de 2022. (Regulamenta o inciso VII do caput do art. 12 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional.)

5.2.3 - INSTRUÇÕES NORMATIVAS

- Instrução Normativa SGD/ME Nº 94, de 23 de Dezembro de 2022 (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).
- Instrução Normativa Nº 5 de 25 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.)
- Instrução Normativa SEGES/ME Nº 65, de 7 de Julho de 2021-Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.
- Boas práticas, orientações e vedações para contratação de Ativos de TIC - Versão 4. Orientações específicas para a aquisição de Ativos de TIC. (Este guia está vinculado à Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, conforme § 2º do Art. 8º)
- Instrução Normativa SEGES Nº 58, de 08 de Agosto de 2022. - Dispõe sobre a elaboração dos Estudos técnicos preliminares-ETP, para a aquisição de bens e contratação de serviços e obras, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o ETP Digital.
- Instrução Normativa Nº 01, de 19 de Janeiro de 2010. (Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências.)

5.2.4 - PORTARIAS

- Portaria MGI Nº 43, de 31 de Janeiro de 2023. (Disciplina o compartilhamento de atividades de administração patrimonial, de material, de gestão de pessoas, de serviços gerais, de orçamento e finanças, de contabilidade, de logística, de contratos, de tecnologia da informação, de planejamento governamental e gestão estratégica e de outras atividades de suporte administrativo realizadas por meio de arranjos colaborativos entre Ministérios ou modelos centralizados, e dispõe sobre medidas transitórias decorrentes da edição da Medida Provisória nº 1.154, de 1º de janeiro de 2023.)
- Portaria GSI/PR Nº 120, de 21 de Dezembro de 2022. (Aprova o Plano de Gestão de Incidentes Cibernéticos para a administração pública federal).
- Portaria MAPA Nº 136, de 25 de Maio de 2021 (Aprova a Política de Segurança da Informação do Ministério da Agricultura, Pecuária e Abastecimento - POSIC/MAPA.)
- Portaria MAPA Nº 499, de 17 de Outubro de 2022 - Política de Gestão de Vulnerabilidades Cibernéticas.

5.3 - REQUISITOS DE GARANTIA

- A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o MAPA e órgãos demandantes (MPA e MDA).
- Segundo o item 1.4.5.1, "Para aquisição de servidores de rede, aplicação, equipamentos de backup, armazenamento, segurança, entre outros, deve-se considerar o tempo de vida útil mínimo de 5 (cinco) anos para fins de posicionamento da tecnologia e de garantia de funcionamento", do documento "Orientações específicas para a aquisição de Ativos de TIC" vinculado à Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, a garantia recomendada é de 60 meses para os equipamentos de segurança. Apesar de possivelmente ser tecnicamente mais vantajoso a contratação por 60 meses, pode ser que financeiramente não seja. Portanto, a garantia contratual dos itens da contratação será decidida (12 meses e prorrogáveis até o limite da lei ou 60 meses direto) após a realização da pesquisa de preços final com o envio do termo de referência para os possíveis licitantes, diante de uma análise de simulação de cenários de pagamento e decisão da equipe de planejamento.
- Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos e demais licenças/firmwares/softwares fornecidos com o objetivo de obter novas funcionalidades e correção de bugs;
- Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução;

- Os chamados poderão ser abertos diretamente com a contratada, autorizada oficial do fabricante ou com o próprio 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 24x7x365 (24 horas por dia, 7 dias por semana);
- A contratada deve fornecer garantia de reposição de hardware para situações que sejam identificados problemas constantes na solução fornecida.
- A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se necessário, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.
- O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada.

5.4 - REQUISITOS DE MANUTENÇÃO

- Em caso de falha do(s) hardware(s), caso não seja feita a troca imediata, a contratada deve disponibilizar hardware(s) reserva(s) que irá(ão) permanecer em ambiente de produção do MAPA até o retorno do(s) hardware(s) original(is) reparado ou novo em substituição, a critério do **MAPA e órgãos demandantes (MPA e MDA).**
- Deverá assegurar que o hardware substituto, em qualquer caso, seja igual ao contratado inicialmente ou que possua características superiores a este, desde que estejam homologadas pelo fabricante como parte compatível da solução;
- As peças de substituição devem ser novas, **não sendo aceitas peças usadas ou recondicionadas**;
- A substituição do hardware será considerada consumada no momento em que a solução voltar ao seu funcionamento normal e for aceita formalmente pela equipe técnica do **MAPA.**

- **Manutenção Preventiva**

    - A **manutenção preventiva** será destinada a atualizar os componentes do software e a **realizar quaisquer operações que evitem uma parada parcial ou total da solução.**
    - Durante a manutenção preventiva, a contratada deverá analisar toda a solução, sua condição atual de funcionamento, seus logs de sistemas e sugerir mudanças para uma melhor prática de utilização de ferramenta. A equipe técnica do MAPA junto ao fiscal técnico decidirá sobre a aplicação ou não das recomendações.
    - A **manutenção preventiva deverá ser executada pelo menos 02 vezes por mês** conforme cronograma a ser definido entre o fiscal técnico e equipe técnica da contratada.
    - O cronograma anual poderá sofrer adequações durante o ano vigente , desde que a contratada e o MAPA estejam de acordo e que não seja descumprido o atendimento mensal.
    - Deverá ser gerado um **relatório mensal a cada manutenção preventiva**, que deverá ser entregue até **05(cinco) dias após a visita da contratada.**

- **Manutenção Corretiva**

    - A **manutenção corretiva** será destinada a remover os defeitos apresentados pelos componentes de software e hardware de toda solução de TIC do contrato, compreendendo também a atualização de versões e correções dos componentes de software e hardware que se fizerem necessários.
    - A **manutenção corretiva** será realizada **sempre** que a solução apresentar falha que impeça o seu funcionamento regular e necessite de uma intervenção técnica especializada e, caso necessário, a substituição dos componentes.
    - A **manutenção corretiva** pode ser **solicitada a qualquer moment**o em que o sistema apresente pane, deficiência ou dificuldade de operação.
    - As visitas para prestação dos serviços de manutenção preventiva e corretiva, independente da quantidade necessária, **NÃO deve implicar em custos adicionais para o MAPA.**

5.5 - REQUISITOS TEMPORAIS

- O serviço de substituição de hardware será prestado na modalidade 24x7x365, ou seja, estará disponível para acionamento 24 horas por dia, 7 dias por semana, devendo substituir quaisquer peças ou componentes defeituosos em um prazo máximo conforme último tópico estipulado no item 4.5.2.2.2, contados a partir da data de abertura do chamado (ticket de atendimento).
- O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da Contratada, devidamente aceita pelo fiscal técnico do contrato.
- A entrega total , configuração e implantação completa de todos os bens e da solução de TIC deve ocorrer em no máximo 60 dias úteis a partir da assinatura da ordem de serviço, devendo ser agendada com antecedência mínima de 48 horas. Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local seguro para download dos arquivos de instalação.
- O treinamento deverá ser iniciado em no máximo 10 dias úteis após a instalação e configuração da solução de TIC contratada.
- A contratada deverá cumprir todos os prazos descritos neste estudo técnico preliminar, respeitando os prazos máximos estabelecidos.
- A seguir, segue um resumo de alguns requisitos temporais mais importantes:

ID	DESCRIÇÃO	PRAZO MÁXIMO (DIAS ÚTEIS)
1	Assinatura do contrato (MAPA e contratada)	Início dos prazos - D
2	Realização da reunião inicial(MAPA e contratada). Apresentação formal da equipe de fiscalização do contrato e do preposto. (contratante e contratada). Repasse à contratada dos conhecimentos necessários à execução dos serviços(MAPA). Entrega do termo de compromisso e de ciência devidamente assinados (contratada).	D + 4
3	Entrega do projeto da implantação (contratada)	D + 9
4	Análise e aprovação do projeto de implantação (MAPA)	D + 14
5	Finalização da execução dos serviços e instalação dos bens. (Contratada)	D
6	Início do treinamento	10 dias após o ID 5 ou a depender da disponibilidade dos recursos do MAPA.

5.6 - REQUISITOS DE SEGURANÇA

Na execução dos serviços contratados, a CONTRATADA deverá zelar, no que for de sua competência, pela garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações custodiadas no ambiente gerenciado. Além disso, deve adotar e se responsabilizar por medidas efetivas quanto ao seguinte:

- A contratada deverá submeter-se à **Política de Segurança da Informação** e Comunicações e demais normas de segurança vigentes no MAPA. (Portaria MAPA Nº 136, de 25 de Maio de 2021).
- Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca dos serviços, sem prévia autorização. Ademais, observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação - TI do MAPA.
- Normas e instruções normativas do GSI/PR no que se aplicar à respectiva contratação.
- Assegurar o adequado tratamento de dados pessoais e informações classificadas dos quais venha a ter conhecimento ou manusear em razão da execução do objeto do contrato, nos termos da Lei Federal n° 13.709/2018 e em aderência aos requisitos de segurança da informação vigentes no ambiente do MAPA.
- Evitar vazamento de dados e fraudes digitais nos ambientes gerenciados sob sua responsabilidade técnica;

Quanto ao acesso físico, a CONTRATADA:

- Deverá credenciar junto ao MAPA os seus profissionais, caso seja necessário o acesso às instalações da Sede do MAPA e **órgãos demandantes (MPA e MDA).** para prestação de serviços.
- A contratada deverá apresentar os empregados devidamente uniformizados e identificados por meio de crachá.

5.7 - REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

- Durante a execução de tarefas no ambiente do MAPA, os funcionários da empresa contratada deverão observar, no trato com os servidores públicos em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público.
- A documentação e os manuais de operação da solução deverão ser apresentados preferencialmente no idioma Português (Brasil – PT-BR) e, em sua ausência, deverão ser apresentados em idioma Inglês;
- A abertura de chamados técnicos e encaminhamentos de demandas deverão ser realizados, preferencialmente, sob a forma eletrônica, evitandose a impressão de papel. Além disso, as configurações de hardware e software deverão ser realizadas visando alto desempenho com a utilização racional de energia.
- Em conformidade com a IN SLTI/MPOG n. 01/2010, a CONTRATADA deverá cumprir com os seguintes requisitos de sustentabilidade ambiental, quando aplicável:
    - Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;

- 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;
- 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;
- Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain HazardousSubstances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenil-polibromados (PBDEs).

6. Necessidades Tecnológicas

Segue abaixo as especificações técnicas básicas que devem ser cumpridas pela solução de TIC:

REQUISITOS TÉCNICOS GERAIS DA SOLUÇÃO DE TIC

- A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior data da proposta.
- Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.
- A solução de balanceamento deverá ser fornecida em Alta Disponibilidade do tipo Ativo/Ativo. Transferir todas as regras e configurações dos Firewalls em produção atualmente.
- Tanto os dispositivos físicos (“appliance”) quanto seus softwares deverão ser novos, de primeiro uso, e disponibilizados em suas versões mais atualizadas.
- As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos do mesmo fabricante, desde que obedeçam a todos os requisitos desta especificação (por item/por equipamento). A solução deve suportar o balanceamento entre os appliances de Next generation Firewall ofertados, de modo a permitir que seus throughputs, suas capacidades de análise, capacidades de inspeção bem como todas as funcionalidades pedidas nos itens 01 e 03 e seus subitens sejam somados.
- Os equipamentos dos itens 01, 03 e 06 devem ser do mesmo fabricante, completamente interoperáveis, e devem ser capazes de fazer escalonamento de desempenho com movimentação de appliances dentro da topologia da rede. Autenticação de dois fatores, no que couber, principalmente na plataforma de gerenciamento (item 6 da contratação).
- A solução deve suportar a possibilidade de manutenção dinâmica de um equipamento de um grupo para outro, de acordo com a necessidade da arquitetura definida, sem que haja a perda do tráfego.
- A solução deverá possuir a quantidade de transceptores suficientes para conectar toda a solução à rede corporativa, o que inclui a gerência.

6.1 - REQUISITOS GERAIS DOS ITENS 01 E 03

- Solução integrada de proteção de rede do tipo “Next Generation Firewall” (NGFW), formada pelo conjunto de dispositivos ,obrigatoriamente físicos (appliances), interconectados e operando em modo de alta disponibilidade, com recursos de virtualização de sistemas, filtragem de pacotes, filtro de URL (web-filtering) com controle de transmissão de dados e de acesso à internet, controle de aplicação, controle por meio de identificação de usuários, controle de uso de largura debanda (QoS), VLAN, NAT, DHCP services (server, client e relay), sistema de prevenção de intrusão (IPS) e prevenção contra ameaças de vírus, spywares e malwares, incluindo os de tipo “Zero Day”.
- Conjunto de dispositivo físico (appliance) de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), sistema operacional embarcado no dispositivo e software para sua gestão e monitoramento, permitindo o controle granular das políticas de segurança de rede, atuando além da camada 2 a 4 do modelo OSI, ou seja, além da filtragem por endereços MAC e endereços e portas TCP/IP, permitindo a configuração de políticas de segurança também por aplicações, incluindo seu conteúdo, usuários e tipos de tráfego de rede, recursos tipicamente executados em camada 7.
- O Firewall NGFW deve ser do tipo “rackmount”, permitindo sua instalação em racks de Datacenter , devendo consumir um espaço no rack de no máximo 4U por dispositivo.
- Não serão aceitos equipamentos servidores (“rack servers”) e sistemas operacionais de uso genérico, como Microsoft Windows ou distribuições Linux para usuários finais, adaptados para funcionar como “appliance” físico, ou seja, a solução como um todo de ser fabricada pelo mesmo fornecedor, tanto em seus componentes físicos de hardware quando seus softwares embarcados principais, sendo vedada solução de software livre.
- Todas as funcionalidades da solução Firewall NGFW deverão operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo após o fim do contrato, e mesmo que o MAPA não tenha mais o direito de receber atualizações por descontinuidade da solução por parte da fabricante.

- A solução deve suportar a possibilidade de movimentação dinâmica de um equipamento de um grupo para outro, de acordo com a necessidade da arquitetura definida, sem que haja a perda do tráfego.
- A solução deverá ser provida de forma redundante, de modo que se houver a falha de um ou mais dispositivos, outro(s) possa(m) assumir totalmente o controle, sem que haja perda do tráfego.
- A solução deve ser compatível com SMPv2 e SMPv3. Os appliances devem permitir aceso ao equipamento via interface de comando(CLI), console, SSH, além de interface web HTTPS.
- Os appliances deverão vir acompanhados de todos os conectores, cabeamento e peças de fixação no Rack, necessários à sua instalação e funcionamento, conforme as especificações deste Termo de Referência.
- Todos os componentes devem ser próprios para montagem em rack “19” e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário.

6.2 - REQUISITOS GERAIS DOS ITENS 02,04 E 07

6.2.1 - REQUISITOS BÁSICOS DO ITEM 03

REQUISITOS DE SUPORTE/GARANTIA E MANUTENÇÃO

6.2.1.1 - GARANTIA

- A garantia será prestada com vistas a manter os equipamentos fornecidos e demais itens da solução de TIC em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o MAPA e órgãos demandantes (MPA e MDA).
- Segundo o item 1.4.5.1, "Para aquisição de servidores de rede, aplicação, equipamentos de backup, armazenamento, segurança, entre outros, deve-se considerar o tempo de vida útil mínimo de 5 (cinco) anos para fins de posicionamento da tecnologia e de garantia de funcionamento", do documento "Orientações específicas para a aquisição de Ativos de TIC" vinculado à Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, a garantia recomendada é de 60 meses para os equipamentos de segurança. Portanto, a garantia contratual exigida dos bens será de no mínimo 60 meses para os itens 01,03 e 06 ,contada a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto. Para os itens 02,04,07 e 09, como é inviável realizar o pagamento de todos esses itens em uma parcela, eles terão pagamentos de garantia de forma anual.
- Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos e demais licenças/firmwares/softwares fornecidos com o objetivo de obter novas funcionalidades e correção de bugs. Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução;
- Os chamados poderão ser abertos diretamente com a contratada, autorizada oficial do fabricante ou com o próprio 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 24x7x365 (24 horas por dia, 7 dias por semana); A contratada deve fornecer garantia de reposição de hardware, pelo prazo de vigência do contrato, para situações que sejam identificados problemas constantes na solução fornecida.
- A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se necessário, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.
- Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas). Ao final do contrato, o MAPA deve ter as licenças mais recentes instaladas em modo definitivo (licenças perpétuas).

O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada. Os serviços de “Garantia” também incluem:

- Solução de problemas relativos à indisponibilidade da solução decorrentes de problemas de fabricação, desenvolvimento ou ocasionada pelo uso normal dos equipamentos.
- Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros.
- Esclarecimento de dúvidas de alto nível.
- Instalação de novas versões ou atualizações e patches.

Os chamados abertos envolvendo garantia e manutenção deverão ser atendidos conforme os índices de criticidade que serão detalhados no termo de referência.

6.2.1.2 - MANUTENÇÃO

- Em caso de falha do(s) hardware(s), caso não seja feita a troca conforme prazo especificado, a contratada deve disponibilizar hardware(s) reserva(s) que irá(ão) permanecer em ambiente de produção do MAPA até o retorno do(s) hardware(s) original(is) reparado ou novo em substituição, a critério do MAPA e órgãos demandantes (MPA e MDA).
- Deverá assegurar que o hardware substituto, em qualquer caso, seja igual ao contratado inicialmente ou que possua características superiores a este, desde que estejam homologadas pelo fabricante como parte compatível da solução; As peças de substituição devem ser novas, não sendo aceitas peças usadas ou recondicionadas;

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

6.2.1.2.1 - MANUTENÇÃO PREVENTIVA

- A manutenção preventiva será destinada a atualizar os componentes do software e a realizar quaisquer operações que evitem uma parada parcial ou total da solução. Deve compreender a checagem da saúde e funcionamento da solução já implementada, permitindo diagnóstico preciso dos status da atual rede. Ao final de cada manutenção preventiva, deverá ser elaborado um relatório detalhado dos serviços executados.
- Durante a manutenção preventiva, a contratada deverá analisar toda a solução, sua condição atual de funcionamento, seus logs de sistemas e sugerir mudanças para uma melhor prática de utilização de ferramenta. A equipe técnica do MAPA junto ao fiscal técnico decidirá sobre a aplicação ou não das recomendações. A manutenção preventiva deverá ser executada pelo menos 02 vezes por mês conforme cronograma a ser definido entre o fiscal técnico e equipe técnica da contratada.
- O cronograma anual poderá sofrer adequações durante o ano vigente , desde que a contratada e o MAPA estejam de acordo e que não seja descumprido o atendimento mensal.
- A futura contratada deverá realizar manutenção preventiva, realizando: Análise de logs e configurações da solução, identificando possíveis erros, conflitos e as correções necessárias; Análise de desempenho do funcionamento da solução no que diz respeito ao uso de CPU e memória e recomendar ajustes; Análise física dos equipamentos, incluindo verificações de temperatura, ventilação e eventuais alertas de falhas de hardwares; Análise de vulnerabilidades e de pendências de atualizações de versões de firmwares, engines, assinaturas ou qualquer componente da solução passível de atualização e recomendar as ações necessárias para regularização.

6.2.1.2.2 - MANUTENÇÃO CORRETIVA

- A manutenção corretiva será destinada a resolver os defeitos apresentados pelos componentes de software e hardware de toda solução de TIC do contrato, compreendendo também a atualização de versões e correções dos componentes de software e hardware que se fizerem necessários. Ademais, entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.
- Corresponde ao tratamento dos problemas encontrados na operação da solução, incluindo esclarecimentos de dúvidas relacionadas à instalação, configuração, uso e atualização, além de reposição de peças defeituosas.
- A manutenção corretiva será realizada sempre que a solução apresentar falha que impeça o seu funcionamento regular e necessite de uma intervenção técnica especializada e, caso necessário, a substituição dos componentes. A manutenção corretiva pode ser solicitada a qualquer momento em que o sistema apresente pane, deficiência ou dificuldade de operação.
- As visitas para prestação dos serviços de manutenção preventiva e corretiva, independente da quantidade necessária, não deve implicar em custos adicionais para o MAPA.
- Entende-se por "manutenção corretiva", toda atividade do tipo corretiva não periódica que variavelmente poderá ocorrer durante o período de garantia. A atividade corretiva possui suas causas em falhas e erros no software/hardware e trata da correção dos problemas atuais e não iminentes de fabricação dos equipamentos. Essa "garantia" inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:
    - **Do hardware:** Desinstalação, reconfiguração ou reinstalação decorrente de falhas de fabricação no hardware, fornecimento de peças de reposição, substituição de hardware defeituoso por defeito de fabricação ou ocasionada pelo uso normal dos equipamentos, atualização da versão de drivers e firmwares, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados.
    - **Do Software:** Desinstalação, reconfiguração ou reinstalação decorrente de falhas de desenvolvimento do software, atualização da versão de software, outros problemas envolvidos, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados. Quanto às atualizações pertinentes aos softwares, entende-se como atualização o provimento de toda e qualquer evolução de software, incluindo correções, patches, fixes, updates, service packs, novas releases, versions, builds, upgrades, englobando inclusive versões não sucessivas, nos casos em que a solicitação de atualização de tais versões ocorra durante o período de garantia.
- A contratada deverá substituir as peças quebradas, com defeito ou gastas pelo uso normal dos equipamentos, por outras de configuração igual ou superior, originais e novas, sem que isso implique acréscimo aos preços contratados. Substituir, temporária ou definitivamente, o equipamento defeituoso por outro de mesma marca e modelo e com as mesmas características técnicas, novo e de primeiro uso, quando então, a partir de seu efetivo funcionamento, ficará suspensa a contagem do prazo de reparo, nos casos em que não seja possível o reparo dentro dos prazos máximos estipulados.
- A CONTRATADA fornecerá e aplicará pacotes de correção, em data e horário a serem definidos pelo Contratante, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em software ou firmware dos aparelhos que integrem o objeto do contrato. O atendimento deste requisito está condicionado a liberação pelo fabricante dos pacotes de correção e/ou novas versões de software. Deverá fornecer, ainda, serviços de configuração, instalação, transferência de conhecimento, com licenciamento e garantia durante o período de 60 meses, ao

longo do qual deverão ser fornecidas sem custo adicional todas as correções (patches) e atualizações, inclusive de "firmware", da solução, sempre que houver adição de novas funcionalidades ou correções.

- A contratada deverá substituir os appliances (itens 01, 03 e 06) componentes e/ou acessórios que apresentem defeitos, de forma definitiva, após a intervenção corretiva nos seguintes prazos:
  - Máximo de 15 dias úteis para os itens 01, 03 e 06.
  - Máximo de 20 dias úteis para os demais componentes e acessórios.

6.3 - REQUISITOS DE PROJETO, IMPLEMENTAÇÃO, IMPLANTAÇÃO E DEMAIS ASPECTOS TÉCNICOS REFERENTE AO ITEM 05

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

- Reunião de alinhamento para criação do escopo do projeto previamente a instalação.
- Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte do MAPA. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo e ativo/ativo), a ser decidido no momento da instalação.
- Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados.
- Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos; Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7.
- Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução.
- Configuração do sistema de firewall, IPS, Filtro URL, Antivírus e Anti-Malware de acordo com as exigências levantadas. 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.
- Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances.
- Todos os cabos de conexão, acessórios e itens relacionados ao completo funcionamento das soluções adquiridas devem ser fornecidos pela contratada.

6.4 - REQUISITOS REFERENTE AO ITEM 06

A utilização de um appliance físico 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:

- A solução de gerência deverá ser separada dos appliances de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas nesse tópico.
- Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada.
- Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução.
- Deve possuir solução de gerenciamento e administração centralizado, funcionando ON PREMISES e em nuvem pública, e também possibilitando o gerenciamento dos diversos equipamentos licitados neste termo de referência.
- Suportar validação de regras antes da aplicação.
- Suportar validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing); O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.
- O Software de Gestão Centralizada deverá ser homologada e totalmente compatível com os itens 01 e 03.
- Deve permitir a exportação de logs via SCP ou FTP assim como permitir a exportação para soluções de gerenciamento de logs compatível com Syslog.).
- Centralizar a administração de regras e políticas dos Firewalls, usando uma única interface de gerenciamento. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.
- Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança.
- 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 física /lógica ou topologia de rede.
- Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls.
- 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.

- 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.
- Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado; 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.
- Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes, etc....
- O relatório deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos firewalls, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e Sandboxing).
- A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.
- Deve ser possível exportar os logs em CSV ou TXT.
- Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML.
- Simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões regulatórios apresentados no item anterior.
- Permitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança. Monitorar constantemente o status de conformidade da solução aos padrões regulatórios informados.
- Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade manual.
- Gerar alertas de conformidade notificando os usuários sobre o impacto de suas decisões de segurança trazendo as considerações regulatórias na gestão de segurança.
- Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação. Possuir alertas de políticas e os potenciais violações de conformidade.
- Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança.
- Gerar relatórios regulamentares com base nas configurações de segurança em tempo real.
- Permitir que os relatórios possam ser salvos, enviados e impressos.
- Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino etc..
- A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:
- Visualizar quantidade de tráfego utilizado de aplicações e navegação.
- Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada.
- A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando gráficos referentes a consumo de banda, ataques sofridos e quantidade de eventos gerados e protegidos.
- Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius.
- Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada.
- Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente.
- Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição.
- A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como por exemplo pesquisar logs de Antivirus e navegação web simultaneamente na mesma query de pesquisa.
- O relatório das emulações (sandboxing) deve conter, pelo menos, o print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado.
- A plataforma de gerência centralizada e monitoração deve possibilitar a procura por endereços IP e redes, sendo que os resultados mostrem estas informações nos campos de origem e destino dos logs na mesma tela de pesquisa.
- Possuir mecanismo para que logs antigos sejam removidos automaticamente. Possuir a capacidade de personalização de gráficos como barra, linha e tabela.
- Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino.
- Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU.
- A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria. A solução deve ser capaz de personalizar e criar regras de correlação.

- A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior.
- A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.

6.5 - REQUISITOS REFERENTE AO ITEM 07

- Suporte, garantia e manutenção, compreendendo a atualização do software com o objetivo de obter novas funcionalidades e correções de bugs. No que couber e sempre que necessário, os demais de suporte, garantia e manutenção deste item, serão os mesmos que estão especificados no tópico 4.5.2 e seus subitens (Requisitos de suporte /garantia/manutenção).

6.6 - REQUISITOS REFERENTE AO ITEM 08

- Treinamento oficial sobre a solução de Firewall NGFW oferecida, a ser ministrada aos colaboradores do MAPA(no mínimo 03 pessoas) que atuarão diretamente na administração e operação da solução após sua implementação, com carga horária mínima de 30 horas ou carga horária oficial. Obrigatoriamente, é necessário emitir certificado de participante para 03 pessoas e outros colaboradores poderão participar como ouvintes.
- O treinamento deve iniciar em no máximo 10 dias úteis após a instalação e configuração da solução contratada ou a depender da disponibilidade do pessoal do MAPA.
- Os dias e horários para capacitação serão definidos pelo MAPA, conforme demanda do mesmo, podendo optar por utilizar apenas meio período do dia(ou até menos, se necessário) até completar a carga total prevista, e serão acordados com a contratada com uma antecedência mínima de 15 dias corridos antes do início do treinamento.
- O treinamento deverá abranger tanto teoria quanto exercícios práticos, voltados para conhecimento da arquitetura da solução, sua implantação, configuração/operação e gerenciamento, administração e monitoramento da solução, contemplando todos os aspectos essenciais de funcionamento, além de tratamento de problemas típicos envolvendo a operação da solução. Ademais, deve cobrir os seguintes tópicos: Arquitetura da solução; Configurações iniciais básicas; Alta disponibilidade; Controle de acesso dos administradores da solução; Configuração de Interfaces; Criação e gerenciamento de Zonas de Segurança, Políticas de Segurança e Endereçamento NAT; Controle por Identificação de Aplicações; Controle por Identificação de Usuários, com conexão a fontes externas de autenticação; Criação e gerenciamento de Filtro URL; Descriptografia de tráfego; Configurações de VPN (SSL e IPSec); Monitoramento e Relatórios; Log e Auditoria.
- Deverá ser fornecido certificado a cada um dos servidores públicos participantes do treinamento. A apresentação destes certificados é requisito obrigatório para a comprovação da execução do serviço, sendo o principal artefato a ser utilizado pela equipe de fiscalização contratual para validação do serviço e emissão do Termo de Recebimento Definitivo da solução.
- Todo material didático a ser utilizado deverá ser fornecido pela contratada ou pelo fabricante, devendo esse ser uma documentação oficial do próprio fabricante, impresso ou em PDF com todos os tópicos abordados no treinamento, inclusive com exemplos práticos e ilustrações.
- O instrutor deve ser profissional certificado pelo fabricante dos produtos e com experiência comprovada nos produtos fornecidos.

A critério do MAPA, o treinamento poderá ocorrer em:

- Nas instalações do MAPA. Neste caso, a contratada arcará com todas as despesas relativas e necessárias, tais como transporte, hospedagem e diárias do(s) instrutor(es); infraestrutura complementar da sala e instalações; material didático e coffee break, e demais gastos para a execução do treinamento;
- Em Brasília-DF. A contratada arcará com todas as despesas relativas e necessárias, tais como transporte, hospedagem e diárias do(s) instrutor(es); infraestrutura da sala, das instalações e equipamentos; material didático e coffee break, e demais gastos para a execução do treinamento.

6.7 - REQUISITOS REFERENTE AO ITEM 09

Deverá ter a característica de Zero Trust Network Access e funcionalidades para no mínimo 500 usuários simultâneos com os seguintes aspectos:

- Deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas.
- Deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão.
- Deve prover um método para controlar o acesso, identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust.
- A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por cada usuário.

- Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem.
- Deve ser escalável até 3.000 agentes.
- O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante.
- Deve ser compatível com pelo menos os seguintes sistemas operacionais: Microsoft Windows: 7 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11 (64 bits); Microsoft Windows Server: 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022; Mac OS X: versões 13, 12, 11 e 10.15; Linux: Ubuntu 18.04 e posterior, Debian 11 e posterior, CentOS Stream 8, CentOS 7.4 e posterior, RedHat 7.4 e posterior, Fedora 36 e posterior.
- Deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel.
- A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.2 e 1.3.
- Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários.
- A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso.
- Deve ser possível revogar o certificado de um agente por meio da console central.
- O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso.
- No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados esteja diferente, o acesso deverá ser bloqueado por padrão.
- Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional.
- A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até 05 dias anteriores ao ocorrido.
- Deve existir a possibilidade de restringir o usuário de realizar backup da configuração do agente.
- Deve ser possível enviar os logs para uma ferramenta de consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes.
- A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4.
- Deve ser possível agrupar agentes em grupos e atribuir grupos de agentes a perfis de políticas específicas.
- Deve ser possível exigir uma senha para desconectar o agente da console central.
- Deve ser possível evitar que o usuário realize shutdown do agente após estar registrado na console central. A console central deve apresentar um resumo das informações de cada endpoint, tais como nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede cabeada e WiFi, detalhes do hardware como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão de agente está em uso em um respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA.
- Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem oadministrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas.
- A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa.
- Deve possibilitar definir funções administrativas relacionadas às permissões dos endpoints, de políticas e de configurações gerais.
- Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente que não esteja em conformidade possa se conectar a redes críticas.
- Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos.
- A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de endpoint, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional. Além disso, deve ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows.
- Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as opções de permitir, bloquear ou monitorar.

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

7.1 - REQUISITOS SOCIAIS, METODOLOGIA DO TRABALHO, AMBIENTAIS E CULTURAIS

- Durante a execução de tarefas no ambiente do MAPA, os funcionários da empresa contratada deverão observar, no trato com os servidores públicos em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público.
- A documentação e os manuais de operação da solução deverão ser apresentados preferencialmente no idioma Português (Brasil – PT-BR) e, em sua ausência, deverão ser apresentados em idioma Inglês;
- A abertura de chamados técnicos e encaminhamentos de demandas deverão ser realizados, preferencialmente, sob a forma eletrônica, evitandose a impressão de papel. Além disso, as configurações de hardware e software deverão ser realizadas visando alto desempenho com a utilização racional de energia.
- Em conformidade com a IN SLTI/MPOG n. 01/2010, a CONTRATADA deverá cumprir com os seguintes requisitos de sustentabilidade ambiental, quando aplicável:
    - Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;
    - 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;
    - 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;
    - Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain HazardousSubstances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenil-polibromados (PBDEs).
- 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 matériasprimas 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.
- O MAPA 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.

7.2 - REQUISITOS DE EXPERIÊNCIA PROFISSIONAL/ FORMAÇÃO DA EQUIPE

- Os profissionais que irão implantar a solução de TIC devem ter experiência mínima de 3 anos em implantações /configurações da solução adquirida.
- Os profissionais deverão possuir certificação do Fabricante que o credencie na implantação da solução contratada.

7.3 - REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Na execução dos serviços contratados, a CONTRATADA deverá zelar, no que for de sua competência, pela garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações custodiadas no ambiente gerenciado. Além disso, deve adotar e se responsabilizar por medidas efetivas quanto ao seguinte:

- A contratada deverá submeter-se à Política de Segurança da Informação e Comunicações e demais normas de segurança vigentes no MAPA. (Portaria MAPA Nº 136, de 25 de Maio de 2021).
- Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca dos serviços, sem prévia autorização. Ademais, observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação - TI do MAPA.
- Normas e instruções normativas do GSI/PR no que se aplicar à respectiva contratação.
- Assegurar o adequado tratamento de dados pessoais e informações classificadas dos quais venha a ter conhecimento ou manusear em razão da execução do objeto do contrato, nos termos da Lei Federal n° 13.709/2018 e em aderência aos requisitos de segurança da informação vigentes no ambiente do MAPA.
- Evitar vazamento de dados e fraudes digitais nos ambientes gerenciados sob sua responsabilidade técnica.
- A contratada deverá assinar o termo de compromisso de manutenção de sigilo para fins de segurança de dados e da prestação do serviço, conforme o modelo de Termo de compromisso de Manutenção de Sigilo (https://www.gov. br /governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao).
- Os colaboradores da contratada que atuarem nos serviços iniciais e durante toda a vigência do contrato e do prazo de suporte e garantia, deverão assinar o termo de ciência, conforme o modelo no Anexo-Termo de Ciência (https://www. gov.br/governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao).
- A contratada deverá obedecer, quando aplicável, as normas de segurança da família ISO/IEC 27000.

- A contratada deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, no que diz respeito a todo e qualquer assunto de interesse do MAPA ou de terceiros de que tomar conhecimento em razão da execução do objeto deste documento, devendo orientar seus empregados nesse sentido.
- A contratada deverá manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações de que vier ter acesso durante a execução do contrato.
- A contratada deverá implementar processo de gestão de capacidade e recursos para redundância de forma que a utilização dos recursos seja monitorada, ajustada e as projeções das necessidades de capacidade futura sejam avaliadas para garantir o desempenho dos ativos relacionados ao objeto do contrato, assegurando também a disponibilidade e recuperação de dados e informações, em conformidade com um plano de continuidade relacionado ao objeto contratado, que garanta o nível requerido de continuidade para a segurança da informação durante uma situação adversa.
- A contratada deverá manter controles e procedimentos específicos para assegurar o nível adequado de segurança da informação às redes corporativas da Contratante e da Contratada, de forma a reduzir o nível de risco ao qual a Solução de TIC e a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante;
- A contratada deverá implementar e manter controles específicos para registro de eventos e rastreabilidade de forma a manter trilha de auditoria de segurança da informação e privacidade, aderente a disposto em dispositivo legal correlato publicado pelo GSI/PR, de forma a assegurar a rastreabilidade do tráfego por meio de logs de transações e acessos, conforme especificação de requisitos, e gerá-los e disponibilizá-los à contratante para fins de auditorias e inspeções.
- A contratada deverá utilizar recursos de segurança da informação e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e em versões comprovadamente seguras e atualizadas, de forma reduzir o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante.
- A contratada deverá implementar e manter controles e procedimentos específicos para assegurar completo e absoluto sigilo quanto a todos os dados e informações de que o preposto ou os demais empregados da contratada venham a tomar conhecimento em razão da execução do contrato, de forma a assegurar que seus empregados e outros profissionais sob sua direção e/ou controle respeitem o uso dos dados somente para as finalidades previstas em contrato e as restrições de uso dos ativos utilizado para desenvolvimento e/ou operação da Solução de TIC, cumprindo e fazendo cumprir o disposto nos Termo de Compromisso e Termo(s) de Ciência firmados respectivamente, pelo representante legal e pelo(s) empregado(s) da contratada.
- Todas as informações, documentos e especificações técnicas as quais a contratada tiver acesso em função da execução contratual deverão ser tratadas como confidenciais, sendo vedada sua reprodução, utilização ou divulgação à terceiros, devendo essa zelar pela manutenção do sigilo absoluto do conhecimento adquirido.

7.4 - REQUISITOS DE VISTORIA TÉCNICA

- A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 09:00 às 12:00 / 14:00 às 17:00 horas.
- Embora opcional, é recomendável a realização de visita técnica, e esta deve ser realizada até 03 (três) dias antes da data fixada para a sessão pública, mediante agendamento prévio de acordo com os contatos da Subsecretaria de Tecnologia da Informação do MAPA através dos e-mails: coseg@agro.gov.br e/ou cginfra.sti@agro.gov.br. (Telefone 3218-2208). A realização da visita técnica não se consubstancia em condição para a participação na licitação, ficando, contudo, as licitantes cientes de que após a apresentação das propostas não serão admitidas, em hipótese alguma, alegações no sentido da inviabilidade de cumprir com as obrigações, em face do desconhecimento dos serviços e de dificuldades técnicas não previstas.
- Para vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprando sua habilitação para a realização da vistoria.
- O MAPA emitirá "Declaração de Realização de Vistoria Técnica", ao qual deverá ser apresentado junto a proposta de preços, conforme Anexo-Vistoria, deste Termo de Referência para os licitantes que fizerem a vistoria.
- Caso o licitante opte por não realizar a vistoria, deverá prestar declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação (Conforme anexo-Vistoria). A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

7.5 . FORMA DE PAGAMENTO

7.5.1. O artigo 40, inciso I, da Lei 14.133 de 2021, estabelece que as compras públicas, sempre que possível, devem pautar-se pelas condições de aquisição e pagamento semelhantes às do setor privado, confirmado pelo Acórdão 1177/2014 – Plenário, sendo juridicamente viável aquisição de bens de informática, com a prestação de garantia por determinado período, mediante pagamento integral no momento da entrega e aceitação dos equipamentos.

> *“Art. 15. As compras, sempre que possível, deverão: (...)*
> *III - submeter-se às condições de aquisição e pagamento semelhantes às do setor privado;” Lei 8.666/1993 (GRIFO NOSSO) e "Jurisprudência - Número 196*
> *É juridicamente viável a aquisição de bens de informática, com a prestação de garanti a por determinado período, mediante o pagamento integral no momento da entrega e aceitação dos equipamentos.*
> *Consulta apresentada pelo Presidente do Tribunal Superior do Trabalho indagou ao Tribunal a possibilidade de aquisição de bens de informática, com a prestação de garantia (assistência técnica de preços e serviços) por determinado período, mediante o pagamento integral do valor contratado no momento da entrega e aceitação dos equipamentos. O relator, de início, mencionou que o objeto da Consulta não trata de pagamento antecipado “típico”, em que a entrega do numerário ao fornecedor é feita antes do recebimento do bem ou serviço pela Administração. Na espécie, trata-se de contratação de equipamentos de informática, em que está embutida a prestação de um serviço (assistência técnica durante o período de garanti a), distinção que, na ótica do relator, tem relevância, pois no pagamento antecipado o risco para a Administração configura-se bem maior, já que efetuado antes de qualquer contraprestação por parte do fornecedor. Na situação em tese, o pagamento só seria realizado após o recebimento do bem, objeto principal da contratação. A prestação futura referiria-se apenas ao serviço de suporte técnico durante o período de garanti a, espécie de acessório em relação ao objeto principal. Depois de estabelecer tal distinção, o relator concluiu que é possível a contratação de bens de informática, com a prestação de garanti a, realizando-se o pagamento integral do valor contratado quando do recebimento dos bens." (GRIFO NOSSO)*

7.5.2 . O pagamento antecipado da garantia no momento da entrega e aceitação dos equipamentos é, em tese, considerado, por vezes em diversos órgãos da APF uma prática comum e aceitável. Entende-se que isto se dê pela mitigação de riscos inerentes às variações econômicas, crises e volatilidades, enfrentados em um cenário de 5 (cinco) anos de prestação de serviço.

7.5.3 . Esse entendimento é explicitado no Acórdão TCU 2569/2018 que tratou da auditoria operacional, práticas comerciais adotadas por grandes fabricantes de tecnologia da informação (TI) na relação com a administração pública, por ocasião da contratação de licenciamento de software e seus serviços agregados, em que os serviços agregados são normalmente comercializados junto com as licenças na primeira aquisição, quando têm a conotação de “garantia”, remetendo-se ao Código de Defesa do Consumidor, sendo a renovação opcional após o fim da vigência do primeiro período contratado. Nesse contexto, costuma-se, inclusive, exigir o pagamento à vista:

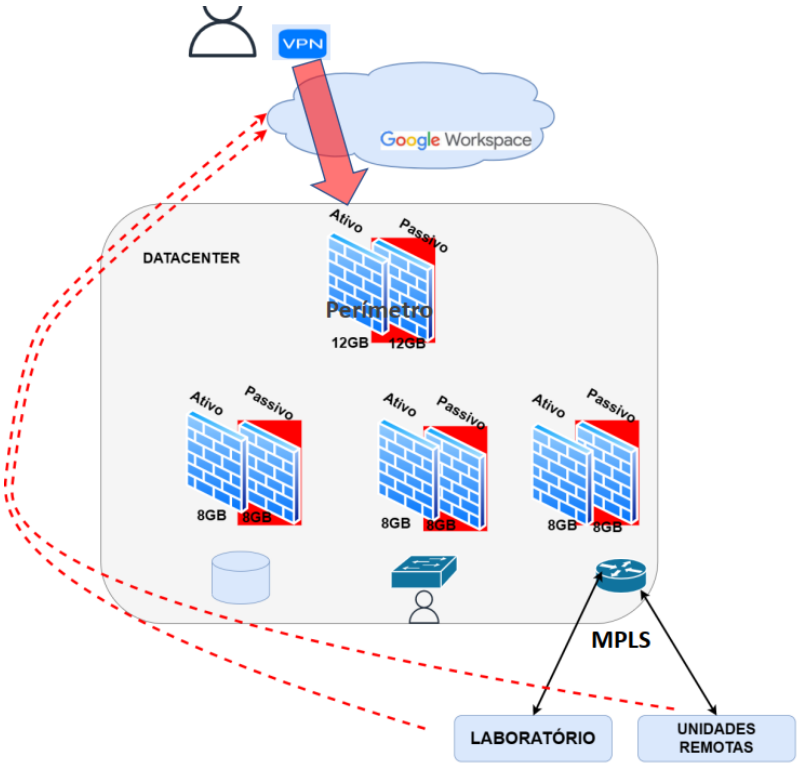
> *"156. Os fabricantes costumam exigir o pagamento à vista para o fornecimento de licenças e de serviços agregados, o que pode resultar na não utilização dos itens adquiridos devido à demora para viabilizar a utilização do software ou à interrupção de projetos. Por outro lado, o pagamento parcelado costuma incluir um custo financeiro da operação no preço final obtido pelas organizações públicas." (GRIFO NOSSO)*
> *"157. Os grandes fabricantes de soluções de TI costumam adotar, no país e também no exterior, a venda de licenças e de serviços agregados mediante recebimento de quantia à vista, seja quando a venda é direta, seja por intermédio de um representante (peça 69, p. 4, questão 6.b; peça 92, p. 4, questões 6.2 e 6.3; peça 95, p. 3, questão 6.2; peça 100, p. 2). Tanto as licenças quanto os serviços agregados possuem peculiaridades que devem ser consideradas pelos gestores na decisão de optar-se pelo pagamento à vista ou parcelado durante o processo da contratação. Além disso, a compra de licenças e de serviços agregados deve ocorrer em momento oportuno dos projetos para evitar que haja dispêndio de recursos em período no qual não há utilização desses itens." (GRIFO NOSSO)*
> *"172. O modelo de pagamento à vista é adotado pela maioria dos fabricantes tanto para licenças como para serviços agregados (parágrafo 157)." (GRIFO NOSSO)*

7.5.4 . Diante do exposto, ratifica-se o posicionamento pelo pagamento à vista dos 5 (cinco) anos - 60 meses - de prestação de serviços agregados de garantia e suporte. Ademais, justificativas adicionais podem ser descritas no termo de referência.

8. Estimativa da demanda - quantidade de bens e serviços

8.1 - CONTEXTUALIZAÇÃO DA DEMANDA

Atualmente o parque computacional de perímetro do MAPA conta com a seguinte arquitetura:



Nota-se que é de posse do MAPA 08 equipamentos de Firewall, distribuídos da seguinte forma:

- 12 Gbps para perímetro. Sendo 1 equipamento de 12Gbps como ativo e outro equipamento de 12Gbps como passivo;
- 8 Gbps para aplicações e banco de dados. Sendo 1 equipamento de 8 Gbps como ativo e outro equipamento de 8Gbps como passivo;
- 8 Gbps para intranet. Sendo 1 equipamento de 8 Gbps como ativo e outro equipamento de 8Gbps como passivo;
- 8 Gbps para rede MPLS ligada a localidades remotas. Sendo 1 equipamento de 8 Gbps como ativo e outro equipamento de 8Gbps como passivo.

Tais equipamentos encontram-se em operação constante e com sua capacidade computacional sendo consumida pelo MAPA. Para o estudo em questão, estima-se uma arquitetura similar com a mesma quantidade de equipamentos, com interesses de trafégo diferentes , de modo a prover flexibilidade e redundância ao MAPA. Além disso, trazendo os outros benefícios que a solução atual não proporciona ao MAPA.

Contudo, há que se pensar que o MAPA possui uma perspectiva de crescimento em seu ambiente computacional, devendo incluir esse ponto nesta contratação. A estimativa da demanda relacionada aos bens e serviços de TIC inclusos nesta contratação consta especificada na tabela abaixo:

ESTIMATIVA DA DEMANDA DA CONTRATAÇÃO

LOTE	ITEM	DESCRIÇÃO	QUANTIDADE
ÚNICO	1	Appliance físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall(NGFW), com licenciamento incluso.	01
	2	Suporte,garantia e manutenção do item 01.	01
	3	Appliance físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall(NGFW), com licenciamento incluso.	03
	4	Appliances físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall (NGFW).	01
	5	Serviço de instalação e configuração dos firewalls NGFW dos itens 01 e 03.	01
	6	Appliance - Plataforma de gestão e monitoramento centralizado, com licenciamento, instalação e configuração.	01
	7	Suporte, garantia e manutenção do item 06.	01
	8	Treinamento ministrado por profissional certificado pelo fabricante.	01
	9	Plataforma de ZTNA - Zero Trust Network Access.	01

9. Levantamento de soluções

Este estudo técnico preliminar identificou como solução para a aquisição de equipamentos Firewall do tipo "Next Generation Firewall(NGFW)" contemplando serviço de instalação, licenciamento, suporte, garantia e treinamento para o ambiente do MAPA, possíveis soluções para a terceirização desse tipo de serviço, conforme pode ser observado no quadro abaixo:

LEVANTAMENTO DE SOLUÇÕES (CENÁRIOS)

ID	DESCRIÇÃO DA SOLUÇÃO (CENÁRIO)
01	Utilização de software livre.
02	Solução de Firewall UTM.
03	Composição de soluções de segurança.
04	Solução de Firewall "*Next Generation Firewall*" (NGFW).

A seguir, iremos demonstrar em detalhes cada cenário, levantando suas vantagens e desvantagens, entre outros aspectos:

9.1 - SOLUÇÃO 01 (UTILIZAÇÃO DE SOFTWARE LIVRE)

Não há disponibilidade de solução de software livre capaz de atender aos requisitos técnicos dessa contratação. Os *firewalls* baseados em código aberto ou livre possuem limitações em funcionalidades essenciais, por exemplo, controle e identificação de aplicações. Ademais, o volume de tráfego vem crescendo a cada ano, desta forma, exigindo hardwares dedicados para essa função. Segue abaixo outras limitações da utilização dessa solução:

- **Suporte limitado:** Embora muitos firewalls de software livre possam ser usados com sucesso em ambientes corporativos, o suporte pode ser limitado, especialmente no Administração Pública. Isso pode resultar em problemas de desempenho ou segurança que podem ser difíceis de resolver sem o suporte adequado.

- **Falta de recursos avançados:** Muitas soluções de firewall de software livre oferecem apenas recursos básicos de segurança e gerenciamento de rede. Isso pode ser suficiente para pequenas empresas ou redes domésticas, mas pode não ser adequado para ambientes maiores ou redes complexas que exigem recursos avançados de segurança, por exemplo, O Ministério da Agricultura e Pecuária.

- P**ossíveis vulnerabilidades de segurança:** Como qualquer software, os firewalls de software livre podem ter vulnerabilidades de segurança que podem ser exploradas por hackers e outros invasores. Embora as comunidades de software livre geralmente sejam rápidas em corrigir vulnerabilidades conhecidas, pode haver um risco maior de exposição a ataques se as atualizações de segurança não forem aplicadas imediatamente.

Um exemplo de solução seria a utilização do software livre (PFSENSE). O PFSense é uma distribuição customizada, livre e open source (de código aberto) do projeto FreeBSD. O fato de se ter uma solução *open source* realizando a proteção de perímetro pode trazer grande preocupação, tendo em vista que não há suporte 24x7 para tal solução, não há um centro de descoberta de ameaças cibernéticas sendo utilizado, e principalmente, não há diversas funcionalidades de segurança de última geração, já amplamente em uso nos dias de hoje. Ainda podemos citas outras desvantagens de uma solução baseada em software livre caso fosse adotada como solução no MAPA, são elas:

1. **Dependência de hardware:** Embora o pfSense possa ser instalado em um hardware existente, o desempenho do firewall pode depender da qualidade do hardware usado. Isso pode ser um problema para organizações que desejam implementar firewalls em larga escala por exemplo, o Ministério da Agricultura e Pecuária e seus Ministérios demandantes.
2. **Gerenciamento de patches:** O pfSense pode exigir atualizações regulares de segurança para manter-se protegido contra ameaças atuais, o que pode ser um desafio para algumas organizações que têm dificuldade em gerenciar patches e atualizações em seus sistemas.
3. **Integração com outros sistemas:** O pfSense pode não ser tão compatível com outros sistemas e aplicativos de segurança, o que pode ser um problema para organizações que desejam integrá-lo com outros produtos e serviços de segurança.

9.2 - SOLUÇÃO 02 (CONTRATAÇÃO DE FIREWALL UTM)

O Firewall UTM é uma solução de segurança de rede que oferece várias funcionalidades de segurança, como firewall de rede. Esse tipo de firewall é adequado para pequenas e médias empresas que precisam de proteção básica contra ameaças cibernéticas. A solução atual está ultrapassada e não comporta o crescimento dos próximos anos. Há que se dizer ainda que tal contrato não possui a possibilidade de utilização de acesso remoto seguro no modelo ZTNA, e que tal fato, caracteriza grande problema de segurança ao ambiente do MAPA.

O firewall UTM não é a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

9.3 - SOLUÇÃO 03 (COMPOSIÇÃO DE SOLUÇÕES DE SEGURANÇA)

A proposta dessa solução é composta de equipamentos e softwares de diversos fabricantes, cada um atuando em uma funcionalidade específica. Por se tratar de diferentes tipos de soluções, muitas vezes são necessários diversos treinamentos para operação dos equipamentos e softwares, que apesar de similares trabalham com sintaxes distintas, sendo necessário treinamento para cada fabricante. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.
Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato, visto que para cada solução será necessária uma licença. Esse tipo de solução dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para as funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

9.4 - SOLUÇÃO 04 (SOLUÇÃO DE FIREWALL "NEXT GENERATION FIREWALL")

O tema de proteção de perímetro com solução de Next Generation Firewall é amplamente conhecido no mercado de Cybersegurança. O que pode diferenciar um fabricante de outro é a capacidade de responder rapidamente a uma ameaça. Para que se tenha esta resposta rápida, se faz necessário o emprego de diversos profissionais e tecnologias.

A titulo de exemplo, imagine que uma vulnerabilidade foi descoberta, fabricantes de NGFW diferente levarão tempos diferentes para defesa de tal vulnerabilidade. Dessa forma quanto mais rápido o fabricante puder defender o seu cliente maior será sua eficiência.

É uma plataforma de rede integrada, baseada em inspeção profunda (deep packet inspection), provendo múltiplos mecanismos de proteção em um único equipamento, tais como Intrusion Prevention System (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte.

O Firewall de Próxima Geração permite: Instalação on-line sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, Stateful Inspection Protocol, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas. Além disso, diversas vantagens de segurança são encontradas nesse cenário de contratação, tais como: Detecção de ameaças avançadas do dia zero, Inspeção de tráfego criptografado, Filtragem de URL, Antimalware, Anti-Phishing, Anti-bot, Políticas de segurança mais granulares, Análise de comportamento de rede, gerencia única e simplificada, configuração facilitada entre outros.

No intuito de buscar quais fabricantes possuem tal eficiência o MAPA recorreu ao Gartner afim de objetivar este estudo. O Gartner é uma empresa de consultoria fundada em 1979 que desenvolve tecnologias relacionadas a introspecção necessária para seus clientes tomarem suas decisões todos os dias. A Gartner trabalha com mais de 10.000 (dez mil) empresas, incluindo CIOs e outros executivos da área de TI, nas corporações e órgãos do governo. A companhia consiste em Pesquisa, Execução de Programas, Consultoria e Eventos.

No que tange a tecnologia de NGFW , o Gartner se posiciona da seguinte forma:

Ante a imagem acima, buscando as melhores soluções de mercado, devemos observar os fabricantes com maior capacidade de execução e visão, quadrante superior direito (Frotinet, Palo Alto Networks e Check Point Software Technologies) para balizar nosso estudo. Tendo como premissa uma solução que possa realizar as funcionalidade de NGFW com escalabilidade, acesso remoto seguro e emulação de arquivos, com correlacionamento de eventos central e gerência unificada.

Outro ponto a ser levado em consideração é que os fabricantes de firewall (NGFW) não participam diretamente das licitações, quem disputa são os revendedores parceiros e distribuidores das respectivas soluções.

10. Análise comparativa de soluções

Dentre as soluções identificadas, a tabela a seguir foi preenchida com o objetivo de identificar quais soluções se encaixam nos requisitos exigidos pelo órgão central do SISP:

REQUISITO	SOLUÇÃO	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 01	X		
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 01		X	
	Solução 02			X
	Solução 03			X
	Solução 04			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 01	X		
	Solução 02		X	
	Solução 03		X	
	Solução 04		X	
	Solução 01			X
	Solução 02			X

A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 03			X
	Solução 04			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 01			X
	Solução 02			X
	Solução 03			X
	Solução 04			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 01			X
	Solução 02			X
	Solução 03			X
	Solução 04			X

A equipe de planejamento da contratação entende que os requisitos mínimos definidos pelo órgão central do SISP não é suficiente para fazer uma comparação das soluções, desta forma, definimos abaixo outras características para comparação:

REQUISITO	**SOLUÇÃO**	**SIM**	**NÃO**	**NÃO SE APLICA**
Gerenciamento simplificado centralizado com funções básicas de relatórios e histórico.	Solução 01		X	
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
Interface WEB de gerência e configuração de toda solução.	Solução 01		X	
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
Compatibilidade com software de gerência e análise de logs.	Solução 01		X	
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
Suporte oficial do fabricante.	Solução 01		X	
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
Garantia de funcionamento.	Solução 01		X	
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
A solução é ou está defasada tecnologicamente ou não é adequada para a Administração Pública Federal.	Solução 01	X		
	Solução 02	X		
	Solução 03	X		
	Solução 04		X	
Treinamento e implantação oficial da solução.	Solução 01		X	
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
Laboratório de segurança para descobertas de ameaças	Solução 01		X	
	Solução 02		X	

/ Inspeção de trafego criptografado / Filtragem de URL avançada.	Solução 03		X	
	Solução 04	X		
Detecção de ameaças avançadas zero-day ; Análise de comportamento de rede.	Solução 01		X	
	Solução 02		X	
	Solução 03		X	
	Solução 04	X		

11. Registro de soluções consideradas inviáveis

11.1 - JUSTIFICATIVA DAS SOLUÇÕES INVIÁVEIS

Diante do exposto abaixo, considerando as diferenças de tecnologia, primando pela segurança cibernética do MAPA, entendemos que as soluções 01,02 e 03 são consideradas inviáveis.

ID	DESCRIÇÃO DA SOLUÇÃO(CENÁRIO)	JUSTIFICATIVA DA INVIABILIDADE DA SOLUÇÃO
01	Utilização de software livre.	Não existe um único produto baseado em software livre que seja capaz de oferecer todas as funcionalidades oferecidas por outras soluções proprietárias reunidas em um único produto. Para implementação da solução por meio de software livre, **seria necessário utilizar várias soluções diferentes e não integradas**, tais como Firewall Iptables, Web Filter Squid, OpenVPN e IPS Snort, entre outras, aumentando exponencialmente **o esforço de implementação e sustentação**, falta de garantia em caso de falhas no software e **ausência de suporte**. Além disso, deve ser considerada a curva de aprendizagem, com capacitação e especialização do corpo técnico existente nas diversas soluções *open sources* citadas e o **possível custo de contratação de mão de obra especializada**, tempo para implementação e custos indiretos. Além disso, podemos citar outras **desvantagens** dessa solução: • Configuração e gerenciamento: O firewall de software livre pode exigir mais **conhecimento técnico para configurá-lo e gerenciá-lo em comparação com os firewalls proprietários**. Isso pode ser um desafio para os profissionais de TI que não estão acostumados a trabalhar com software livre. • Suporte: Embora existam comunidades de usuários e desenvolvedores de software livre que podem oferecer suporte, pode ser **difícil encontrar uma empresa especializada em software livre** para fornecer suporte técnico, **especialmente em caso de falhas críticas**. • Hardware e compatibilidade: A escolha de hardware pode ser mais limitada em relação aos firewalls proprietários, e pode haver **problemas de compatibilidade** com outros softwares e dispositivos de rede • Personalização: Enquanto o software livre oferece mais flexibilidade para personalização, pode haver um custo mais alto para adaptar esta solução às necessidades específicas do MAPA em comparação às soluções proprietárias. • Interoperabilidade: Pode haver **dificuldades em garantir a interoperabilidade** entre um firewall de software livre e outros sistemas de rede e segurança. • Segurança: Pode haver p**reocupações sobre a segurança de dados confidenciais** e sistemas críticos quando se trata desse tipo de firewall. • Conformidade: pode ser necessário garantir que o firewall de software livre atenda a regulamentos e normas de segurança específicas, o que pode ser um desafio para a equipe de TI.
	Solução de Firewall UTM.	Para atender as necessidades da MAPA, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução. Com o intuito de adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos **problemas de performance**

		quando todas as inspeções são habilitadas e ocorre o **compartilhamento do hardware entre vários serviços**, podendo prejudicar o bom funcionamento dos sistemas, **gerando lentidão nos acessos e inclusive ocasionar em parada total.**
03	Composição de soluções de segurança.	A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. Nesse tipo de solução, **não existe nenhuma integração de gerenciamento entre esses servidores e seus respectivos serviços**. Dessa forma, em determinadas situações, por exemplo, obter informações sobre um incidente de acesso indevido, é necessário realizar diversas consultas, em diversos sistemas de armazenamento de logs. Assim, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, **comprometendo a disponibilidade e segurança das informações.** A necessidade da aquisição de diferentes licenças e de diferentes fabricantes poderia fazer com os preços fossem maiores quando comparados a aquisição de uma solução que atenda a todas as necessidades. Além disso, seria necessário que **diferentes treinamentos fossem realizados**, visto que essas soluções, apesar de similares, trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada solução implantada. Isso iria demandar mais tempo dos analistas de TI da UFSM para realizar os treinamentos e possivelmente, se tornaria mais caro que realizar o treinamento de uma única solução. Outro aspecto que deve ser considerado é a **dificuldade de se estabelecer processos de gerenciamento**, pois quando se tem diversos tipos de soluções, fica mais difícil implementar um gerenciamento centralizado, pois muitos equipamentos não permitem integração, conforme já citado anteriormente.

12. Análise comparativa de custos (TCO)

12.1 - ANÁLISE COMPARATIVA DE CUSTOS (SOLUÇÃO 04)

Uma vez detalhado o escopo, cenário ideal e requisitos técnicos mínimos para a solução de TIC em questão, foi realizada uma rápida pesquisa de contratações similares para os itens desta contratação. Bem, a IN SGD/ME nº 94, de 23 de Dezembro de 2022 indica, em seu artigo 20, que as pesquisas de preços devem seguir o método prescrito na antiga Instrução Normativa SEGES/ME no 65, de 7 de julho de 2021, da Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, que inclui:

> 1. Composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços, observado o índice de atualização de preços correspondente;
> 2. Contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;
> 3. Dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;
> 4. Pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou
> 5. Pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

Vale destacar que esta IN dispõe que devem ser priorizados os dois primeiros mecanismos, conforme definido no seu artigo 5º, §1. Lembremos, porém, **que neste momento estamos, em princípio, realizando estudo preliminares,** de forma que podemos utilizar quaisquer desses parâmetros, ou uma combinação deles, zelando sempre para que as estimativas estejam próximas à realidade do mercado. Independentemente, um**a pesquisa de preços completa será formalizada, de acordo com a** Instrução Normativa SEGES/ME no 65, de 7 de julho de 2021, **nos autos do processo quando da estimativa do preço final da contratação.**

Abaixo, segue a tabela com a **estimativa de preços preliminar** através de contratos similares:

- Ministério das Comunicações-MCOM (Documento SEI Nº 27909400)
- INEP - Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Documento SEI Nº27909355)
- PREVIC - Superintendência Nacional de Previdência Complementar (Documento SEI Nº27909466)
- IFB-DF - Instituto Federal de Educação, Ciência e Tecnologia de Brasília (Documento SEI Nº 27909585)
- EBSERH - Hospital Universitário de Santa Maria da Universidade Federal de Santa Maria (Documento SEI Nº 28068591)

Diante de tais contratações, a característica principal (throughput) dos equipamentos ofertados foram analisadas conforme abaixo:

Contratação	**Fabricante**	**Throughput**	**Valor**	**Vigência**
Contratação MCOM	Fortinet	3Gbps	R$ 560.000,00	Vigência do contrato de 12 meses e garantia de 60 meses.
Contratação INEP	N/A	10Gbps	R$ 2.214.800,00	Vigência do contrato de 36 e garantia de 36 meses.
Contratação PREVIC	N/A	4,4Gbps	R$ 550.000,00	Vigência do contrato de 12 meses e garantia de 48 meses.
Contratação IFB-DF	Checkpoint	5Gbps	R$ 729.300,02	Vigência do contrato de Garantia de 60 meses.
Contratação EBSERH	Palo Alto	1Gbps	R$ 386.000,00	Garantia de 36 meses.

Logo após, obteve-se o valor estimado por 1 Gb, com licenciamento para o período de 12 meses.

Contratação	**Valor Gb**	**Valor Gb / mês**	**Valor Gb/ano**	**Média de Gb /ano**
Contratação MCOM	R$ 186.666,66	R$ 3.111,11	R$ 37.333,32	R$ 60.049,71
Contratação INEP	R$ 221.480,00	R$ 6.152,22	R$ 73.826,66	
Contratação PREVIC	R$ 125.000,00	R$ 2.604,16	R$ 31.249,92	
Contratação IFB-DF	R$ 145.860,00	R$ 2.431,00	R$ 29.172,00	
Contratação EBSERH	R$ 386.000,00	R$ 10.722,22	R$ 128.666,67	

Em seguida, estimamos com base na quantidade de throughput desejada (23Gbps e 11Gbps) para os itens 01 e 03, aos quais foram calculados abaixo.

Estimativa para o item 01 e 03

Valor Média Gb ano	Throughput estimado	Estimativa Média do item 01 (Unitário)	Throughput estimado	Estimativa do item 02 (Unitário)
R$ 60.049,71	23Gbps	R$ 1.381.143,42	11Gbps	R$ 660.546,85
Estimativa média para o item 01 **R$ 1.381.143,42**			Estimativa média para o item 03 **R$ 660.544,83**	

Consolidando todos os valores chegamos aos valores médios por item, conforme explicitado abaixo:

LOTE	ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
ÚNICO	1	Appliance físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall(NGFW), com licenciamento incluso.	01	R$ 1.381.143,42	R$ 1.381.143,42
	2	Suporte,garantia e manutenção do item 01.	01	R$ 1.472.136,55	R$ 1.472.136,55
	3	Appliance físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall(NGFW), com licenciamento incluso.	03	R$ 660.544,83	R$1.981.634,49
	4	Appliances físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall (NGFW).	01	R$ 2.070.923,69	R$ 2.070.923,69
	5	Serviço de instalação e configuração dos firewalls NGFW dos itens 01 e 03.	01	R$ 223.237,26	R$ 63.562,50
	6	Appliance - Plataforma de gestão e monitoramento centralizado, com licenciamento, instalação e configuração.	01	R$ 118.072,29	R$ 118.072,29
	7	Suporte, garantia e manutenção do item 06.	01	R$ 50.040,16	R$ 50.040,16
	8	Treinamento ministrado por profissional certificado pelo fabricante.	01	R$ 62.896,12	R$ 62.896,12
	9	Plataforma de ZTNA - Zero Trust Network Access.	01	R$ 208.674,70	R$ 208.674,70
Desta forma, a estimativa preliminar para a contratação é de R$ 7.409.083,92					

Observações: É importante ressaltar que no mercado existem diversos modelos e soluções de firewall próximas/diferentes, resultando em uma quantidade de combinações e características relativamente amplas (capacidade de throughput de diversos tipos, quantidade de sessões novas e simultâneas, quantidade de interface, usuários simultâneos, quantidade de políticas de firewall, entre vários outros fatores.), desta forma, não foi possível observar nenhuma que pudesse trazer o mesmo escopo da contratação ora pretendia. Diante disso, após a elaboração do termo de referência será feita uma pesquisa de preços completa conforme a legislação em vigor, conforme dito anteriormente acima, com o objetivo de refletir a realidade do mercado e preços atualizados de acordo especificamente com o detalhado no termo de referência.

12.2 - MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE(TCO)

Conforme o § 1º do inciso V do artigo 11 da Instrução Normativa SGD/ME Nº94, de 23 de Dezembro de 2022, a equipe de planejamento da contratação está dispensando a realização dos respectivos cálculos de custo total de propriedade das soluções consideradas inviáveis. Portanto, conforme apresentado no presente estudo, **apenas a solução 04 foi classificada como viável**.

Observações: Após o envio do termo de referência para os possíveis licitantes, a equipe de planejamento da contratação decidirá se o mais vantajoso economicamente é um contrato de vigência de 24 sendo prorrogáveis até o limite da Lei Nº 14.133 com um item de garantia separadamente ou se é melhor ter um contrato com vigência de 60 meses com garantia de mesmo período e valor incluso nos equipamentos.

Cenário 01- Contrato com vigência de 60 meses com garantia de mesmo período e valor incluso nos equipamentos.

ESTIMATIVA de TCO ao longo da contratação (cenário 01 de pagamento)

ANO 1	ANO 2	ANO 3	ANO 4	ANO 5	TOTAL
R$ 7.409.083,92	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	**R$ 7.409.083,92**

Cenário 02 - Contrato com vigência de 24 meses sendo prorrogáveis até o limite da Lei Nº 14.133, tendo o item de garantia separadamente. Nesse caso, dos contratos consultados, em nenhum deles o item de garantia foi cobrado separadamente, por isso não há como fazer um TCO desse cenário de pagamento no momento.

13. Descrição da solução de TIC a ser contratada

A solução de TIC a ser contratada será através do item 04 Solução de Firewall "*Next Generation Firewall*" (NGFW).

13.1 - PARCELAMENTO DA SOLUÇÃO

O objeto do certame não será parcelado, uma vez que os bens e serviços que compõem o objeto formam um conjunto indissociável, composto pela interligação dos serviços que funcionam harmonicamente. As melhores práticas de gestão em TI se baseiam na integração dos serviços, que são indissociáveis e apresentam inter-relação entre si, de forma que assegurem o alinhamento e a coerência em termos de qualidade técnica, resultando assim, no perfeito atendimento dos princípios da celeridade, economicidade e eficiência.
Somente a execução de forma integrada dos serviços garante a disponibilidade, segurança e a preservação dos dados de execução, evitando transferência de responsabilidades, nos casos de eventuais problemas causados por serviços prestados por mais de uma empresa CONTRATADA.

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 MAPA. 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.

Ademais, 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.

É importante também, se observar o posicionamento do Egrégio Tribunal de Contas da União, nos autos do Acórdão nº 1916 /2009 – Plenário, sob a matéria:

> *“15. Acerca da alegada possibilidade de fragmentação do objeto, vale notar que nos termos do art. 23, § 1º, da Lei n. 8.666/1993, exige-se o parcelamento do objeto licitado sempre que isso se mostre técnica e economicamente viável. A respeito da matéria, esta Corte de Contas já editou a Súmula n. 247/2004, in verbis: “É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das*

licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes...” (grifou-se).

Depreende-se, portanto, que a divisão do objeto deverá ser implementada sempre que houver viabilidade técnica e econômica para a sua adoção.
Nesse ponto, calha trazer à baila o escólio de Marçal Justen Filho: “O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. Não é possível desnaturar um certo objeto, fragmentando-o em contratações diversas e que importam o risco de impossibilidade de execução satisfatória.” (Comentários à Lei de Licitações e Contratos Administrativos. 10. ed. São Paulo: Dialética, 2004. p. 209).”
Adicionalmente, em virtude da especificidade do objeto, pode-se afirmar ser tecnicamente inadequado o seu desmembramento, sob pena de não se atender o objetivo buscado, no sentido de fortalecer a disponibilidade, segurança, a preservação dos dados e ativos de TI do MAPA na manutenção da operabilidade do ambiente de TI.
Ainda, sob o ponto de vista econômico, não há elementos nos autos que permitam concluir que a adoção do parcelamento do objeto, seria, no caso concreto, mais vantajosa para o MAPA.

Por fim, o objeto não será parcelado, pois constitui-se em uma única solução de TIC e os serviços que compõem o objeto licitado são serviços de mesma natureza, dependentes entre si, e sua divisão impactaria na execução do projeto e tornaria a contratação menos econômica, eficaz e eficiente para a Administração. Assim, considerando-se a inviabilidade técnica e econômica para o parcelamento do objeto da presente contratação, bem como consideradas as suas respectivas peculiaridades, interdependência e natureza acessória entre os serviços que compõem o objeto, a **contratação pretendida deverá ser realizada em um único grupo.**

14. Estimativa de custo total da contratação

Valor (R$): 7.409.083,92

A metodologia usada para estimativa de valores da contratação foi o valor médio das contratações similares encontradas nos últimos 02 anos. A estimativa de custo total para esta aquisição , de acordo com as necessidade do Ministério da Agricultura e Pecuária-MAPA, é de **R$ 7.409.083,92,** pelo período de 12 meses.

LOTE	ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
ÚNICO	1	Appliance físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall(NGFW), com licenciamento incluso.	01	R$ 1.381.143,42	R$ 1.381.143,42
	2	Suporte,garantia e manutenção do item 01.	01	R$ 1.472.136,55	R$ 1.472.136,55
	3	Appliance físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall(NGFW), com licenciamento incluso.	03	R$ 660.544,83	R$ 1.981.634,49
	4	Appliances físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall (NGFW).	01	R$ 2.070.923,69	R$ 2.070.923,69
	5	Serviço de instalação e configuração dos firewalls NGFW dos itens 01 e 03.	01	R$ 223.237,26	R$ 63.562,50
	6	Appliance - Plataforma de gestão e monitoramento centralizado, com licenciamento, instalação e configuração.	01	R$ 118.072,29	R$ 118.072,29
	7	Suporte, garantia e manutenção do item 06.	01	R$ 50.040,16	R$ 50.040,16
	8	Treinamento ministrado por profissional certificado pelo fabricante.	01	R$ 62.896,12	R$ 62.896,12
	9	Plataforma de ZTNA - Zero Trust Network Access.	01	R$ 208.674,70	R$ 208.674,70

Desta forma, a estimativa preliminar para a contratação é de R$ 7.409.083,92

15. Justificativa técnica da escolha da solução

Considera-se tecnicamente viável a Solução 04 pela necessidade de um equipamento para atender as demandas de segurança e gestão da rede do MAPA e seus Ministérios demandantes, tendo em vista a não renovação do contrato atual de firewall. Além de oferecer um nível maior de segurança à rede, um firewall de próxima geração, com uma maior capacidade de processamento, possibilita a implementação de novos serviços, por exemplo, análise do tráfego, ZTNA, entre outros. Com isso, será possível ter uma visualização detalhada da utilização da rede e das aplicações utilizadas. Adicionalmente, o processo de identificação de ameaças é facilitado e permite a aplicação de políticas de segurança mais eficientes.

Do ponto de vista da solução de Acesso Remoto Seguro, há que se dizer que o MAPA possui atualmente cerca de 200 licenças de VPN, aos quais funcionam em modelo flutuante, ou seja, podem ter apenas 200 conexões ao mesmo tempo. Tal modelo de acesso remoto deverá ser substituído por um modelo de acesso seguro, sem a necessidade de VPN, em modelo de confiança zero. Adicionalmente, a solução atual de firewall tem difícil integração com outras soluções de segurança do mercado.

Outra funcionalidade importante que pode ser implementada é a identificação de usuários que utilizam a rede e o registro de conexões, permitindo um melhor inventário dos ativos de TI do MAPA e seus Ministérios demandantes. Com o aumento no número de usuários trabalhando de casa, a quantidade de conexões externas para trabalho fora das instalações dos Ministério (trabalho remoto) aumentou consideravelmente durante o período de pandemia, aumentando a necessidade de conexões VPN suportadas pelo equipamento antigo. O aumento na quantidade de ataques às empresas, precipuamente na tentativa de sequestro de dados em troca de resgate, fez com que a necessidade de um firewall que pudesse mitigar melhor ataques de negação de serviço, bloquear infecções maliciosas, ter uma maior e mais rápida análise do tráfego de dados na rede institucional. principalmente em casos de ataques de ransomware, ficasse evidente para o setor de tecnologia da informação do MAPA.

15.1 . DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS

Não se aplica.

16. Justificativa econômica da escolha da solução

Deve-se atentar não somente os custos de cada solução possível, mas também aos diversos benefícios que elas proporcionam, pois o objetivo não é apenas gastar menos recursos públicos, mas qualificar o gasto, isto é, atender satisfatoriamente às necessidades sem esquecer da razoabilidade. Outras justificativas econômicas estão pormenorizadas ao longo dos itens 09 ao 12.

Deste modo, tivemos apenas uma solução viável e não há como fazer comparação econômica em relação às demais soluções levantadas.

16.1 . DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS

Não se aplica.

17. Contratações Correlatas

Atualmente o MAPA possui o contrato Nº 19/2021 com a empresa OGASEC CONSULTORIA E INFORMÁTICA S.A cujo objeto é prestação de serviço de atualização da solução de segurança integrada AKER de firewall e analisador de conteúdo web existente no Ministério da Agricultura e Pecuária. Além desse, é importante citar o contrato 33/2022, em que temos perfis profissionais de segurança da informação que podem executar os serviços de Gerenciamento de acessos, Administração de IPS, ZTNA, Administração/Configuração de Firewall, Configuração de regras de firewall, configuração de filtro de URL, entre outros.

Portanto, este respectivo estudo visa a substituição e aprimoramento da contratação com diversos novos recursos.

18. Benefícios a serem alcançados com a contratação

Os **resultados pretendidos** com essa contratação são:

1. Aumento da capacidade de resposta aos incidentes cibernéticos.
2. Melhorar o acesso remoto de maneira estável aos colaboradores de forma segura.
3. Aprimorar a segurança de TIC do Ministério da Agricultura ,e demais órgãos atrelados, frente às recentes ameaças.
4. Contribuir para a garantia de um nível adequado de Confidencialidade, Integridade e Disponibilidade.
5. Maior visibilidade do trafego das informações e da rede, possibilitando a detecção e proteção em tempo real contra as ameaças. Com isso, será possível corrigir comportamentos inadequados; direcionar recursos para demandas mais relevantes; controlar serviços e aplicações suspeitas ou que interferem diretamente na produtividade.
6. Permitir a criação de políticas de proteção da rede contra eventuais ataques de usuários mal-intencionados, através do bloqueio de portas não utilizadas e controle mais refinado de uso de banda de internet, a fim de evitar abusos em sua utilização;
7. Maior rapidez na detecção - Priorização de alertas de segurança e avisos constantes sobre normas de cibersegurança dentro de uma organização, evitando que erros humanos sejam cometidos na hora de acessar links duvidosos e outras páginas maliciosas.
8. Aprimorar a detecção e bloqueio de ameaças avançadas, como malware, ataques de negação de serviço distribuídos (DDoS) e tentativas de invasão de rede.
9. Melhoria na geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
10. Melhoria na filtragem de conteúdo web, implementando uma filtragem mais abrangente, com criação de regras de uso de aplicações web, que permitam a limitação de acesso a certas categorias de serviços, por meio de análise de tráfego.

19. Providências a serem Adotadas

Não se aplica.

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 artigo 11 da Instrução Normativa Nº 94/2022 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 benefícios em termos de eficácia, eficiência, efetividade e economicidade, detalhados ao longo deste documento. Em complemento, os requisitos listados atendem adequadamente às demandas formuladas, os custos são compatíveis e os riscos identificados são administráveis, pelo que recomendamos o prosseguimento da pretensa contratação.

21. Responsáveis

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

THIAGO PEREIRA DA COSTA

Chefe da Divisão de Privacidade e Proteção de Dados

Assinou eletronicamente em 17/07/2023 às 14:54:57.

MARCO ANTONIO BITTENCOURT SUCUPIRA

Membro da comissão de contratação

Assinou eletronicamente em 18/07/2023 às 09:22:18.

CAMILO MUSSI

Autoridade competente

Assinou eletronicamente em 18/07/2023 às 16:09:16.