

Estudo Técnico Preliminar 3/2023

1. Informações Básicas

Número do processo: 01400.000997/2023-52

2. Descrição da necessidade

2.2. Características institucionais e vinculação da necessidade à transformação do Ministério da Cultura (MinC)

2.2.1. Por meio da publicação do Decreto nº11.336, de 1º de janeiro de 2023, foi formalizado o desmembramento da Secretaria Especial de Cultura do Ministério do Turismo para a criação do Ministério da Cultura.

2.2.1.1. Desta forma, o Ministério da Cultura é o órgão da administração pública federal direta, que tem como principais competências os seguintes temas:

I - política nacional de cultura e política nacional das artes;

II - proteção do patrimônio histórico, artístico e cultural;

III - regulação dos direitos autorais;

IV - assistência ao Ministério do Desenvolvimento Agrário e Agricultura Familiar e ao Instituto Nacional de Colonização e Reforma Agrária nas ações de regularização fundiária, para garantir a preservação da identidade cultural dos remanescentes das comunidades dos quilombos;

V - proteção e promoção da diversidade cultural;

VI - desenvolvimento econômico da cultura e a política de economia criativa;

VII - desenvolvimento e a implementação de políticas e ações de acessibilidade cultural; e

VIII - formulação e implementação de políticas, de programas e de ações para o desenvolvimento do setor museal.

2.2.2. Com a criação do Ministério da Cultura, verifica-se a necessidade de que todos os servidores e colaboradores do Ministério da Cultura, que até então, utilizavam-se da infraestrutura de tecnologia da informação do Ministério do Turismo, passem a ter uma infraestrutura própria e independente daquela ofertada e gerenciada pelo Ministério do Turismo, uma vez que tratam-se de Órgãos da Administração Pública Federal Direta distintos e que possuem características específicas onde cada um atua com foco em suas próprias políticas públicas.

2.2.3. Neste cenário em que é preciso prover os recursos de tecnologia da informação para atender as demandas do Ministério da Cultura, *en passant* pela necessidade de manter os serviços essenciais em andamento, é preciso mesclar a manutenção do uso de recursos de infraestrutura providos pelo Ministério do Turismo com a implementação e a modernização do próprio parque de tecnologia da informação do Ministério da Cultura.

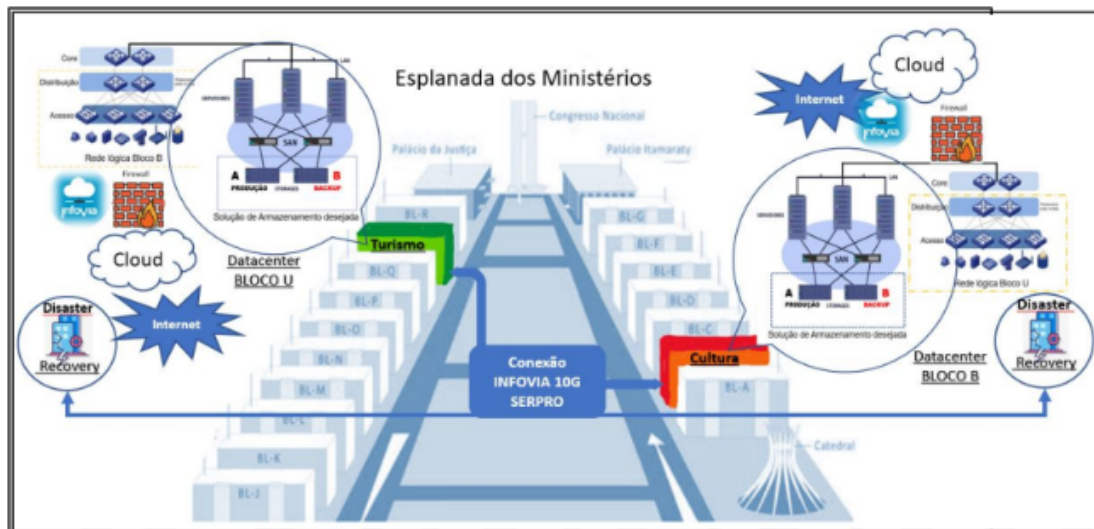
2.2.4. Assim, as ações de aquisições de equipamentos, de contratações de serviços e soluções de tecnologia da informação para atender as demandas do Ministério da Cultura precisam ser realizadas de forma gradativa e concatenada com aquelas realizadas no âmbito do Ministério do Turismo de modo a que seja possível realizar a adaptação da infraestrutura de tecnologia da informação do Edifício Sede do Ministério da Cultura (localizado no bloco B da Esplanada dos Ministérios) e dos demais anexos e unidades vinculadas à pasta, sem colocar em risco a continuidade das atividades laborais dos servidores e colaboradores do Ministério da Cultura que ainda fazem uso de equipamentos e serviços de tecnologia da informação providos pelo Ministério do Turismo.

2.3. Características do Ambiente do Datacenter

2.3.1. Após análise das condições do datacenter do Ministério da Cultura, restou verificado que a pasta possui uma sala-cofre composta por: uma célula certificada com isolamento térmico acústico, à prova de fogo, possuindo sistemas de

alerta e combate a incêndio, sistema de climatização de precisão, sistema de alta disponibilidade com redundância de energia elétrica, controle de umidade e monitoramento 24 x 7. O datacenter possui ainda contrato de manutenção preventiva e corretiva, desta forma verifica-se que o Ministério possui ambiente devidamente adequado para a utilização de soluções on-premise.

2.3.2. O datacenter do Ministério da Cultura é interligado ao datacenter do Ministério do Turismo por meio de um link INFOVIA de 10 Gigas, conforme ilustrado na figura a seguir, o que possibilita a realização de operações de transferência de backup e integrações de soluções com alta performance:



2.3.3. A característica de interligação entre os dois datacenters possibilita a implementação de serviços de forma compartilhada entre os dois ministérios, sendo possível ainda a realização do planejamento de soluções de segurança integrada, guarda de cópias de segurança em ambientes apartados daqueles em produção e implantação de soluções de *Disaster Recovery*, por exemplo.

2.3.4. Neste cenário em que já existem os ambientes físicos e as soluções de conectividade adequadas à necessidade do Ministério da Cultura e do Ministério do Turismo, verifica-se oportuno que as soluções de infraestrutura explorem os recursos e características existentes de forma a otimizar os investimentos já realizados em ambos os órgãos.

2.4. Motivação/Justificativa

2.4.1. Tendo em vista a atividade fim deste Ministério, é competência da área de Tecnologia da Informação prover a infraestrutura necessária para o bom desempenho das atividades finalísticas e administrativas, sejam elas executadas na sede em Brasília ou sejam nos diversos escritórios regionais conectados à sede.

2.4.2. Devido à recriação do MinC e à sua grande visibilidade para os cidadãos, se faz necessário que a rede de computadores deste Ministério seja composta de uma estrutura robusta e que faça o uso de recursos tecnológicos capazes de garantir sua alta disponibilidade com segurança e em alinhamento às normas e legislação pertinentes.

2.4.3. Atualmente, o MinC possui uma solução de firewall de código aberto (*open source*) chamada pfSense, para atender as necessidades institucionais de proteção na rede. Esta solução provê toda a segurança de perímetro visando interligar de forma segura a rede central do Ministério da Cultura com seus anexos.

2.4.3.1. Antes a segurança de perímetro do Ministério da Cultura era realizada com a utilização dos seguintes equipamentos da marca Palo Alto: dois appliances PA-3050 (externo) e dois appliances PA-5050 (interno). Estes equipamentos foram descontinuados, pois não possuem contrato vigente de suporte técnico com reposição de peças e componentes.

2.4.3.2. Além disso, estes equipamentos, conforme avaliação do fabricante, não possuem condições para atualização com a extensão de garantia, ou seja, por questões comerciais e técnicas estes equipamentos apresentam como encerrada a sua vida útil, *EoL (End of Life)* e *EoS (End of Support)*.

2.4.3.3. Ademais, cabe frisar que os firewalls internos operavam em alta disponibilidade, controlando todo o roteamento das redes internas e inspecionando o tráfego contra vulnerabilidades. Porém, verificou-se que os equipamentos utilizados para a segurança interna apresentavam três fontes danificadas. Portanto, apenas um firewall interno estava operacional, com somente uma fonte de alimentação.

2.4.4. Portanto, apesar do MinC possuir uma solução que não possui custo mensal para funcionamento, este firewall apresenta algumas limitações por ser *open source* baseada no sistema operacional FreeBSD e possui funcionalidades limitadas, não implementando - de forma completa - recursos como: anti-malware, anti-spyware, antivírus, antibot, filtro de conteúdo, controle de aplicações, relatórios gerados por um servidor a parte, inspeção de pacotes em tempo real, anti-DoS de rede - recursos presentes em soluções de firewall de próxima geração.

2.4.5. Cabe ressaltar que o firewall de próxima geração (Next Generation Firewall - NGFW) se refere a uma solução de segurança capaz de controlar o tráfego entre uma rede local e as conexões oriundas ou destinadas à internet e demais redes filiais ou externas à instituição, sendo composto por hardware e software que permitem a detecção e bloqueio de ataques sofisticados através das funções de firewall de rede (aplicação de políticas de acesso), IPS (Sistema de Prevenção de Intrusão com análise de tráfego) e controle de aplicações.

2.4.6. Diante disso, a aquisição de uma solução de segurança para o MinC, que contemple a implantação de firewall de próxima geração, tende a contribuir significativamente com o aumento do nível de disponibilidade dos serviços de TI, com prevenção de ataques, evitando que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers, além de bloquear “portas” que eventualmente possam ser usadas por pessoas mal-intencionadas ou bloquear acesso a programas não autorizados na rede, impedindo que usuários acessem serviços ou sistemas indevidos por meio do software de gerenciamento.

2.4.7. Portanto, esta pretensa contratação tem como objetivo melhorar o apoio tecnológico à realização da missão institucional do MinC, uma vez que deverá proporcionar a disponibilidade, confiabilidade, integridade e autenticidade dos dados e dos serviços prestados pelo Ministério e que, por sua vez, são necessários para atender com qualidade às expectativas de seus usuários.

2.4.8. Conforme os apontamentos elencados, restou verificado que há a necessidade do estudo de solução para atender a demanda de melhoria de segurança da rede, modernização e implementação de camadas de segurança à rede de computadores do MinC, proporcionando uma ferramenta capaz de auxiliar às equipes de segurança da informação quanto à necessidade de respostas rápidas aos ajustes de segurança e automação de identificação de ameaças a segurança das informações do MinC.

2.4.9. Desta forma, considerando que após a criação do Ministério da Cultura, a antiga Secretaria Especial de Cultura passou a ter uma estrutura maior contemplando mais cargos e postos de trabalho, e ainda, considerando que a segurança de perímetro é composta por equipamentos obsoletos, verifica-se que há a necessidade célere da realização de um processo de aquisição de uma solução que venha disponibilizar equipamentos em quantidade e qualidade, capazes de atender as necessidades dos servidores e colaboradores constantes na nova estrutura organizacional do Ministério da Cultura.

2.4.10. Consta ainda a necessidade de melhoria de controles para proteção da confidencialidade do tráfego de rede nesta Pasta, além da implementação de recursos de controle de acesso e recursos de segurança cibernética, conforme apontados por meio do ACÓRDÃO Nº 1318/2023 – TCU – Plenário.

3. Área requisitante

Área Requisitante	Responsável
STII	Jaime Heleno Correa de Lisboa

4. Necessidades de Negócio

4.1. Devido às características da rede de computadores já elencadas no tópico sobre a descrição da necessidade, a solução de segurança deve ser do tipo integrada em formato de appliance, ou seja, deve ser composta de hardware e software projetados e dimensionados especificamente para analisar e suportar grandes volumes de tráfegos e que permitam a implementação de diversos recursos de segurança.

4.2. Desta forma, deve ser do tipo Next Generation Firewall (Firewall de nova geração) devendo ser capaz de realizar reconhecimento de aplicações e de usuários, auxiliar na prevenção de ameaças e no controle de permissões e políticas de acesso com maior granularidade.

4.3. Tais exigências são justificáveis tendo em vista o risco da exposição indevida de informações ou de ataques que reduzam a disponibilidade de sistemas do MinC, desta forma a solução deverá permitir a verificação do comportamento do tráfego em tempo real, identificando acessos abusivos ou indevidos que podem caracterizar tentativas de invasão aos ambientes digitais do Ministério, coleta de dados ou simplesmente tentativas de derrubada dos serviços digitais.

4.4. Deverá fazer parte da composição da solução a elaboração de projeto de instalação e configuração de modo a possibilitar a análise prévia da equipe técnica do MinC quanto aos procedimentos necessários para a implementação da solução, com o planejamento de janelas de indisponibilidades e plano de comunicação de modo a dar maior transparência do processo para os usuários da rede MinC.

4.5. Todos os serviços de instalação e configuração deverão ser executados pela CONTRATADA inclusive com um período de operação assistida, de modo a não sobrecarregar a equipe de servidores e colaboradores do MinC, porém as atividades deverão ser acompanhadas pelos servidores e colaboradores que atuarão na operação da solução após entregue pela CONTRATADA.

4.6. A solução deverá ter ainda em sua composição um item para treinamento, para garantir que ocorra a transferência do conhecimento para os servidores e colaboradores que atuam na infraestrutura de TI do MinC.

4.7. Ademais, a solução contemplará módulos de segurança para as redes filiais do MinC, a citar: Centro Técnico Audiovisual - CTAv e 26 (vinte e seis) escritórios regionais..

4.8. De modo a tornar viável o investimento sem riscos da continuidade dos serviços e com garantia de atualização de softwares e componentes da solução, será exigido garantia, assistência técnica e suporte técnico por período não inferior a 60 meses, em regime 24x7.

5. Necessidades Tecnológicas

5.1. Para garantir a disponibilidade evitando-se que falhas em um equipamento cause a indisponibilidade dos serviços, a solução deverá ser baseada em hardware e software projetados especificamente para análise de tráfego de dados, composta por 2 (dois) equipamentos idênticos para prover alta disponibilidade, a serem instalados no Bloco B da Esplanada dos Ministérios.

5.2. Para garantir a rastreabilidade de acessos indevidos, a solução deverá possuir recurso para armazenamento de eventos relacionados ao tráfego de dados para registro e análise.

5.3. De modo a garantir que a solução esteja sempre atualizada quanto ao surgimento de novos recursos maliciosos, a solução deverá dispor de biblioteca de assinatura de código malicioso atualizável.

5.4. Para garantir a análise aprofundada e redução de riscos de acessos a sites e serviços comumente utilizados por hackers e que portanto representam ameaças ou que prejudicam o uso otimizado dos recursos de acesso à internet, a solução deverá ser capaz de implementar filtragem de pacotes, controle de aplicações, administração de largura de banda, prevenção contra intrusão, rede virtual privada segura, prevenção contra código malicioso, filtro de endereços e controle de acesso à internet.

5.5. Possuir ambiente controlado para análise e acesso de endereços e execução de arquivos suspeitos.

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

6.1. Requisitos de Continuidade do Negócio

6.1.1. Caso seja efetuada a opção pela compra de solução, deverá ser exigido a garantia, assistência e suporte técnico executados pelo fabricante da solução pelo prazo de 60 meses para os equipamentos (manutenção corretiva de hardware e software, em regime 24x7), de modo a que se garanta que os serviços funcionem sem períodos de interrupções que possam comprometer a disponibilidade dos serviços durante a vida útil do equipamento sem acrescentar custos adicionais ao MinC.

6.1.2. Para possibilitar o controle de suporte e manutenção, deverá ser previsto que a execução dos serviços seja através da abertura de chamados técnicos com prazos de atendimento e solução em conformidade com os níveis de serviços requeridos pelo MinC.

6.1.3. Para garantir a transferência do conhecimento, deverá ser exigido junto à contratação a realização de treinamento na solução abrangendo instalação, configuração, gerenciamento e operação, que deverá ser ministrado por profissional qualificado pela fabricante.

6.2. Requisitos de sustentabilidade da solução de TIC

6.2.1. Em atenção aos critérios de sustentabilidade, sobretudo como forma de observância à Lei n. 12.305, de 2 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos e o Decreto n. 7.746, de 5 de junho de 2012, que estabelece critérios e práticas para a promoção do desenvolvimento nacional sustentável nas contratações realizadas pela administração pública, procurou-se incluir requisitos mínimos nas especificações dos equipamentos que buscam garantir a observância da responsabilidade ambiental no âmbito da presente contratação.

6.3. Requisitos Legais

6.3.1. O presente processo de contratação deve estar aderente à Constituição Federal, ao Decreto-Lei nº 200/1967, à Lei nº 14.133/2021 (Lei de Licitações), à IN SGD/ME nº 94/2022 (Contratação de Soluções de TIC) e a outras legislações aplicáveis.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. Sede do MinC - Bloco B da Esplanada dos Ministérios

7.1.1. Para atender a demanda do edifício sede, a solução deverá ser fornecida em um cluster do tipo ativo-ativo, ou seja, todos os nós que compõem o cluster de alta disponibilidade respondem às requisições, e além de garantir a continuidade do ambiente, em caso de queda de algum dispositivo, eles distribuem a carga de processamento.

7.1.2. Para a composição da solução de segurança (NGFW), conforme apontamentos constantes deste ETP, deverão ser garantidos os seguintes itens:

7.1.2.1. Equipamentos Firewall (cluster);

7.1.2.1. Equipamentos Firewall para as filiais do MinC;

7.1.2.2. Serviços de Instalação para a implantação no Datacenter do MinC e no CTAy;

7.1.2.3. Serviços de Treinamento para os servidores e colaboradores da CGINF;

7.1.3. A solução a ser fornecida deverá estar totalmente licenciada para as funcionalidades mínimas listadas a seguir:

- a) Controle por política de Firewall;
- b) Controle de Aplicações;
- c) Prevenção de Ameaças;
- d) Filtro de URL;
- e) Prevenção de ameaças avançadas (zero day);
- f) Identificação de Usuários;
- g) QoS;
- h) VPN site-to-site (IPsec);
- i) VPN client-to-site;
- j) SD-WAN.

7.2. Centro Técnico Audiovisual - CTAy

7.2.1. Este Centro, localizado na cidade do Rio de Janeiro - RJ, possui um acervo iconográfico contendo expressiva quantidade de itens sobre o cinema nacional, uma biblioteca que possui dentre outras, uma rica coleção de catálogos de eventos e periódicos da área, uma videoteca com sua coleção de filmes e eventos, devendo assim ter seus registros descritos e disponibilizados ao público interno e externo, por meio de uma base de dados já consolidada e que abrigará itens digitais ou digitalizados, tais como fotografias, cartazes, capas de catálogos, dentre outros.

7.2.2. Para atender a esta demanda, a solução deverá ser fornecida em um equipamento com fontes redundantes, de modo a garantir a continuidade do funcionamento do equipamento mesmo quando ocorrer dano a uma das fontes, até que o mecanismo seja reparado ou substituído sem a necessidade do desligamento do equipamento.

7.2.3. Para esta localidade se faz necessário um equipamento Firewall de médio porte, que tenha capacidade para atender aproximadamente 200 servidores/colaboradores, que será implementado garantindo total compatibilidade e integração com o Firewall e o Módulo de Gerência, presentes na Sede do MinC.

7.2.4. Desta forma, será implementado o gerenciamento centralizado, simplificando o monitoramento das políticas de segurança; e uma garantia de rastreabilidade de eventos que possam ter comprometido a segurança dos dados pessoais tratados no âmbito do MinC.

7.2.5. A solução a ser fornecida deverá estar totalmente licenciada para as funcionalidades mínimas listadas a seguir:

- a) Controle por política de Firewall;
- b) Controle de Aplicações;
- c) Prevenção de Ameaças;
- d) Filtro de URL;
- e) Prevenção de ameaças avançadas (zero day);
- f) Identificação de Usuários;
- g) QoS;
- h) VPN site-to-site (IPsec);
- i) VPN client-to-site;
- j) SD-WAN

7.3. Escritórios Regionais

7.3.1. Há a expectativa da criação de 26 (vinte e seis) escritórios regionais em cada estado brasileiro. Portanto, se faz necessário estimar equipamentos Firewall de pequeno porte, que atendam uma demanda de aproximadamente 20 usuários entre servidores e colaboradores, nestas localidades.

7.3.2. Assim como previsto no item anterior, teremos um gerenciamento centralizado, simplificando o monitoramento das políticas de segurança; e uma garantia de rastreabilidade de eventos que possam ter comprometido a segurança dos dados pessoais tratados no âmbito do MinC.

7.4. Desta forma, elencada a metodologia adotada, restaram estimados os itens e quantitativos que deverão compor o registro de preços conforme quadro ilustrado a seguir:

LOTE /GRUPO	ITEM	DESCRIÇÃO	UNIDADE	CATMAT/CATSER	QUANTIDADE
1	1	Módulo de Segurança (cluster) - tipo I	Un.	484747	1
	2	Módulo de Segurança - tipo II	Un.	484747	1
	3	Módulo de Segurança - tipo III	Un.	484747	26
	4	Sistema de gerência centralizada com armazenamento de logs	Un.	27472	1
	5	Serviço de instalação e configuração para a solução	Un.	26972	2

	6	Treinamento “hands on” sobre solução de firewall	Un.	20052	2
--	---	--	-----	-------	---

8. Levantamento de soluções

8.1. Opção 01 - Contratação de extensão de garantia com expansão da capacidade da segurança de perímetro

8.1.1. Trata-se da contratação de serviços de extensão da garantia de suporte técnico com fornecimento de peças e componentes, para equipamentos já em uso no datacenter do CONTRATANTE.

8.1.2. Neste tipo de contratação verifica-se a vantagem de que, em muitos casos, não há a necessidade do desligamento ou de interrupção dos serviços por muito tempo para a realização de atualizações de softwares e até para a troca de alguns componentes.

8.1.3. Como desvantagem verifica-se que, embora ocorra a troca de alguns componentes, a continuidade de utilização do hardware principal não garante a compatibilidade com os novos recursos e também não garante o aumento da vida útil do equipamento.

8.2. Opção 02 - Contratação de Softwares Livres Gratuitos

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

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

8.3. Opção 03 - Locação de equipamento de segurança de perímetro

8.3.1. Neste tipo de contratação, a CONTRATADA aluga os equipamentos para uso do CONTRATANTE por tempo determinado, arcando com as despesas de suporte e manutenção, instalação e etc.

8.3.2. Verifica-se o fator positivo de que não há a necessidade da realização de aquisições de equipamentos por parte da administração cabendo à CONTRATADA a obrigação de entregar sempre o equipamento em condições de utilização, devendo substituir o equipamento sempre que necessário, garantidos os critérios de atualização e demais exigências que couberem.

8.3.3. O principal ponto negativo observado é o fato de que há a necessidade de intervenções da CONTRATADA nos ambientes mantidos pelo CONTRATANTE, além da necessidade de adaptação dos equipamentos alugados ao parque próprio, tendo o risco de ter que realizar a troca dos equipamentos de forma não planejada caso ocorra algum problema com o fornecedor durante a vigência do contrato.

8.4. Opção 04 - Aquisição de solução de proteção de rede Next Generation Firewall (NGFW) de maior capacidade, com suporte e garantia

8.4.1. Trata-se da realização de substituição da solução de segurança de perímetro por meio da aquisição de um equipamento novo com garantia de suporte técnico e com fornecimento de peças e componentes.

8.4.2. A opção tem como ponto positivo o fato de que o equipamento adquirido, mesmo após o período de garantia continua disponível para uso do órgão, podendo ainda ocorrer, desde que comprovada a viabilidade técnica e econômica, a contratação de extensão de garantia, o que garante ao Ministério maior controle sobre os recursos quando comparado às soluções de locação e hospedagem em nuvem.

8.4.3. Como ponto negativo em comparação às soluções de locação e hospedagem é a necessidade de investimento inicial maior, e a necessidade de disponibilização de ambiente adaptado para a instalação do equipamento, quando o CONTRATANTE não possui datacenter próprio.

9. Análise comparativa de soluções

9.1. Existem hoje no mercado a possibilidade de contratação de serviços de extensão de garantia do equipamento existente, contratação de software livre, locação de equipamentos de TI e aquisição de solução *on-premise*.

- **Solução 1** - Modernização e contratação de extensão de garantia para o Equipamento existente;
- **Solução 2** - Contratação de Software Livre e Gratuito;
- **Solução 3** - Locação de equipamento; e
- **Solução 4** - Aquisição de solução de segurança de perímetro *on-premise*.

9.2. Examina-se nesta seção, para cada solução, os aspectos previstos na IN SGD/ME nº 94/2022 que devem ser avaliados em uma contratação de TIC:

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
	Solução 4	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2	X		
	Solução 3		X	
	Solução 4		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
	Solução 4	X		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			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 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X

10. Registro de soluções consideradas inviáveis

10.1. As soluções consideradas inviáveis neste estudo são aqueles consideradas antieconômicas do ponto de vista técnico.

10.2. **Opção 01 - Contratação de extensão de garantia com expansão da capacidade da segurança de perímetro:** foi realizada consulta junto ao fornecedor para análise de viabilidade comercial e técnica para a expansão da capacidade do equipamento atualmente em produção com a contratação de suporte técnico com reposição de peças e componentes. Após a análise do fabricante, restou verificado como encerrada a sua vida útil, *EoL (End of Life)* e *EoS (End of Support)*. Portanto, o equipamento não dispõe de peças de reposição no mercado, desta forma não existe viabilidade comercial para a contratação de extensão de garantia com suporte técnico e reposição de peças e componentes.

10.3. Opção 02 - Contratação de Softwares Livres Gratuitos: evidencia-se que essa solução não tem custos com a aquisição do software, mas possui custos indiretos de configuração e de gestão difíceis de mensurar. Deste modo, a solução apresenta aumento significativo no volume de gestão, passíveis de criar alto impacto ao negócio por gestão ineficiente e/ou ineficaz.

10.4. Opção 03 - Locação de equipamento de segurança de perímetro: é inviável pelo fato que as empresas que realizam esse tipo de comercialização praticamente parcelam o custo do equipamento e de sua manutenção ao longo do período de aluguel e seria necessário que a operação realmente fosse vantajosa para o órgão, o que ainda não foi possível constatar em outros órgãos da Administração Pública. A prática de locação de equipamentos de TI é vista com extrema restrição pelo Tribunal de Contas da União, exceto para períodos de uso curto e específico, conforme posicionamento da Corte, expresso no AC-3091- 45/14- Plenário:

"Foram encontrados apenas dois artigos publicados em revistas especializadas, dos quais se destacam os seguintes trechos:

(...) alugar vale a pena quando é preciso cumprir projetos de curto prazo, em situações de sobrecarga de trabalho, para viagens de funcionários ou quando a empresa participa de convenções e exposições. As situações mostram que o aluguel está diretamente relacionado a negócios de curto período de duração. (BALIEIRO, Silvia. Quando alugar vale a pena. Revista Info Exame, v. 14, n. 160, p. 118-119, jul. 1999)

Locação de equipamentos conquista empresas que precisam de produtos como PCs, projetores ou filmadoras por períodos específicos. (SOSNOWSKI, Alice. Computador de aluguel. Revista PC World, n. 169, p. 18-20, ago 2006).

De tais excertos, depreende-se que a locação de equipamentos de informática é apropriada para períodos específicos, geralmente curtos. No caso de microcomputadores isto se deve ao fato de que a vida útil de tais equipamentos é de, no mínimo, três anos.

Destarte, verifica-se que a jurisprudência do TCU é firme no sentido de que a locação de equipamentos de informática é medida excepcionalíssima, devendo restar inequivocamente demonstrada nos autos a vantajosidade da opção pela locação em detrimento da aquisição, quando for adotada tal solução." (g.n.)

11. Análise comparativa de custos (TCO)

11.1. Das quatro soluções apresentadas, a **Solução 4 - Aquisição de solução de proteção de rede Next Generation Firewall (NGFW) de maior capacidade, com suporte e garantia** - foi considerada a melhor alternativa dentre as opções elencadas. Esta solução trata-se da aquisição dos equipamentos por meio de recursos orçamentários de investimentos com suporte e garantia mínima de 60 (sessenta) meses.

11.2. O levantamento dos valores para a aquisição de bens e contratação de serviços em geral para os órgãos e entidades participantes do SISG - Sistema de Serviços Gerais, deve seguir os procedimentos administrativos definidos pela Instrução Normativa nº 65/2021 da Secretaria de Gestão (SEGES) do Ministério da Economia. Este levantamento servirá para balizar a viabilidade financeira do projeto.

11.3. Em atendimento ao art. 5º da Instrução Normativa nº 65, de 07 de Julho de 2021:

"Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:

I - 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 em saúde, observado o índice de atualização de preços correspondente;

II - 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;

III - 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;

IV - 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

V - 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.

§ 1º Deverão ser priorizados os parâmetros estabelecidos nos incisos I e II, devendo, em caso de impossibilidade, apresentar justificativa nos autos."

11.4. Conforme orienta a referida Instrução Normativa, foi realizada pesquisa no Pannel de Preços (disponível em <https://paineldeprescos.planejamento.gov.br/>) no dia 03 de abril de 2023 e verificou-se que há vários órgãos/entidades que adquiriram bem similar ao objeto deste estudo. Para isso, utilizou-se os seguintes filtros:

- Ano da compra: **2022 e 2023;**
- Código Material/Serviço: **484747;**
- Modalidade de Compra: **Pregão.**

11.5. Com essa busca foram retornados 24 pregões, conforme o filtro aplicado, demonstrados no ANEXO I deste ETP. É importante ressaltar que há no mercado diversos modelos de soluções de firewall, resultando em uma quantidade de possíveis combinações e características relativamente amplas (capacidade de throughput, quantidade de sessões novas simultâneas, quantidade de interfaces, etc.). Além das possíveis combinações e características de hardware, existem ainda diferentes tipos de licenciamento (período de suporte e garantia, filtro de URL, prevenção a ameaças conhecidas ou desconhecidas, antivírus, segurança para DNS, etc.). Portanto, entre os processos de compras listados em nossa filtragem, apenas 5 apresentaram compatibilidade aos requisitos buscados neste processo de contratação, conforme demonstrado a seguir:

ID	Identificação da Compra	Fornecedor	Órgão	Data da Compra
1	108/2022	GLOBAL SEC. TECNOLOGIA & INFORMACAO LTDA	DEFENSORIA PUBLICA DA UNIAO	13/12/2022
2	59/2022	TELTEC SOLUTIONS LTDA	UNIVERSIDADE FEDERAL DA FRONTEIRA SUL	02/12/2022
3	81/2022	TLD TELEDATA COMERCIO E SERVICOS LTDA	TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS	09/09/2022
4	19/2022	APPROACH TECNOLOGIA LTDA	TRIBUNAL DE CONTAS DO ESTADO DO PIAUÍ	07/12/2022
5	12/2022	NCT INFORMATICA LTDA	MINISTERIO DAS COMUNICACOES	20/09/2022

- A Defensoria Pública da União (DPU) - UASG: 290002 realizou o Pregão 108/2022 para a contratação de empresa especializada no fornecimento de ativos de segurança de rede do tipo Next Generation Firewall (NGFW), com SD-WAN integrada, instalação, treinamento e suporte técnico, para a Defensoria Pública da União em âmbito nacional, com garantia de 36 (trinta e seis meses). Os itens que atendem ao escopo do MinC são:

- Item 1 - Firewall tipo I com SD-WAN. Quantidade: 2;
- Item 4 - Sistema de Gerência Centralizada. Quantidade: 1;
- Item 5 - Serviço de Instalação e Configuração. Quantidade: 2;
- Item 6 - Treinamento "hands on" sobre a solução de Firewall. Quantidade: 1.

- A Universidade Federal da Fronteira Sul (UFFS) - UASG: 158517 realizou o Pregão 59/2022 para a solução de tecnologia da informação e comunicação de aquisição de licenciamento, garantias e suporte de firewall para atender as necessidades da Universidade Federal da Fronteira Sul, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos, com garantia de 36 (trinta e seis meses). Os itens que atendem ao escopo do MinC são:

- Item 1 - Firewall PA-3410 para Data Center. Quantidade: 2;
- Item 3 - Projeto de Instalação, Migração e Configuração do Firewall PA-3410. Quantidade: 1.

- O Tribunal Regional Eleitoral de Alagoas (TRE-AL) - UASG: 70011 realizou o Pregão 81/2022 para o registro de preço para eventual aquisição de solução Firewall para o Prédio Sede do TRE/AL, cartórios Eleitorais, unidades e escritórios remotos da Justiça Eleitoral em Alagoas, com garantia de 36 (trinta e seis meses). Os itens que atendem ao escopo do MinC são:

- Item 1 - Solução de Segurança e Gerência de Redes NGFW Tipo 1 (CLUSTER). Quantidade: 1;
- Item 9 - Unidade Centralizada de Armazenamento de Logs e Relatoria. Quantidade: 1;
- Item 10 - Unidade de Gerência Centralizada de Equipamentos. Quantidade: 1;
- Item 11 - Serviços Profissionais de Implantação e Configuração para Solução De Segurança e Gerência De Redes NGFW Tipo 1. Quantidade: 1;
- Item 16 - Treinamento Oficial do Fabricante para Solução de Segurança e Gerência de Redes NGFW. Quantidade: 1;
- Item 17 - Treinamento Oficial do Fabricante para Unidade de Gerência Centralizada de Equipamentos. Quantidade: 1;
- Item 18 - Treinamento Oficial do Fabricante para Unidade Centralizada de Armazenamento de Logs e Relatoria. Quantidade: 1;

- O Tribunal de Contas do Estado do Piauí (TCE-PI) - UASG: 925466 realizou o Pregão 19/2022 para a aquisição de solução de segurança em redes de computadores, com alta disponibilidade HA (High-Availability) do tipo Firewall NGFW - Appliance (NextGeneration Firewall) da marca Palo Alto, modelo PA-3410 ou superior. Faz parte da solução a instalação, configuração e testes, além da garantia, subscrições "Threat Prevention", "Advanced URL Filtering", "GlobalProtect", "Virtual System" e suporte técnico pelo período de 60 (sessenta) meses, de acordo com as condições estabelecidas e demais características detalhadas neste termo de referência. Os itens que atendem ao escopo do MinC são:

- Item 1 - Firewall do tipo Next Generation, incluindo instalação, configuração, subscrições e suporte técnico. Quantidade: 2.
- **Obs:** este item já contempla o serviço de instalação e configuração, além do repasse de conhecimento. (g.n.)

- O Ministério das Comunicações (MCOM) - UASG: 410003 realizou o Pregão 12/2022 para a contratação de solução de proteção de rede Next Generation Firewall (NGFW), em cluster, contemplando o hardware, software de gerenciamento, licenciamento, implantação, configuração e treinamento, incluindo, garantia, atualizações e suporte técnico, por 60 (sessenta) meses, para atender às necessidades do Ministério das Comunicações - MCOM, conforme quantidades e exigências estabelecidas neste instrumento. Os itens que atendem ao escopo do MinC são:

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

11.6. Conforme o art. 6º da Instrução Normativa nº 65, de 07 de Julho de 2021: "*Serão utilizados, como métodos para obtenção do preço estimado, a média, a mediana ou o menor dos valores obtidos na pesquisa de preços, desde que o cálculo incida sobre um conjunto de três ou mais preços, oriundos de um ou mais dos parâmetros de que trata o art. 5º, desconsiderados os valores inexequíveis, inconsistentes e os excessivamente elevados*".

11.6.1. Visto isso, o Pregão 12/2022 do MCOM será desconsiderado da pesquisa de preços, pois, por se tratar de uma solução de subscrição, o valor da solução será pago de forma anual (R\$ 1.260.000,00). Como o objeto desta contratação possuirá suporte e garantia de 5 anos, ao final deste período o MinC deverá desembolsar R\$ 6.300.000,00 comparado aos outros pregões que se referem à aquisição de appliances.

11.7. Além disso, foram analisados projetos similares, identificados no Portal de Compras do Governo Federal (www.gov.br/compras), para subsidiar esta pesquisa de preços, conforme demonstrado a seguir:

- A SUPERINTENDÊNCIA DA ZONA FRANCA DE MANAUS – SUFRAMA - UASG: 193028 realizou o Pregão 1/2023 para a aquisição de solução de segurança do tipo firewall NGFW (next generation firewall) incluindo todos os softwares, licenças de uso, garantia de atualização contínua, suporte técnico durante o período de garantia e serviços de instalação com repasse de conhecimento da solução, conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos. Os itens que atendem ao escopo do MinC são:

- Item 1 - Solução de Segurança - Tipo 01. Quantidade: 1;
- Item 5 - Solução de Segurança - Tipo 02. Quantidade: 26.

- O Tribunal Regional Eleitoral de Pernambuco – TRE-PE - UASG: 70010 realizou o Pregão 73/2022 para a aquisição de firewall com software de análise de logs, conexão 2FA para VPN e suporte/garantia de 60 meses, de acordo com as especificações constantes do Termo de Referência (ANEXO I) do Edital. Os itens que atendem ao escopo do MinC são:

- Item 9 - FIREWALL DE NÚCLEO TIPO III. Quantidade: 2.

- O Ministério da Defesa – MD - UASG: 110404 realizou o Pregão 26/2022 para aquisição de soluções de segurança de TI. Os itens que atendem ao escopo do MinC são:

- Item 7 - Equipamento de segurança de rede do tipo Firewall com licenciamento e garantia de 36 (trinta e seis) meses (Tipo I). Quantidade: 4.

11.8. Desta forma, visando evitar valores inexequíveis, inconsistentes e os excessivamente elevados, será utilizado como preço estimado a média dos pregões similares, exceto para o item 1, conforme demonstrado a seguir:

ITEM	DESCRIÇÃO	QTD.	Pregão 108 /2022 (DPU)	Pregão 59 /2022 (UFFS)	Pregão 81 /2022 (TRE-AL)	Pregão 230 /2022 (TCE-PI)	Pregão 73 /2022 (TRE-PE)	Pregão 1 /2023 (SUFRAMA)
1	Módulo de Segurança (CLUSTER) - tipo I	1	3.220.000,00	2.334.710,00	1.978.259,17	2.099.000,00	1.292.915,20	-
2	Módulo de Segurança - tipo II	1	-	-	-	-		278.471,00
3	Módulo de Segurança - tipo III	26	-	-	-	-		34.575,00
4	Sistema de gerência centralizada com armazenamento de logs	1	179.500,00	-	188.951,90	-		-
5	Serviço de instalação e configuração para a solução	2	39.000,00	33.195,00	95.000,00	-		-
6	Treinamento “hands on” sobre solução de firewall	1	72.000,00	-	36.600,00	-		-

Obs1: Os valores unitários do item 1 dos pregões da DPU, UFFS e TRE-AL foram ajustados para que se adequem ao prazo de 60 (sessenta) meses de garantia, atualizações e suporte técnico, de acordo com a necessidade do objeto do MinC.

11.9. Com relação ao item 1 - Módulo de Segurança (CLUSTER) - tipo I e diante da composição dos levantamentos de pregões similares feito pela equipe de planejamento da contratação, combinada com os pregões citados pelo TCU, foi possível chegar a um universo de 06 (seis) licitações, compostas de valores finais de pregões, conforme memória de cálculo, ANEXO II deste ETP.

11.10. Portanto, diante do cenário das discrepâncias entre o valor mais baixo e o valor mais alto, no intuito de que o valor estimado esteja o mais próximo do valor praticado no mercado, foi adotada a Mediana para a composição de preços do item 1, gerando o quadro a seguir:

ITEM	DESCRIÇÃO	QUANTIDADE	UNIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Módulo de Segurança (CLUSTER) - tipo I	1	Un.	R\$ 2.038.629,58	R\$ 2.038.629,58
2	Módulo de Segurança - tipo II	1	Un.	R\$ 278.471,00	R\$ 278.471,00
3	Módulo de Segurança - tipo III	26	Un.	R\$ 34.575,00	R\$ 898.950,00
4	Sistema de gerência centralizada com armazenamento de logs	1	Un.	R\$ 184.225,95	R\$ 184.225,95
5	Serviço de instalação e configuração para a solução	2	Un.	R\$ 55.731,67	R\$ 111.463,33
6	Treinamento “hands on” sobre solução de firewall	2	Un.	R\$ 54.300,00	R\$ 108.600,00

VALOR GLOBAL

R\$ 3.620.339,86

11.11. Com base na consolidação dos preços pesquisados, o valor estimado para contratação é de **R\$ 3.620.339,86 (três milhões, seiscentos e vinte mil, trezentos e trinta e nove reais e oitenta e seis centavos).**

12. Descrição da solução de TIC a ser contratada

12.1. A contratação do objeto dar-se-á por meio de Pregão Eletrônico para Registro de Preços do tipo Menor Preço por grupo. Os itens do objeto deverão ser licitados e adjudicados por grupo considerando a indivisibilidade dos mesmos, pois as soluções e os serviços são de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia.

12.1.1. A aquisição do objeto da licitação em apenas um lote garante a unicidade técnica dos processos, assim como o nível de serviços prestados, permitindo que a empresa contratada esteja capacitada tecnicamente para trabalhar de forma integrada com os componentes desta solução.

12.1.2. Outro fator importante a ser levado em consideração: a otimização dos recursos necessários à gerência de um único contrato e o foco na melhoria do processo, visto que a STII possui uma equipe de servidores públicos reduzida, além de ser responsável pela gestão de outros contratos de TI.

12.2. Portanto, diante das análises qualitativa e quantitativa realizadas ao longo do presente estudo técnico preliminar, constata-se que, para fins de um processo de contratação de uma solução de perímetro, o objeto mais adequado é a aquisição de uma solução de proteção de rede Next Generation Firewall (NGFW) com garantia e suporte.

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

LOTE /GRUPO	ITEM	DESCRIÇÃO	UNIDADE	CATMAT /CATSER	QUANTIDADE
1	1	Módulo de Segurança (CLUSTER) - tipo I	Un.	484747	1
	2	Módulo de Segurança - tipo II	Un.	484747	1
	3	Módulo de Segurança - tipo III	Un.	484747	26
	4	Sistema de gerência centralizada com armazenamento de logs	Un.	27472	1
	5	Serviço de instalação e configuração para a solução	Un.	26972	2
	6	Treinamento "hands on" sobre solução de firewall	Un.	20052	2

12.3. O item 1 refere-se ao cluster de Firewall com suporte, garantia e licenças de proteção com vigência de 60 meses. Esta solução deve funcionar em cluster do tipo ativo-ativo com balanceamento interno.

12.4. Os itens 2 e 3 referem-se ao módulo de segurança a serem instalados nos anexos do MinC tendo garantia de atualização de licenças e suporte técnico pelo período mínimo de 60 (sessenta) meses. Estes módulos serão implementados em redes internas com até 200 usuários (tipo II) e com até 30 usuários (tipo III).

12.5. O item 04 refere-se ao sistema de gerência centralizada visando gerenciar os acessos à internet dos anexos do MinC (CTaV e Escritórios Regionais), de forma a armazenar os logs de acesso para futuras auditorias e apuração de responsabilidade quando necessário. A utilização de um software de gerenciamento centralizado facilita as tarefas de gestão de regras e políticas em um firewall. Por meio desse gerenciamento centralizado é possível gerenciar diversos appliances por meio de uma única interface. Além disso, é possível acessar registros (logs) de diversos equipamentos.

12.6. O item 05 refere-se ao serviço de instalação da solução considerando a instalação em duas localidades distintas, a citar: Sede do MinC (Bloco B da Esplanada dos Ministérios) - item 01 e CTaV (Avenida Brasil na cidade do Rio de Janeiro - RJ) - item 02. Para realizar estas instalações devem ser realizadas reuniões para planejar e definir datas e eventuais necessidades, como por exemplo: avaliação e/ou manutenção do datacenter e também, análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados. Com relação ao serviço de instalação e configuração dos itens 3, estes módulos de segurança deverão ser entregues e instalados pela CONTRATADA.

12.7. O item 06 refere-se ao treinamento específico da solução, com carga horária mínima de 20 horas, para o gerenciamento da aplicação do Firewall, conduzido pelo próprio fabricante ou por um parceiro certificado e autorizado pelo fabricante ministrar

treinamentos oficiais. O quantitativo registrado em Ata de 2 (dois) eventos se deve ao fato de prever o serviço de treinamento conjunto para a equipe de infraestrutura do MinC com até 5 pessoas, sendo um evento no primeiro ano e outra a ser agendando no segundo ano como repasse de conhecimento para novas equipes.

12.8. Os bens objeto desta contratação são caracterizados como comuns, uma vez que tratam-se de equipamentos e serviços disponíveis em grande escala no mercado, e cujas características e condições de fornecimento são práticas comuns e podem ser fornecidas por diferentes fabricantes e fornecedores no mercado nacional.

12.9. Os requisitos mínimos e demais detalhes técnicos da solução de TIC constam no caderno de especificações técnicas (ANEXO III), conforme a Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

13. Estimativa de custo total da contratação

Valor (R\$): 3.620.339,86

ITEM	DESCRIÇÃO	QUANTIDADE	UNIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Módulo de Segurança (CLUSTER) - tipo I	1	Un.	R\$ 2.038.629,58	R\$ 2.038.629,58
2	Módulo de Segurança - tipo II	1	Un.	R\$ 278.471,00	R\$ 278.471,00
3	Módulo de Segurança - tipo III	26	Un.	R\$ 34.575,00	R\$ 898.950,00
4	Sistema de gerência centralizada com armazenamento de logs	1	Un.	R\$ 184.225,95	R\$ 184.225,95
5	Serviço de instalação e configuração para a solução	2	Un.	R\$ 55.731,67	R\$ 111.463,33
6	Treinamento "hands on" sobre solução de firewall	2	Un.	R\$ 54.300,00	R\$ 108.600,00
VALOR GLOBAL					R\$ 3.620.339,86

14. Justificativa técnica da escolha da solução

14.1. A aquisição de uma solução de segurança de perímetro visa assegurar a continuidade, integridade e disponibilidade dos serviços do MinC. A qualidade e o acesso e/ou disponibilidade dos serviços e das aplicações do MinC serão significativamente comprometidas caso não haja a renovação dos equipamentos de informática para este ministério.

14.2. Ademais, algumas justificativas técnicas para a contratação desta solução são:

14.2.1. Facilitar e agilizar a implantação de VPN segura, sem necessidade de configuração nas unidades remotas, garantindo a continuidade da conexão da VPN entre as Unidades do MinC e a Sede em casos de falhas em um dos links de dados, assegurando também o acesso à Internet;

14.2.2. Dar maior eficiência na execução dos processos que dependem do ambiente computacional, com a introdução de equipamentos de melhor rendimento;

14.2.3. Atender à crescente dependência dos recursos de tecnologia da informação, que fazem com que a infraestrutura de rede deva apresentar cada vez maior confiabilidade, resiliência, disponibilidade, segurança, capacidade de resolução de problemas de maneira proativa e rápida e melhorar a experiência para todos os usuários da rede do MinC;

14.2.4. Permitir gestão centralizada de todos os dispositivos de segurança e borda da rede das unidades remotas, otimizando o monitoramento do uso da rede local nas Unidades fora da Sede, agilizando a recuperação de desastres (*disaster recovery*).

15. Justificativa econômica da escolha da solução

15.1. Conforme demonstrado no item 11 - Análise comparativa de custos (TCO), após a realização da pesquisa de mercado, apurou-se a média e a mediana dos preços dos últimos pregões realizados de soluções para objetos similares e verificou-se que o valor está em conformidade com os preços praticados no mercado.

15.2. Ademais, o prazo de garantia de 60 (sessenta) meses para a solução proporcionará maior vantajosidade econômica ao MinC, pois eliminará o custo administrativo da realização de novas licitações anuais, permitindo que a equipe de tecnologia da informação foque sua atuação na aplicação de métodos e procedimentos que agreguem valor tecnológico aos usuários dos serviços de tecnologia do Ministério.

15.2.1. O período de 60 (sessenta) meses para a solução de Firewall se justifica com base nas recomendações presentes no guia de BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC - Versão 4 (https://www.gov.br/governodigital/pt-br/contratacoes/orientacoes_ativos-de-tic-v-4.pdf) publicada em 23/03/2017 e detalhada a seguir:

"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." (g.n.)

15.3. Conforme dispõe o Inciso I, § 2º, art. 12, da IN SGD/ME nº 94/2022, restou verificado que não é viável particionar o objeto da contratação, uma vez que colocaria em risco o objetivo final desejado. Este não parcelamento da solução gera uma viabilidade econômica trazendo benefícios para a Administração licitante, pois proporciona um aumento da competitividade e uma consequente diminuição dos custos para a execução do objeto.

15.4. No entanto, para uma real noção da viabilidade econômica do parcelamento, é preciso ter em mente a redução de custos proporcionada pela economia de escala. Neste sentido, o grupo único é mais satisfatório do ponto de vista da eficiência técnica também, por manter a qualidade da solução de TI, haja vista que o gerenciamento permanece todo o tempo a cargo de um mesmo administrador. Nesse ponto, as vantagens seriam o maior nível de controle pela Administração na execução dos serviços, a maior interação entre as diferentes fases da implantação/implementação, a maior facilidade no cumprimento do cronograma preestabelecido e na observância dos prazos, concentração da responsabilidade pela execução em uma só pessoa e concentração da garantia dos resultados.

15.5. Dessa forma, por suas especificidades, esta contratação ao estar alinhada às práticas de mercado, deverá ter a sua adjudicação da licitação pelo menor preço global. Ademais, o não parcelamento do objeto não restringe a competitividade do certame e nem traz prejuízo ao erário, visto que os itens que compõem o objeto são de mesma natureza e guardam relação entre si.

16. Benefícios a serem alcançados com a contratação

16.1. Os resultados a serem alcançados constam no Documento de Formalização de Demanda (DFD) e estão a seguir relacionados:

- Contribuir para a garantia de um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;
- Aprimorar a segurança de TIC do MinC frente a ameaças sofisticadas;
- Possibilitar o controle de acesso e complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;
- Possibilitar o acesso remoto de maneira estável aos colaboradores de forma segura;
- Prestar os serviços de TIC mantendo a segurança adequada às informações organizacionais, principalmente quanto à garantia de disponibilidade e integridade dos dados necessários ao pleno funcionamento dos processos administrativos.
- Assegurar a sustentabilidade e o desempenho dos serviços deste Ministério, conforme sua nova topologia e tráfego de rede;
- Aumento da capacidade de resposta incidentes de segurança;
- Propiciar um ambiente seguro nos acessos aos recursos de TIC;

- Aprimorar a segurança, proteção e autenticidade dos dados sensíveis da organização, controlando de forma proativa as vulnerabilidades em recursos de TIC; e
- Modernizar a infraestrutura da rede, com a aquisição de solução do tipo firewall de próxima geração, ampliando o nível de segurança para garantir maior eficiência frente as frequentes tentativas de ataques cibernéticos.

17. Providências a serem Adotadas

17.1. A solução de um cluster de Firewall NGFW a ser adquirida para a Sede do MinC deverá ser dimensionada de forma compatível com a sala-cofre do Bloco B da Esplanada dos Ministérios, de forma a possibilitar a sua conexão com os demais ativos de rede existentes.

17.2. Além disso, para a implantação da solução constante destes estudos nos anexos do MinC, a citar: CTaV e Escritórios Regionais, será necessário a contratação de serviços de acesso à internet, preferencialmente do tipo IP Dedicado. Para tanto, as especificações técnicas deste serviço a ser contratado por estas localidades com apoio das áreas de licitações deste Ministério, serão fornecidas pela STII em processo vinculado ao processo que originou estes estudos.

17.3. Além disso deverá ser encaminhado aos responsáveis destes anexos um documento com as orientações gerais quanto:

- a) as providências necessárias para a adequação dos ambientes que receberão os ativos de rede;
- b) as rotinas de verificação e conservação dos ambientes;
- c) canais de comunicação para solucionar dúvidas quanto à preparação de ambientes;
- d) canais de comunicação para registros de problemas quanto à instalação ou operação dos equipamentos na Unidade;
- e) os modelos de processo para contratação de serviços de acesso à internet.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Em atendimento ao art. 11, Inciso V, § 1º e 3º, da Instrução Normativa SGD/ME nº 94/2022, a equipe de elaboração entende que o estudo de soluções viáveis para esta demanda está de acordo com as necessidades do MinC.

Portanto, o presente Estudo Técnico Preliminar é justificadamente viável quanto aos requisitos de negócios, administrativos e técnicos a serem alcançados.

19. Responsáveis

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

FELIPE FINGER SANTIAGO

Integrante Técnico



Assinou eletronicamente em 03/11/2023 às 10:48:52.

FREDERICO GUIMARAES CARDOSO

Integrante Administrativo



Assinou eletronicamente em 03/11/2023 às 11:42:23.

RAMON LEONN VICTOR MEDEIROS

Integrante Requisitante



Assinou eletronicamente em 03/11/2023 às 10:53:56.

JAIME HELENO CORREA DE LISBOA

Autoridade máxima da área de TIC



Assinou eletronicamente em 03/11/2023 às 11:22:23.

Lista de Anexos

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

- Anexo I - ANEXO I - painel de preços.pdf (84.62 KB)
- Anexo II - Memória de Cálculo - item 1.pdf (301.22 KB)
- Anexo III - Anexo - Caderno de Especificações Técnicas - Firewall.pdf (158.42 KB)

Anexo I - ANEXO I - painel de preços.pdf



MINISTÉRIO DA
ECONOMIA

MÉDIA

R\$ 423.725,09

MEDIANA

R\$ 153.750,00

MENOR

R\$ 25.000

FILTROS APLICADOS

Código Material/Serviço Ano da Compra Modalidade da Compra

484747 2022, 2023 Pregão

Quantidade total de registros: 24

Registros apresentados: 1 a 24

Identificação da Compra	Número do Item	Modalidade	Código do CATMAT	Descrição do Item	Descrição Complementar	Unidade de Fornecimento	Quantidade Ofertada	Valor Unitário	Fornecedor	Órgão	UASG	Data da Compra
00108/2022	00003	Pregão	484747	FIREWALL		UNIDADE	44	R\$25000	GLOBAL SEC. TECNOLOGIA & INFORMACAO LTDA	DEFENSORIA PUBLICA DA UNIAO	290002 - DEFENSORIA PUBLICA DA UNIAO	13/12/2022
00006/2022	00009	Pregão	484747	FIREWALL		UNIDADE	1	R\$26190	ESTRATEGIA IT LTDA	CONSELHO FEDERAL DE EDUCAÇÃO FÍSICA	925042 - CONSELHO FEDERAL DE EDUCAÇÃO FÍSICA/RJ	21/10/2022
13710/2022	00001	Pregão	484747	FIREWALL		UNIDADE	1	R\$29400	ISH TECNOLOGIA S/A	INST.FED.DE EDUC.,CIENC.E TEC. DE SÃO PAULO	158154 - INST.FED.DE EDUC.,CIENC.E TEC.DE SÃO PAULO	27/12/2022
00004/2022	00008	Pregão	484747	FIREWALL		UNIDADE	6	R\$35500	STRATEGIO SISTEMAS SERVICOS E INFORMATICA LTDA.	INDUSTRIA DE MATERIAL BELICO DO BRASIL	168003 - IMBEL-INDUSTRIA DE MATERIAL BELICO DO BRASIL	06/06/2022
00075/2022	00014	Pregão	484747	FIREWALL		UNIDADE	3	R\$39200	BY INFORMATION TECHNOLOGY SERVICES LTDA	ESTADO DO RIO DE JANEIRO	926850 - FUNDO MUNICIPAL DE SAÚDE DE VOLTA REDONDA	19/08/2022
00108/2022	00002	Pregão	484747	FIREWALL		UNIDADE	26	R\$55500	GLOBAL SEC. TECNOLOGIA & INFORMACAO LTDA	DEFENSORIA PUBLICA DA UNIAO	290002 - DEFENSORIA PUBLICA DA UNIAO	13/12/2022

05712/2022	00001	Pregão	484747	FIREWALL		UNIDADE	1	R\$66000	ISH TECNOLOGIA S/A	INST.FED.DE EDUC.,CIENC.E TEC. DE SÃO PAULO	158154 - INST.FED.DE EDUC.,CIENC.E TEC.DE SÃO PAULO	09/06/2022
00018/2022	00002	Pregão	484747	FIREWALL		UNIDADE	1	R\$84000	IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIRELI	TRIBUNAL DE JUSTICA DO ESTADO DO AMAPA	925306 - TRIBUNAL DE JUSTICA DO ESTADO DO AMAPÁ	30/08/2022
00025/2022	00001	Pregão	484747	FIREWALL		UNIDADE	1	R\$109900,99	ITVALE - COMERCIO DE EQUIPAMENTOS DE INFORMATICA LTDA	ESTADO DO PARANA	928684 - CAMARA MUNICIPAL DE CASCAVEL	13/12/2022
00016/2022	00001	Pregão	484747	FIREWALL		UNIDADE	2	R\$125227	NTSEC SOLUCOES EM TELEINFORMATICA LTDA	ESTADO DO CEARA	451116 - SERVICO NACIONAL DE APRENDIZAGEM COMERCIAL	18/05/2022
00016/2022	00002	Pregão	484747	FIREWALL		UNIDADE	1	R\$130236,10	NTSEC SOLUCOES EM TELEINFORMATICA LTDA	ESTADO DO CEARA	451116 - SERVICO NACIONAL DE APRENDIZAGEM COMERCIAL	18/05/2022
00013/2022	00001	Pregão	484747	FIREWALL		UNIDADE	4	R\$137500	GLOBAL SEC. TECNOLOGIA & INFORMACAO LTDA	CONSELHO FEDERAL DE ODONTOLOGIA	926655 - CONSELHO FEDERAL DE ODONTOLOGIA	25/10/2022
00018/2022	00004	Pregão	484747	FIREWALL		UNIDADE	1	R\$170000	IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIRELI	TRIBUNAL DE JUSTICA DO ESTADO DO AMAPA	925306 - TRIBUNAL DE JUSTICA DO ESTADO DO AMAPÁ	30/08/2022
00016/2022	00003	Pregão	484747	FIREWALL		UNIDADE	4	R\$282647,10	NTSEC SOLUCOES EM TELEINFORMATICA LTDA	ESTADO DO CEARA	451116 - SERVICO NACIONAL DE APRENDIZAGEM COMERCIAL	18/05/2022
00097/2022	00001	Pregão	484747	FIREWALL		UNIDADE	2	R\$325000	INTEGRASUL SOLUCOES EM INFORMATICA LTDA	ESTADO DO RIO GRANDE DO SUL	988841 - PREFEITURA MUNICIPAL DE SANTA MARIA/RS	22/08/2022
00056/2022	00001	Pregão	484747	FIREWALL		UNIDADE	1	R\$451844	NETSOL LTDA	UNIVERSIDADE FEDERAL DE LAVRAS	153032 - UNIVERSIDADE FEDERAL DE LAVRAS/MEC/MG	19/09/2022
00230/2022	00001	Pregão	484747	FIREWALL		UNIDADE	2	R\$514800	APPROACH TECNOLOGIA LTDA	UNIVERSIDADE FEDERAL DE SANTA MARIA	153164 - UNIVERSIDADE FEDERAL DE STA.MARIA/RS	25/11/2022
00025/2022	00001	Pregão	484747	FIREWALL		UNIDADE	1	R\$545544	TELMEX DO BRASIL S/A	CIA.DE ENTREPOSTOS E ARMAZENS GER.DE S.PAULO	225001 - CIA, DE ENTREPOSTOS E ARMAZENS GER. DE SP	23/09/2022
00012/2022	00001	Pregão	484747	FIREWALL		UNIDADE	2	R\$560000	NCT INFORMATICA LTDA	MINISTERIO DAS COMUNICACOES	410003 - COORDENACAO GERAL DE RECURSOS LOGISTICOS	20/09/2022

00059/2022	00001	Pregão	484747	FIREWALL		UNIDADE	1	R\$700413	TELTEC SOLUTIONS LTDA	UNIVERSIDADE FEDERAL DA FRONTEIRA SUL	158517 - UNIVERSIDADE FEDERAL DA FRONTEIRA SUL	02/12/2022
00020/2022	00001	Pregão	484747	FIREWALL		UNIDADE	1	R\$740000	UNDER PROTECTION CONSULTORIA EM INFORMATICA LTDA	CONSELHO REG. ENGENHARIA E AGRONOMIA DO PR	389088 - CONSELHO REG.DE ENGENHARIA E AGRONOMIA DO PR	18/10/2022
00108/2022	00001	Pregão	484747	FIREWALL		UNIDADE	2	R\$966000	GLOBAL SEC. TECNOLOGIA & INFORMACAO LTDA	DEFENSORIA PUBLICA DA UNIAO	290002 - DEFENSORIA PUBLICA DA UNIAO	13/12/2022
00019/2022	00001	Pregão	484747	FIREWALL		UNIDADE	2	R\$1049500	APPROACH TECNOLOGIA LTDA	TRIBUNAL DE CONTAS DO ESTADO DO PIAUI	925466 - TRIBUNAL DE CONTAS DO ESTADO DO PIAUI	07/12/2022
00081/2022	00001	Pregão	484747	FIREWALL		UNIDADE	1	R\$3000000	TLD TELEDATA COMERCIO E SERVICOS LTDA	JUSTICA ELEITORAL	070011 - TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS	09/09/2022

Anexo II - Memória de Cálculo - item 1.pdf



MINISTÉRIO DA CULTURA
SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO
STII/GSE/GM/MinC

Ofício nº 517/2023/STII/GSE/GM/MinC

Brasília, na data da assinatura eletrônica.

Ao Senhor

Bruno Henrique Lins Duarte

Subsecretário de Planejamento, Orçamento e Administração

Esplanada dos Ministérios, Bloco B, 2º andar - Bairro Zona Cívica Administrativa,

Brasília/DF, CEP 70068-900

Assunto: **Pedido de informações preliminares pelo TCU - Pregão Eletrônico SRP 09/2023.**

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 01400.000997/2023-52.

Senhor Subsecretário,

1. Cumprimentando-o cordialmente, faço referência ao pregão eletrônico para a contratação de solução de firewall encaminhada pela Subsecretaria de Tecnologia da Informação e Inovação (STII), conforme Edital e seus anexos (SEI nº 1461189) e ao Ofício nº 984/2023/CGLC/SPOA/GSE/GM/MinC (1468498), o qual faz referência ao E-mail TCU - PE 09.2023 (SEI nº 1467894), solicitando informações preliminares acerca do Pregão Eletrônico SRP 09/2023, que devem ser respondidas por e-mail até o dia **27/10/2023**.

2. De modo a fornecer as informações necessárias para a elaboração de resposta ao pedido TCU - PE 09.2023 (SEI nº 1467894) e ainda, visando compor o estudo dos valores estimados a serem adotados para o processo de contratação em epígrafe, faço os seguintes apontamentos:

2.1. Verifica-se que o órgão de controle procedeu com a análise das informações disponíveis no processo de contratação apresentando, de forma didática, a planilha ilustrada a seguir, acrescentando alguns pregões de processos similares no intuito de auxiliar o estudo desta Pasta quanto ao valor estimado.

B	C	D	E	F	G	H	I	J	K	L
UASG	ORGANIZAÇÃO	PREGÃO	ITEM	SOLUÇÃO	GARANTIA (MESES)	Valor Unitário	Preço do Cluster (duas unidades)	Valor ajustado conforme item 11.8 do ETP	Qtd no TR MC	Valor Total
420001	ESTIMATIVA MINISTÉRIO DA CULTURA		1	Módulo de Segurança (cluster) tipo I	60	R\$ 1.256.643,20	R\$ 2.513.286,40	R\$ 2.513.286,40	3	R\$ 7.539.859,20
290002	DEFENSORIA PÚBLICA DA UNIÃO	108/2022	1	Fortnet 1801-F	36	R\$ 966.000,00	R\$ 1.932.000,00	R\$ 3.220.000,00	3	R\$ 9.660.000,00
158517	UNIVERSIDADE FEDERAL DA FRONTEIRA SUL	59/2022	1	PA-3410 (PALO ALTO)	36	R\$ 700.413,00	R\$ 1.400.826,00	R\$ 2.334.710,00	3	R\$ 7.004.130,00
70011	TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS	81/2022	1	Fortinet FG-1101E	36	R\$ 593.477,75	R\$ 1.186.955,50	R\$ 1.978.259,17	3	R\$ 5.934.777,50
925466	TRIBUNAL DE CONTAS DA UNIÃO DO ESTADO DO PIAUÍ	19/2022	1	PA-3410 (PALO ALTO)	60	R\$ 1.049.500,00	R\$ 2.099.000,00	R\$ 2.099.000,00	3	R\$ 6.297.000,00
110404	MINISTÉRIO DA DEFESA	26/2022	7	PA-3410 (PALO ALTO)	36	R\$ 454.750,00	R\$ 909.500,00	n/a	n/a	n/a
70010	TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO	73/2022	9	Fortnet 1801-F	60	R\$ 646.457,60	R\$ 1.292.915,20	n/a	n/a	n/a
150182	UNIVERSIDADE FEDERAL FLUMINENSE	75/2021	3	Fortinet FG-1101E	36	R\$ 275.348,55	n/a	n/a	n/a	n/a

2.2. **Apontamento TCU - Os ajustes nos preços tiveram como premissa a existência de uma linearidade mensal para todo o equipamento, inclusive para elemento de hardware, ou seja, sem considerar as proporções de valor de cada elemento (partnumber) que compõe a solução e daqueles que são de fato mensurados conforme um prazo;**

2.2.1. Primeiramente cabe ressaltar que, para a composição da solução de segurança a ser adquirida a equipe adotou o padrão de contratações de soluções de NGF firewall observado em vários órgãos similares a esta Pasta, onde opta-se pela especificação técnica dos recursos mínimos necessários para atender a necessidade do órgão, possibilitando ao Licitante a junção dos equipamentos e dos licenciamentos necessários da forma que melhor atenda sua estratégia comercial para a composição do equipamento a ser ofertado, essa estratégia possibilita a ampliação da concorrência e dando transparência ao processo.

2.2.2. Desta forma, considerando que as licitantes podem combinar equipamentos e licenciamentos de diversos *partnumbers*, desde que atendam aos requisitos mínimos exigidos, o estudo para a estimativa do valor da contratação foi realizado por meio da comparação de pregões similares, observando-se a compatibilidade do porte das soluções de firewall exigidas e as condições de garantia.

2.3. ***Apontamento TCU - Não foram identificadas no processo as composições dos preços unitários das soluções encontradas nas outras contratações públicas, isto é, os preços unitários de cada partnumber que compõe a solução;***

2.3.1. Para o levantamento das informações que subsidiaram a composição do valor estimado foram observadas as informações publicadas nos resultados dos pregões, uma vez que a equipe optou por a comparação do item, não sendo realizado detalhamento para um levantamento por cada partnumber que compõe o item dos pregões.

2.3.2. Neste sentido, considerando que cada órgão possui características e exigências distintas, mas que vários podem ser atendidos por um mesmo tipo ou modelo de equipamento, embora a análise com nível de detalhamento até o partnumber possa trazer maior refinamento ao estudo, há possibilidade de que ocorram situações que um pregão possua componentes detalhados de forma diferente daqueles previstos pela equipe, porém isso não inviabiliza o fato de que o mesmo equipamento possa atender os requisitos mínimos previstos para o pregão em estudo, assim para que fosse possível comparar os processos de contratações a equipe optou pela análise dos itens licitados não adentrando as questões de partnumber ou grupos de partnumber que venha a compor o item.

2.4. ***Apontamento TCU - Não foram identificados no processo pedidos de informação às organizações responsáveis pelos pregões utilizados, a fim de se obter maiores informações acerca dos valores da garantia;***

2.4.1. Para o levantamento das informações que subsidiaram a composição do valor estimado foram observadas as informações publicadas nos certames, uma vez que a equipe optou por adotar a adequação da garantia de forma linear.

2.4.2. Como pode ser observado na amostra de pregões constante da planilha, em 07 pregões diferentes sagraram-se vencedores 02 fabricantes com 3 modelos diferentes, embora todos os modelos dos equipamentos vencedores dos certames por suas características técnicas poderiam atender a demanda do Ministério, as diferenças em relação ao período de garantia tornaria alguns incompatíveis com o objeto a ser contratado para o MINC.

2.5. ***Apontamento TCU - Não foi identificada no processo análise crítica dos preços após os referidos ajustes, a fim de se verificar a razoabilidade e a aderência aos preços de soluções para 60 meses de garantia.***

2.6. Quanto a análise, considerando os apontamentos realizados pelo TCU, onde restou identificada a necessidade de melhorar a instrução processual de forma a tornar mais claros os fatores que motivaram a escolha da composição do valor estimado, consta registrada uma nova análise aproveitando a contribuição constante da planilha as informações fornecidas, pelo Órgão de Controle. *In Verbis*:

Análise crítica dos preços estimados, considerando as seguintes contratações públicas e os seguintes pontos: Referente ao item 1. No cenário a seguir, as linhas amarelas contêm as informações referentes aos pregões utilizados no estabelecimento do preço estimado; Após os ajustes realizados nos valores unitários, conforme item 11.8 do ETP, há uma variação de 63%. Tendo em

vista o valor total, essa variação equivale a R\$ 3.725.222,50;
A IN SEGES/ME 65/2021, art. 6º, § 4º, estabelece que os preços coletados devem ser analisados de forma crítica, em especial, quando houver grande variação entre os valores apresentados;
Seguem mais três licitações que adquiriram soluções semelhantes àquelas utilizadas no cálculo do preço estimado, a fim de trazer mais insumos para a análise crítica;
A título de exemplo, considerando os dois pregões já com 60 meses de garantia (em negrito na tabela), o valor médio do cluster seria de R\$ 1.695.957,60;
Ressalta-se que a tabela abaixo não tem o objetivo de substituir a pesquisa de preço realizada, cabendo aos gestores a gestão dos riscos quanto aos valores das licitações versus as soluções ofertadas.

UASG	Organização	Pregão	Item	Solução	Garantia (meses)	Valor Unitário (R\$)	Preço do Cluster (2 unidades)	Valor ajustado, conforme item 11.8 do ETP	Qtd no TR MC	Valor Total
420001	Ministério da Cultura	-	1	Módulo de Segurança (Cluster) Tipo I	60	1.256.643,20	2.513.286,39	2.513.286,39	3	7.539.859,17
290002	DEFENSORIA PUBLICA DA UNIAO	108/2022	1	Fortinet 1801-F	36	966.000,00	1.932.000,00	3.220.000,00	3	9.660.000,00
158517	UNIVERSIDADE FEDERAL DA FRONTEIRA SUL	59/2022	1	PA-3410	36	700.413,00	1.400.826,00	2.334.710,00	3	7.004.130,00
70011	TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS	81/2022	1	Fortinet FG-1101E	36	593.477,75	1.186.955,50	1.978.259,17	3	5.934.777,50
925466	TRIBUNAL DE CONTAS DO ESTADO DO PIAUI	19/2022	1	PA-3410	60	1.049.500,00	2.099.000,00	2.099.000,00	3	6.297.000,00
110404	MINISTERIO DEFESA	26/2022	7	PA-3410	36	454.750,00	909.500,00	N/A	-	-
70010	TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO	73/2022	9	Fortinet 1801-F	60	646.457,60	1.292.915,20	N/A	-	-
150182	UNIVERSIDADE FEDERAL FLUMINENSE	75/2021	3	Fortinet FG-1101E	36	275.348,55	550.697,10	N/A	-	-
MÉDIA DAS CONTRATAÇÕES UTILIZADAS PARA CALCULAR O PREÇO ESTIMADO										7.223.976,88
VARIAÇÃO ENTRE AS CONTRATAÇÕES UTILIZADAS PARA CALCULAR O PREÇO ESTIMADO (%)										63%
VARIAÇÃO ENTRE AS CONTRATAÇÕES UTILIZADAS PARA CALCULAR O PREÇO ESTIMADO (R\$)										3.725.222,50
VALOR MÉDIO DAS CONTRATAÇÕES COM 60 MESES DE GARANTIA (cluster)										1.695.957,60

2.6.1. Infere-se da Planilha que o Valor médio das contratações com 60 meses de garantia (cluster) é de 1.695.957,00 considerando que para alcançar esse valor na planilha foi adotada a média entre o pregão 72/2022 do TRE-PE e o pregão 108/2022 da DPU.

2.6.2. Por meio de uma análise comparativa dos pregões 108/2022 e 73/2022 verifica-se que o TRE-PE conseguiu adquirir o mesmo equipamento que a DPU com 60 meses de garantia por 67% do valor pago pela DPU para um período de 36 meses, conforme quadro ilustrado a seguir:

290002	DEFENSORIA PÚBLICA DA UNIÃO	108/2022	1	Fortnet 1801-F	36	R\$ 966.000,00	R\$ 1.932.000,00	Diferença
70010	TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO	73/2022	9	Fortnet 1801-F	60	R\$ 646.457,60	R\$ 1.292.915,20	R\$ 639.084,80

2.6.3. Neste sentido infere-se que a aquisição do TRE-PE resultou de uma situação atípica, uma vez que o valor pago pela DPU está aproximado dos valores obtidos nos outros pregões constantes das amostras em análise.

2.6.4. Assim uma eventual utilização do preço obtido pelo TRE-PE como valor a ser somado para o alcance da média que deverá compor o valor estimado para o pregão do Minc não representaria um valor similar aos valores alcançados em outros pregões.

2.6.5. Ressalta-se que ajuste realizado para colocar os pregões de 36 meses de garantia em situação próxima daquela em que estão os pregões com 60 meses de garantia, este foi motivado tendo em

vista o alcance da utilização de toda a vida útil do equipamento, que é de 05 anos.

2.6.6. Exigir garantia de ativos de rede de pelo menos 05 anos é uma recomendação do SISP, tendo em vista a vida útil de tais equipamentos, desta forma, considerando que soluções de firewall sem atualização de softwares, vacinas e etc, não atenderia a necessidade para a qual foi adquirida, caso o Minc optasse por adquirir uma solução com 36 meses de garantia, ao término deste prazo seria necessário fazer uma contratação de extensão de garantia ou substituir o equipamento que ainda não teria concluído seu ciclo de vida útil.

2.6.7. Para tanto, segundo a orientação forma do SISP, manual d e *BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC - Versão 4*, Manual CONTRATAÇÃO DE ATIVOS DE TIC (1474791)

1.2. AQUISIÇÃO DE ATIVOS COM GARANTIA VERSUS CONTRATAÇÃO DE SERVIÇOS DE MANUTENÇÃO

1.2.1. Os ativos de TI devem ser adquiridos com garantia de funcionamento provida pelo fornecedor durante sua vida útil, salvo quando justificado o contrário e com relação ao ativo em específico.

1.2.2. Tal procedimento se justifica pelo fato de que, de forma geral a contratação, a posteriori, de serviços de manutenção para ativos fora de garantia, usualmente é mais onerosa para a Administração do que quando o bem é adquirido com garantia para toda sua vida útil. Ainda, os contratos de manutenção têm seus custos elevados na medida em que os bens mantidos se tornam obsoletos. Ou seja, quanto mais antigo for o ativo de TI, menor seu valor comercial e maior será seu custo de manutenção, devido à dificuldade de provimento de peças de reposição e do maior risco do fornecedor descumprir os níveis de serviço exigidos para reparo desses equipamentos.

1.2.3. Tem-se, portanto, que um dos fatores que para definição do posicionamento adequado da tecnologia (item 1.1) é o tempo de vida útil previsto para utilização do ativo e, por conseguinte, o tempo de garantia de funcionamento a ser contratado.

1.2.4. Complementarmente ao tempo de garantia de funcionamento, o nível de serviço mínimo exigido para reparo ou substituição dos ativos defeituosos é outro fator importante que deverá ser observado pela Equipe de Planejamento da Contratação.

1.2.5. A definição do nível de serviço mínimo exigido deverá ser justificada com base na necessidade da Administração, que deverá estabelecer a aplicação de eventuais sanções adequadas por desatendimento ao nível de serviço exigido.

1.2.6. Por fim, cumpre frisar que o tempo de garantia de funcionamento e a exigência de nível de serviço mínimo de atendimento são fatores encarecedores; portanto, a Equipe de Planejamento da Contratação deverá pautar-se na razoabilidade e na observância ao interesse público para a correta definição desses elementos.

2.6.8. Neste sentido o referido manual atribui a vida útil de ativos de rede, do grupo em que se aplica o NG FIREWALL, o prazo de 05 (cinco) anos, conforme item 1.4.5, In Verbis:

1.4.5. SERVIDORES DE REDE, APLICAÇÃO, EQUIPAMENTOS DE BACKUP, ARMAZENAMENTO, SEGURANÇA, ENTRE OUTROS

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.

2.7. Manifestada a justificativa para a opção de aquisição com garantia de atualização e assistência técnica por 60 (sessenta) meses, cabe a realização dos procedimentos relacionados a revisão do valor estimado, vistos todos os apontamentos relacionados a justificativa para a implementação do cenário estimativo de condições de garantia similares entre os pregões estudados, o valor estimado a ser considerado para o item 01 do processo licitatório em epígrafe poderá ser aquele obtido pela média dos valores ajustados no pregão 59/2022 e 81/2022 com o pregão 19/2022.

2.7.1. Assim, diante da composição dos levantamentos de pregões similares feito pela equipe de planejamento da contratação, combinada com os pregões citados pelo TCU, foi possível chegar a um universo de 06 (seis) licitações, compostas de valores finais de pregões.

2.7.2. Verifica-se então que o pregão 73/2022 apresentou o menor valor total e o pregão 108/2022 que apresentou o maior valor total (itens destacados em laranja na ilustração), com uma diferença de 249% entre eles, fator de discrepância que poderia comprometer a qualidade de uma estimativa baseada simplesmente na aplicação da média.

2.7.3. Portanto, diante do cenário das discrepâncias entre o valor mais baixo e o valor mais alto, no intuito de que o valor estimado esteja o mais próximo do valor praticado no mercado, **será adotada a Mediana**, conforme números destacados em amarelo, no quadro a seguir:

B	C	D	E	F	G	H	I	J	K	L
UASG	ORGANIZAÇÃO	PREGÃO	ITEM	SOLUÇÃO	GARANTIA (MESES)	VALOR UNITÁRIO	PREÇO DO CLUSTER (duas unidades)	Valor ajustado conforme item 11.8 do ETP	Qtd no TR MINC.	Valor Total
290002	DEFENSORIA PÚBLICA DA UNIÃO	108/2022	1	Fortnet 1801-F	36	R\$ 966.000,00	R\$ 1.932.000,00	R\$ 3.220.000,00	3	R\$ 9.660.000,00
158517	UNIVERSIDADE FEDERAL DA FRONTEIRA SUL	59/2022	1	PA-3410 (PALO ALTO)	36	R\$ 700.413,00	R\$ 1.400.826,00	R\$ 2.334.710,00	3	R\$ 7.004.130,00
925466	TRIBUNAL DE CONTAS DA UNIÃO DO ESTADO DO PIAUÍ	19/2022	1	PA-3410 (PALO ALTO)	60	R\$ 1.049.500,00	R\$ 2.099.000,00	R\$ 2.099.000,00	3	R\$ 6.297.000,00
70011	TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS	81/2022	1	Fortinet FG-1101E	36	R\$ 593.477,75	R\$ 1.186.955,50	R\$ 1.978.259,17	3	R\$ 5.934.777,50
110404	MINISTÉRIO DA DEFESA	26/2022	7	PA-3410 (PALO ALTO)	36	R\$ 454.750,00	R\$ 909.500,00	R\$ 1.515.833,33	3	R\$ 4.547.500,00
70010	TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO	73/2022	9	Fortnet 1801-F	60	R\$ 646.457,60	R\$ 1.292.915,20	R\$ 1.292.915,20	3	R\$ 3.878.745,60
MÉDIA DAS CONTRATAÇÕES UTILIZADAS PARA CALCULAR O PREÇO ESTIMADO (retirados o valor mais alto e o valor mais baixo)										R\$ 6.220.358,85
MÉDIA DAS CONTRATAÇÕES UTILIZADAS PARA CALCULAR O PREÇO ESTIMADO (retirados o valor mais alto e o valor mais baixo)										R\$ 6.115.888,75
(NA MEDIANA) VARIAÇÃO ENTRE AS CONTRATAÇÕES UTILIZADAS PARA CALCULAR O PREÇO ESTIMADO (%)										5,75%
VARIAÇÃO ENTRE AS CONTRATAÇÕES UTILIZADAS PARA CALCULAR O PREÇO ESTIMADO - UTILIZANDO A MEDIANA (R\$)										R\$ 362.222,50
(retirados o valor mais alto e o valor mais baixo) VARIAÇÃO ENTRE AS CONTRATAÇÕES UTILIZADAS PARA CALCULAR O PREÇO ESTIMADO - UTILIZANDO A MÉDIA (R\$)										R\$ 2.456.630,00
VALOR DA MEDIANA DAS CONTRATAÇÕES COM 60 MESES DE GARANTIA (POR CLUSTER)										R\$ 2.038.629,58

2.7.4. Diante dos apontamentos constantes neste documento, e em complementação aos trabalhos relacionados ao cálculo do valor estimado para o item 01, de forma a retificar os cálculos realizados pela equipe no processo licitatório em epígrafe, será adotado o como valor estimado, **o obtido pela mediana dos pregões**, conforme destacado no quadro supracitado, e de acordo com o previsto no artigo 6º da INSTRUÇÃO NORMATIVA SEGES /ME Nº 65, DE 7 DE JULHO DE 2021. In Verbis:

Art. 6º Serão utilizados, como métodos para obtenção do preço estimado, a média, a **mediana** ou o menor dos valores obtidos na pesquisa de preços, desde que o cálculo incida sobre um conjunto de três ou mais preços, oriundos de um ou mais dos parâmetros de que trata o art. 5º, desconsiderados os valores inexequíveis, inconsistentes e os excessivamente elevados.

2.7.5. Cabe ressaltar que todos os modelos citados nos estudos, apresentam características compatíveis com as necessidades/especificações constantes do objeto da licitação em epígrafe: **FortiGate 1801-F** (fabricante: **Fortnet**) ; **PA-3410** (Fabricante: **Palo Alto**).

3. Portanto, restou verificado que há a necessidade de se realizar a alteração do valor estimado para o Item 01, ainda que se pese o fato de que há a necessidade célere pela aquisição da solução de segurança, é preciso tomar as

providências de ajustes ao processo para sua correta instrução.

4. Neste sentido, encaminho os autos para análise da Subsecretaria de Planejamento, Orçamento e Administração - SPOA, e para a CGLC para o encaminhamento ao órgão de Controle, conforme solicitado.

5. Sem mais para o momento, encaminho os autos e coloco-me a disposição para o fornecimento de informações complementares, caso julgue necessário.

Atenciosamente,

JAIME HELENO CORREA DE LISBOA

Subsecretário de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **Jaime Heleno Correa de Lisboa, Subsecretário(a) de Tecnologia da Informação e Inovação**, em 25/10/2023, às 20:26, conforme horário oficial de Brasília, com fundamento no art. 30, inciso II, da Portaria nº 26/2016, de 01/04/2016, do Ministério da Cultura, Publicada no Diário Oficial da União de 04/04/2016.



A autenticidade deste documento pode ser conferida no site https://sei.cultura.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1471623** e o código CRC **94902127**.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 01400.000997/2023-52

SEI nº 1471623

Anexo III - Anexo - Caderno de Especificações Técnicas - Firewall.pdf



MINISTÉRIO DA CULTURA

SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO

Esplanada dos Ministérios, Bloco B, - Bairro Zona Cívica Administrativa, Brasília/DF, CEP 70068-900

Telefone: - <http://www.cultura.gov.br>

CADERNO DE ESPECIFICAÇÕES TÉCNICAS

PROCESSO: 01400.000997/2023-52

DOCUMENTOS RELACIONADOS

OBJETO - Registro de preços para aquisição de uma solução de proteção de rede Next Generation Firewall (NGFW) com garantia e suporte

ESTUDO TÉCNICO PRELIMINAR **03/2023**

CONTRATAÇÃO: **420001/000047/2023**

QUADRO DE COMPOSIÇÃO - GRUPO/LOTE E ITENS.

LOTE	ITEM	DESCRIÇÃO
01	1	MÓDULO DE SEGURANÇA (CLUSTER) - TIPO I
	2	MÓDULO DE SEGURANÇA - TIPO II
	3	MÓDULO DE SEGURANÇA - TIPO III
	4	SISTEMA DE GERÊNCIA CENTRALIZADA COM ARMAZENAMENTO DE LOGS
	5	SWITCH DE ACESSO TIPO 02 (48 PORTAS GIGABIT POE+)
	6	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO PARA A SOLUÇÃO
	7	TREINAMENTO "HANDS ON" SOBRE SOLUÇÃO DE FIREWALL

1. ITEM 01 - MÓDULO DE SEGURANÇA (CLUSTER) - TIPO I - CARACTERÍSTICAS FÍSICAS E DE PERFORMANCE MÍNIMAS PARA CADA EQUIPAMENTO

1.1. A solução deve possuir throughput de, no mínimo, 19 (dezenove) Gbps de Next Generation Firewall, considerando no mínimo as funcionalidades de Firewall e Controle de Aplicação, sendo comprovado com documentação de domínio público;

1.2. deve possuir throughput de, no mínimo, 10 (Dez) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus, Anti-Spyware e log habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;

1.3. Deve possuir, no mínimo, 2 (duas) interfaces físicas de rede de 40G/100G QSFP/QSFP28, (devendo ser fornecido 2(dois) transceiver 40 G QSFP+ SR ;

1.4. Deve possuir, no mínimo, 2 (duas) interfaces físicas dedicadas para o recurso de alta disponibilidade não sendo permitido o uso de interfaces do quantitativo já solicitado;

1.5. Deve suportar, no mínimo, 2.000.000 (dois milhões) sessões simultâneas;

- 1.6. Deve suportar, no mínimo, 215.000 (Duzentos e quinze mil) novas conexões por segundo;
- 1.7. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 1/10 Gbps do tipo RJ-45;
- 1.8. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1/10 Gbps do tipo SFP/SFP+; (Deverão ser fornecidos 04 (quatro) unidades de Transceivers Conector duplex LC / fibra MMF / 1GBASE-SX) e 04 (quatro) unidades de Transceivers com Conector duplex LC / fibra MMF / 10GBASE-SR)
- 1.9. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 25 Gbps do tipo SFP28; (Deverão ser fornecidos 04 (quatro) unidades de Transceivers com Conector duplex LC / fibra MMF / 25GBASE-SR.)
- 1.10. Deve possuir, no mínimo, 2 (duas) interfaces físicas de rede de 40G/100G QSFP/QSFP28; (Deverão ser fornecidos 02 (duas) unidades de Transceivers Conector duplex LC / fibra SMF ou MMF / 40GBASE-LM4.)
- 1.11. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 10Mbps/100Mbps/1Gbps do tipo RJ-45;
- 1.12. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1Gbps dedicada para gerenciamento;
- 1.13. Deve possuir, no mínimo, 2 (duas) interface física dedicada para o recurso de alta disponibilidade não sendo permitido o uso de interface de propósito geral para essa finalidade.
- 1.14. Deve ser possível, configurar de maneira individual, as características de velocidade de cada interface do equipamento.
- 1.15. O equipamento deverá ter homologação da Agência Nacional de Telecomunicações (ANATEL), exigência a ser comprovada por meio da apresentação pela Licitante do certificado quanto da entrega dos documentos de habilitação.
- 1.16. Deve possuir disco do tipo Solid State Drive (SSD) de, no mínimo, 480 (quatrocentos e oitenta) GB para armazenamento do sistema operacional e registro de logs;
- 1.17. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento;
- 1.18. Deve suportar, no mínimo, 1.800 (mil e oitocentos) túneis de VPN client to site simultaneamente, estando devidamente licenciado para este fim;

2. ITEM 02 - MÓDULO DE SEGURANÇA DO - TIPO II -
CARACTERÍSTICAS FÍSICAS E DE PERFORMANCE MÍNIMAS PARA CADA EQUIPAMENTO

- 2.1. Deve possuir throughput de, no mínimo, 9 (nove) de Gbps de Next Generation Firewall considerando no mínimo as funcionalidades de Firewall e Controle de Aplicação, sendo comprovado com documentação de domínio público;
- 2.2. Deve possuir throughput de, no mínimo, 4.5 (quatro, cinco) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus, Anti-Spyware e log habilitados simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;
- 2.3. Deve suportar, no mínimo, 1.200.000 (um milhão e duzentos mil) sessões simultâneas;
- 2.4. Deve suportar, no mínimo, 120.000 (cento e vinte mil) novas conexões por segundo;

- 2.5. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 1Gbps do tipo RJ-45;
- 2.6. Deve possuir, no mínimo, 2 (duas) interfaces físicas de rede de 1Gbps do tipo SFP; (Deverão ser fornecidos 02 (duas) unidades de Transceivers Conector duplex LC / fibra MMF / 1GBASE-SX.)
- 2.7. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 10Gbps do tipo SFP+; (Deverão ser fornecidos 08 (oito) unidades de Transceivers Conector duplex LC / fibra MMF / 10GBASE-SR)
- 2.8. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1Gbps dedicada para gerenciamento;
- 2.9. Deve possuir, no mínimo, 2 (duas) interface física dedicada para o recurso de alta disponibilidade;
- 2.10. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;
- 2.11. Deve ser possível, configurar de maneira individual, as características de velocidade de cada interface do equipamento.
- 2.12. Deve possuir disco do tipo Solid State Drive (SSD) de, no mínimo, 240 (duzentos e quarenta) GB para armazenamento do sistema operacional e registro de logs;
Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento;
- 2.13. Deve suportar, no mínimo, 1.000 (mil) túneis de VPN client to site simultaneamente, estando devidamente licenciado para este fim;
O equipamento deverá ter homologação da Agência Nacional de Telecomunicações (ANATEL), exigência a ser comprovada por meio da apresentação pela Licitante do certificado quanto da entrega dos documentos de habilitação.

3. ITEM 03 - MÓDULO DE SEGURANÇA DO - TIPO III -
CARACTERÍSTICAS FÍSICAS E DE PERFORMANCE MÍNIMAS PARA CADA EQUIPAMENTO

- 3.1. Deve possuir throughput de, no mínimo, 2 (dois) Gbps de Next Generation Firewall considerando no mínimo as funcionalidades de Firewall e Controle de Aplicação, sendo comprovado com documentação de domínio público;
- 3.2. Deve possuir throughput de, no mínimo, 1 (um) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus, Anti-Spyware e log habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;
- 3.3. Deve suportar, no mínimo, 180.000 (cento e oitenta mil) sessões simultâneas;
Deve suportar, no mínimo, 35.000 (trinta e cinco mil) novas conexões por segundo;
- 3.4. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1Gbps do tipo RJ-45;
- 3.5. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1Gbps dedicada para gerenciamento;
- 3.6. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;
- 3.7. Deve possuir disco interno de no mínimo, 128 (cento, vinte e oitenta) GB para armazenamento do sistema operacional e registro de logs;
- 3.8. O equipamento deve suportar fonte de alimentação elétrica

redundante capaz de operar entre 120 à 240 VAC;

3.9. Deve suportar, no mínimo, 500 (quinhentos) túneis de VPN client to site simultaneamente, estando devidamente licenciado para este fim;

3.10. O equipamento deverá ter homologação da Agência Nacional de Telecomunicações (ANATEL), exigência a ser comprovada por meio da apresentação pela Licitante do certificado quanto da entrega dos documentos de habilitação.

3.11. Deverá ser fornecido na sede do Ministério da Cultura com todas as configurações necessárias homologadas pela equipe de fiscalização, devendo acompanhar o equipamento todos os itens necessários para fixação em rack padrão 19" podendo ser fornecida bandeja ou trilho de fixação de acordo com as recomendações do fabricante.

4. FUNCIONALIDADES GERAIS DOS MÓDULOS DE SEGURANÇA TIPO I, TIPO II e TIPO III

4.1. A solução de deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

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

4.2. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

4.3. A solução de segurança, deve possuir nativamente funcionalidade de Machine Learning capaz de bloquear grande volume dos ataques nas suas redes.

4.4. Os Firewalls de segurança físico, devem possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problemas. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP;

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

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

4.6.1. gregação de links 802.3ad e LACP para o equipamento do tipo I;

4.6.2. Policy based routing ou policy based forwarding;

4.6.3. Roteamento multicast (PIM-SM);

4.6.4. DHCP Relay;

4.6.5. DHCP Server;

4.6.6. Jumbo Frames;

4.6.7. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3
Suportar sub-interfaces ethernet logicas

4.7. Deve suportar os seguintes tipos de NAT:

4.7.1. Nat dinâmico (Many-to-1);

4.7.2. Nat dinâmico (Many-to-Many);

4.7.3. Nat estático (1-to-1);

- 4.7.4. NAT estático (Many-to-Many);
- 4.7.5. Nat estático bidirecional 1-to-1;
- 4.7.6. Tradução de porta (PAT);
- 4.7.7. NAT de Origem;
- 4.7.8. NAT de Destino;
- 4.7.9. Suportar NAT de Origem e NAT de Destino simultaneamente;
- 4.8. Deve implementar Network Prefix Translation (NPTv6), NAT66 ou similar que traduza prefixos de endereços de rede IPv6;
- 4.9. Enviar log para sistemas de monitoração externos;
- 4.10. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- 4.11. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
- 4.12. Proteção contra anti-spoofing;
- 4.13. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 4.14. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- 4.15. Suportar a OSPF graceful restart;
- 4.16. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
- 4.17. O dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 4.18. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 4.19. Modo Camada - 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 4.20. Modo Camada - 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 4.21. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 4.22. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
 - 4.22.1. Em modo transparente;
 - 4.22.2. Em layer 3;
- 4.23. A configuração em alta disponibilidade deve sincronizar:
 - 4.23.1. Sessões;
 - 4.23.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede; Certificados de-criptografados;
 - 4.23.3. Associações de Segurança das VPNs;
 - 4.23.4. Tabelas FIB;
- 4.24. No modo HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

4.25. **SD-WAN**

4.25.1. Deve operacionalizar no mínimo os seguintes critérios de SD-WAN;

4.25.2. A plataforma de segurança deverá recuperar pacotes perdidos antes que seja necessário alterar o caminho principal.

4.25.3. As configurações de perfis de SD-WAN devem partir de um ponto central permitindo alteração e criação dos elementos primordiais para o funcionamento da solução. Deve também entregar a criação automática dos túneis IPSEC entre as localidades.

4.25.4. A solução deve permitir operar em caráter de diagrama hub-spoke.

4.25.5. É considerado diferencial dispositivos que tenham a capacidade de exibir impactos por aplicação.

4.25.6. A solução deve permitir ao administrador métricas de utilização de banda por circuito disponível e desta forma exibir no mínimo os seguintes itens em porcentagem ou contadores, jitter, latência e perda de pacote.

4.25.7. O dispositivo deve compreender o que está causando desempenho de degradação para as aplicações e serviços ativos e assim garantir que a experiência do usuário sofra o menor impacto possível.

4.25.8. O SD-WAN deve suportar os seguintes tipos de conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LT /3G/4G/5G, MPLS, Link de rádio e Link satélite desde que a sua terminação permita conectividade com interfaces ethernet.

4.25.9. A solução deve ter inteligência para executar no mínimo as seguintes lógicas de operação:

a) Distribuição de tráfego por prioridade de circuito, circuitos exclusivos de contingenciamento em 3G/4G/5G devem ser utilizados apenas em caso de falha geral dos circuitos ADSL/MPLS.

b) Distribuição de tráfego de acordo com métricas definidas por origem e destino, o dispositivo deve permitir ao administrador criar perfis com base em latência, jitter ou perda de pacotes para que uma vez que estes limites sejam atingidos o dispositivo possa manter a conexão por circuitos que apresenta resultados abaixo dos limites definidos.

c) Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes.

4.25.10. Quando ambos os pontos de extremidade dos túneis SD-WAN estiverem ativos, deve haver a duplicação de pacotes (PD) para manter a experiência dos usuários mesmo em condição de perda de pacotes. A duplicação de pacotes deve criar uma cópia do fluxo de tráfego do aplicativo e a enviar em ambos os túneis disponíveis, que está orientado ao mesmo destino.

4.25.11. O dispositivo de SD-WAN deve utilizar "*Forward Error Correction*" (FEC) habilitado, para permitir que aplicativos sensíveis à perda de pacotes não sejam impactados em caso de perda de pacote e recupere os pacotes perdidos ou corrompidos usando pacotes de paridade incorporados no fluxo da comunicação. O objetivo é reparar o fluxo antes que ele precise fazer failover para outro caminho.

4.25.12. O SD-WAN deve permitir combinar vários serviços ISP em uma interface Ethernet Agregada (AE) para redundância de link. A interface agregada deve oferecer suporte a subinterfaces para que seja possível marcar diferentes serviços ISP usando tags. de VLAN de camada 3 a fim de obter segmentação de tráfego de ponta a ponta.

4.25.13. O SD-WAN deve permitir o monitoramento de integridade

do caminho de aplicativos SaaS para garantir decisões com base em confiabilidade e experiência do usuário. Nos cenários onde o SD-WAN com link de acesso direto à Internet (DIA), deve permitir o failover para um caminho de desempenho mais alto com base em medições precisas da qualidade da aplicação.

4.25.14. Distribuição orientada a qualidade, o dispositivo deve validar o melhor caminho disponível e utilizar deste "path" para manter sessões ativas, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes.

4.26. CONTROLE POR POLÍTICA DE FIREWALL

4.26.1. Deverá suportar controles por zona de segurança.

4.26.2. Controles de políticas por porta e protocolo.

4.26.3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

4.26.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

4.26.5. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;

4.26.6. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;

4.26.7. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;

4.26.8. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

4.26.9. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).

4.26.10. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

4.26.11. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com HTTP/2 , TLS 1.2 e TLS 1.3;
Controle de inspeção e de-criptografia de SSH por política;

4.26.12. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

4.26.13. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;

4.26.14. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

4.26.15. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
Suporte a objetos e regras IPV6.

4.26.16. Suporte a objetos e regras multicast.

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

4.26.18. Deve possuir ferramenta que indique as regras sobrepostas e objetos não utilizados para otimização das regras. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.

4.27. **CONTROLE DE APLICAÇÕES**

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

- a) Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
- b) Reconhecer pelo menos 3000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- c) Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.
- d) Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- e) Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;
- f) Identificar o uso de táticas evasivas via comunicações criptografadas;
- g) Atualizar a base de assinaturas de aplicações automaticamente;
- h) Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
- i) Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
- j) Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- k) Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;
- l) Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
- m) O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- n) Deve alertar o usuário quando uma aplicação for bloqueada;
- o) Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

4.27.2. Deve permitir criar filtro na tabela de regras de segurança para exibir somente:

- a) Regras que permitem passagem de tráfego baseado na porta e

não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;

b) Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;

c) Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;

4.27.3. Deve possuir mecanismo para controlar vazamento de dados, permitindo a reconhecimento de pelo menos os seguintes tipos de arquivos: * PDF; * EXE; * .Doc; * .PPT; * Excell.

4.27.4. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload"

4.27.5. A solução de controle de dados deve permitir ações como permitir, alertar ou bloquear do envio de arquivos.

4.27.6. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes estiverem sendo trafegados através de aplicações como: Dropbox-uploading, filedropper e outros.

4.28. **PREVENÇÃO DE AMEAÇAS**

4.28.1. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

4.28.2. Deve ter a capacidade de bloquear ameaças desconhecidas em tempo real;

4.28.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado com a última base de assinatura instalada no momento em que a licença expirou, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

4.28.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

4.28.5. As assinaturas podem ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

4.28.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

4.28.7. Deve permitir o bloqueio de vulnerabilidades.

4.28.8. Deve permitir o bloqueio de exploits conhecidos.

4.28.9. Deve incluir proteção contra ataques de negação de serviços.

4.28.10. Deverá possuir os seguintes mecanismos de inspeção de IPS:

a) Análise de padrões de estado de conexões;

b) Análise de decodificação de protocolo;

c) Análise para detecção de anomalias de protocolo;

d) Análise heurística;

e) IP Defragmentation;

f) Remontagem de pacotes de TCP;

g) Bloqueio de pacotes malformados.

- 4.28.11. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;
- 4.28.12. Detectar e bloquear a origem de port scans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;
- 4.28.13. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 4.28.14. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
- 4.28.15. Possuir assinaturas específicas para a mitigação de ataques DoS;
- 4.28.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 4.28.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 4.28.18. Identificar e bloquear comunicação com botnets;
- 4.28.19. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 4.28.20. Deve suportar a captura de pacotes (PCAP), por assinatura de Malware, ou assinatura de IPS ou aplicação;
- 4.28.21. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 4.28.22. Os eventos devem identificar o país de onde partiu a ameaça;
- 4.28.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
- 4.28.24. Bloquear proativamente os ataques sofisticados recém-descobertos em tempo real com IA e serviços avançados de proteção contra ameaças;
- 4.28.25. Proteção contra downloads involuntários usando HTTP de arquivos executáveis.
- 4.28.26. Rastreamento de vírus em pdf.
- 4.28.27. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)

4.29. **FILTRO DE URL**

- 4.29.1. Deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 4.29.2. Deve possuir a função de exclusão de URLs do bloqueio;
- 4.29.3. Deve permitir a customização de página de bloqueio;
- 4.29.4. Deverá permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
- 4.29.5. A solução de segurança deve possuir a capacidade de bloquear o envio de credenciais corporativas para sites maliciosos;
- 4.29.6. A solução deve possuir mecanismos de fazer bloqueio de tipos de arquivos para upload e download, assim evitando exposição de arquivos básicos da infraestrutura.

4.29.7. Deve permitir controlar o envio de credenciais corporativas somente para categorias de URLs permitidas;

4.29.8. Deve prover análise em tempo real de páginas maliciosas e dessa forma permitir a proteção em tempo real antes mesmo da atualização das bases de dados de URLs;

4.30. **PREVENÇÃO DE AMEAÇAS AVANÇADAS (ZERO DAY)**

4.30.1. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

4.30.2. Deve ser capaz de enviar para análise, arquivos tipo Executáveis, DLLs, Arquivos de Código e MSI;

4.30.3. A solução deve detectar e bloquear em tempo real (inline) os artefatos maliciosos desconhecidos (zero day) no próprio GW através de mecanismos de Machine Learning. Não serão aceitas soluções que utilizem equipamentos externos;

4.30.4. Suportar a análise dinâmica de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional, Windows 10, Mac OS X, Android, Linux;

4.30.5. A análise de links em sandbox deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

4.30.6. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

4.30.7. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

4.30.8. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

4.30.9. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência;

4.30.10. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

4.30.11. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

4.30.12. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

4.30.13. Permitir o envio de arquivos para análise no ambiente controlado de forma automática, podendo ser via API;

4.30.14. Implementar, identificar e bloquear malwares de dia zero que trafegam pela rede;

4.30.15. As funcionalidades de sandbox tem como objetivo, analisar e bloquear em tempo real de Ameaças Avançadas Persistentes - APT. Essas funcionalidades têm o objetivo de proteger o ambiente contra a entrada de malwares não conhecidos, e para que ela seja efetiva é necessário que a inspeção e bloqueio sejam feitas em linha (inline), através de features de machine learning;

4.30.16. Deve permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus da solução;

4.30.17. A solução deve analisar os arquivos do tipo malware em bare metal para evitar técnicas de evasão. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.

4.30.18. Deve prevenir contra ataques sem arquivo buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: Powershell e Javascript;

4.30.19. Deve ser capaz de aplicar de forma complementar às assinaturas de antivírus a inspeção inline através de Machine learning em tempo real arquivos tipo PE (portable executable) e Arquivos Microsoft Office, bem como, scripts PowerShell e shell script em tempo real para malwares desconhecidos.

4.31. IDENTIFICAÇÃO DE USUÁRIOS

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

4.31.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle / políticas baseadas em usuários e grupos de usuários;

4.31.3. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários;

4.31.4. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle / políticas baseadas em Usuários e Grupos de usuários;

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

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

4.31.7. Suporte a autenticação Kerberos;

4.31.8. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;

4.31.9. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

4.31.10. O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos à organização;

4.31.11. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

4.32. SEGURANÇA DE DNS

4.32.1. solução deve mostrar nos logs as seguintes informações sobre domínios DGA (Domain Generation Algorithm):

- a) Domínio suspeito identificado;
- b) ID de assinatura de detecção;

- c) Usuário logado na estação/servidor que originou o tráfego;
Aplicação;
- d) Porta de destino;
- e) IP de origem;
- f) Horário;
Ação do firewall;
- g) Severidade;
- h) A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

4.33. **QoS**

4.33.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

4.33.2. Suportar a criação de políticas de QoS por:

- a) Endereço de origem;
- b) Endereço de destino;
- c) Por usuário e grupo do LDAP/AD;
- d) Por aplicações;
- e) Por porta;

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

- a) Banda Garantida;
- b) Banda Máxima;
- c) Fila de Prioridade.

4.33.4. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

4.33.5. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

4.33.6. Deve implementar QOS (traffic-shaping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inbound e outbound);

4.33.7. Disponibilizar estatísticas RealTime para classes de QoS.

4.33.8. Deve suportar QOS (traffic-shaping), em interface agregadas;

4.33.9. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

4.34. **VPN**

4.34.1. A solução de VPN client-to-site deverá ser atendido apenas para o equipamento do tipo II;

4.34.2. Suportar VPN Site-to-Site e Client-To-Site;

4.34.3. Suportar IPSec VPN;

4.34.4. Suportar SSL VPN;

4.34.5. A VPN IPSEC deve suportar:

- a) 3DES;

- b) Autenticação MD5 e SHA-1;
- c) Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
- d) Algoritmo Internet Key Exchange (IKEv1 e v2);
- e) AES 128 e 256 (Advanced Encryption Standard);
- f) Autenticação via certificado IKE PKI.

4.34.6. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

4.34.7. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

4.34.8. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

4.34.9. Deve suportar a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;

4.34.10. Deve suportar a aplicação de políticas de segurança e visibilidade para as aplicações que circulem dentro dos túneis SSL;

4.34.11. O cliente da solução de VPN client-to-site deve suportar a instalação nos seguintes tipos de sistema operacionais:

- a) Microsoft Windows;
- b) Apple macOS e IOS;
- c) Android;
- d) Linux.

4.34.12. A solução de VPN client-to-site deve estar devidamente licenciada para criar perfis customizados de conformidade dos clientes das VPNs client-to-site para no mínimo as seguintes opções:

- a) Sistema operacional;
- b) Antivírus instalado;
- c) Firewall no host;
- d) Chaves de registros (quando aplicável);
- e) Processos ativos.

4.34.13. Os mecanismos de conformidade da solução de VPN client-to-site deverá monitorar durante a conexão do usuário remoto qualquer tipo de atividade não autorizada pelo administrador em tempo real. Por exemplo: Após o usuário ser conectado e admitido pela VPN client-to-site, o seu acesso ao ambiente corporativo pode ser negado caso ele manualmente desative alguma funcionalidade especificada nos testes de conformidade da solução;

4.34.14. Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;

4.35. **ANALÍTICOS**

4.35.1. Configuração dos NGFW referente a versão do Software, modelo do equipamento e a saúde do equipamento;

4.35.2. Utilização das subscrições de Segurança apresentando o que possui licenciamento expirado;

4.35.3. Recomendação de ações e/ou comandos via CLI para remediar os gaps de segurança;

4.35.4. Visibilidade de alertas de segurança de forma consolidada;

- 4.35.5. Alertas de hardware e limites de configuração;
- 4.35.6. Identificação e notificação de anormalidades no estado geral de funcionamento da solução;

4.36. **RELATÓRIOS**

- 4.36.1. A plataforma de segurança deverá possuir relatório de avaliação de boas práticas por meio de análise das configurações atuais;
- 4.36.2. O relatório de boas práticas deverá mostrar o estado atual da solução e a adoção de práticas recomendadas de segurança com sugestões de adequações específicas alinhadas com práticas recomendadas;
- 4.36.3. O relatório deverá mostrar onde melhorar a postura de segurança e definir uma linha de base para comparação posterior, fornecendo links para documentação técnica que mostram como configurar as recomendações;
- 4.36.4. Além de mostrar um comparativo de boas práticas das configurações atuais e posteriores, o relatório deverá apresentar na comparação o grau de boas práticas adotado por instituições do setor público ou similares;
- 4.36.5. O relatório deverá possuir avaliação de melhores práticas recomendadas com base no CIS (Critical Security Controls) e do NIST Security Controls (National Institute of Standards and Technology) sobre as configurações atuais da solução, identificando os riscos e fornecendo recomendações. Exemplo: A solução deverá apontar quais são as configurações que deverão ser ajustadas e indicar local com exemplo de configuração a ser realizada para melhorar a adoção e elevar o grau de segurança;
- 4.36.6. A avaliação de práticas recomendadas deverá mostrar a adoção de recursos de segurança como por exemplo a porcentagem de adoção de regras por usuários e por aplicações;
- 4.36.7. Deverá mostrar informações de adoção da solução, apontando configurações individuais para verificar como os recursos de segurança estão sendo aproveitados. Exemplo: Análise da base de regras para identificar se as mesmas estão sendo aproveitadas e se são relevantes;
- 4.36.8. O relatório poderá ser emitido diretamente na solução ou por meio de portal WEB do fabricante da solução.

5. **ITEM 04 - SISTEMA DE GERÊNCIA CENTRALIZADA COM ARMAZENAMENTO DE LOGS CONSOLE DE GERÊNCIA, MONITORAÇÃO E RELATORIA**

- 5.1. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possui todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual deve ser compatível com com Hyper-V e VMware ESXi;
- 5.2. Caso a solução de gerenciamento, monitoração e relatoria, possua licenciamento relacionado a armazenamento, este deve ser entregue com a maior capacidade suportada ou ilimitada sem a necessidade de licenciamento adicional;
- 5.3. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos;
- 5.4. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.
Controle sobre todos os equipamentos da plataforma de segurança

em uma única console, com administração de privilégios e funções;

5.5. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;

5.6. 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;

5.7. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;

5.8. 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;

5.9. Deve permitir a criação de objetos e políticas compartilhadas;

5.10. Deve consolidar logs e relatórios de todos os dispositivos administrados;

5.11. Deve permitir que exportar backup de configuração automaticamente via agendamento;

5.12. 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;

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

5.14. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

5.15. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

5.16. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;

5.17. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;

5.18. O gerenciamento deve permitir/possuir:

5.18.1. Criação e administração de políticas de firewall e controle de aplicação;

5.18.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

5.18.3. Criação e administração de políticas de Filtro de URL;

5.18.4. Monitoração de logs;

5.18.5. Ferramentas de investigação de logs;

5.18.6. Debugging;

5.18.7. Captura de pacotes;

5.18.8. Acesso concorrente de administradores.

5.19. Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;

5.20. Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou

nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;

5.21. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

5.22. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;

5.23. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;

5.24. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;

5.25. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

5.26. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

5.27. Autenticação integrada ao Microsoft Active Directory e servidor Radius;

5.28. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

5.29. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

5.30. Criação de regras que fiquem ativas em horário definido;

5.31. Criação de regras com data de expiração;

5.32. Backup das configurações e rollback de configuração para a última configuração salva;

5.33. Suportar Rollback de Sistema Operacional para a última versão local;

5.34. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

5.35. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;

5.36. Deve suportar interface de configuração baseada no padrão Openconfig, podendo ser feito por meio de utilização de API fornecido pelo fabricante.

5.37. Validação de regras antes da aplicação;

5.38. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.

5.39. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.

5.40. Validação da políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

5.41. Deve possuir mecanismo interno ou externo que permita que as configurações ainda não instaladas sejam mantidas mesmo na ocasião de uma reinicialização não esperada.

5.42. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem

ou conflitem com outras (shadowing);

5.43. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.

5.44. Deve permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação à versão anterior;

5.45. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);

5.46. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

5.47. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

5.48. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;

5.49. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

5.50. Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day" detectados em sand-box e tráfego bloqueado;

5.51. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

5.52. Deve permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela.

5.53. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

5.54. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;

5.55. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

5.56. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;

5.57. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;

5.58. Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;

5.59. Deve ser possível exportar os logs em CSV;

5.60. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

5.61. Rotação do log;

5.62. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

5.63. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;

5.63.1. Situação do dispositivo e do cluster;

5.63.2. Principais aplicações;

5.63.3. Principais aplicações por risco;

5.63.4. Administradores autenticados na gerência da plataforma de segurança;

5.63.5. Número de sessões simultâneas;

5.63.6. Status das interfaces;

5.63.7. Uso de CPU;

5.64. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

5.64.1. Resumo gráfico de aplicações utilizadas;

5.64.2. Principais aplicações por utilização de largura de banda de entrada e saída;

5.64.3. Principais aplicações por taxa de transferência de bytes;

5.64.4. Principais hosts por número de ameaças identificadas;

5.65. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;

5.66. Deve permitir a criação de relatórios personalizados;

5.67. Gerar alertas automáticos via:

5.67.1. Email;

5.67.2. SNMP;

5.67.3. Syslog;

6. ITEM 05 - SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO

6.1. Refere-se ao serviço de instalação física e lógica para 02 (dois) appliances para a composição do Item 01 e de 01 (um) appliance para o caso do Item 02 desta contratação, sua configuração em modo de alta disponibilidade, configuração de seu sistema operacional, ativação de seus módulos e respectivas licenças de uso, configuração de regras de segurança baseadas tanto nas regras implementadas na solução de Firewall utilizada hoje no CONTRATANTE quanto em novas regras a serem especificadas neste item, assim como em regras acordadas posteriormente entre a equipe técnica do CONTRATANTE e da CONTRATADA, incluindo a migração dos clientes de VPN ativos na solução Firewall utilizada hoje no ambiente para a nova solução Firewall NGFW, além da migração da solução atual de filtro de conteúdo Web Squid/LightSquid, para a solução de filtro de URL disponível pela nova solução de Firewall NGFW.

6.2. Os serviços de instalação deverão ser realizados pela CONTRATADA sob acompanhamento da equipe de infraestrutura do CONTRATANTE, conforme projeto apresentado pela CONTRATADA e aprovado pelo CONTRATANTE, atendendo todos os requisitos e

exigências constantes deste Termo de Referência e demais anexos, além de seguir as orientações do fabricante e melhores práticas relacionadas ao uso de equipamentos similares em ambientes críticos.

6.3. O processo de implantação deverá ser devidamente documentado pela CONTRATADA ao longo de todo o período de execução. Ao fim do processo a CONTRATADA deverá apresentar um relatório com o detalhamento da implantação, contendo todas as etapas, histórico de mudanças, diagramas e detalhamento da estrutura da solução, procedimentos adotados, configurações efetuadas e resultado dos testes e homologação;

6.4. A entrega deste relatório é obrigatória, sendo este o principal artefato comprobatório de conclusão da execução do serviço, a ser utilizado pela equipe técnica de contratação para validação do serviço e emissão do Termo de Recebimento Definitivo da solução.

7. ITEM 06 - TREINAMENTO "HANDS ON" SOBRE A SOLUÇÃO DE FIREWALL

7.1. Treinamento oficial do fabricante com repasse de conhecimento específico sobre a solução instalada para, no mínimo, 05 (cinco) servidores/ colaboradores indicados pela CONTRATADA, conforme requisitos e demais exigências especificadas neste Termo de Referência e demais documentos anexos.

7.2. O treinamento deverá oferecer material didático de apoio gratuito aos participantes, seja por meio de mídia física (livros, apostilas, etc.) ou digital (PDF). O material deverá ser cedido individualmente a cada participante, de modo que ele possa levar consigo e consultá-lo posteriormente;

7.3. O treinamento deverá abranger tanto teoria quanto exercícios práticos, voltados para conhecimento da arquitetura da solução, sua implantação, configuração e gerenciamento, além de tratamento de problemas típicos envolvendo a operação da solução;

7.4. O escopo básico do treinamento deverá conter:

- 7.4.1. Arquitetura da solução;
- 7.4.2. Configurações iniciais básicas;
- 7.4.3. Alta disponibilidade;
- 7.4.4. Controle de acesso dos administradores da solução;
- 7.4.5. Configuração de Interfaces;
- 7.4.6. Criação e gerenciamento de Zonas de Segurança, Políticas de Segurança e Endereçamento NAT; Controle por Identificação de Aplicações;
- 7.4.7. Controle por Identificação de Usuários, com conexão a fontes externas de autenticação; Criação e gerenciamento de Filtro URL;
- 7.4.8. Decriptografia de tráfego;
- 7.4.9. Configurações de VPN (SSL e IPSec);
- 7.4.10. Monitoramento e Relatórios;
- 7.4.11. Logging e Auditoria;

7.5. Ao final do treinamento, deverá ser emitido certificado comprobatório da participação de cada participante do treinamento.

7.6. A apresentação destes certificados é requisito obrigatório para a comprovação da execução do serviço, sendo o principal artefato a ser utilizado pela equipe técnica de contratação para validação do serviço e emissão do Termo de Recebimento Definitivo da solução.



Documento assinado eletronicamente por **Jaime Heleno Correa de Lisboa, Subsecretário(a) de Tecnologia da Informação e Inovação**, em 03/11/2023, às 10:36, conforme horário oficial de Brasília, com fundamento no art. 30, inciso II, da Portaria nº 26/2016, de 01/04/2016, do Ministério da Cultura, Publicada no Diário Oficial da União de 04/04/2016.



A autenticidade deste documento pode ser conferida no site https://sei.cultura.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1485263** e o código CRC **220B02E7**.

Referência:Processonº 01400.000997/2023-52

SEI nº 1485263