# ESTUDO TÉCNICO PRELIMINAR

Instrução Normativa SGD/ME nº 01, de 04/04/2019.

## Aquisição de solução para mitigação de ataques do tipo DoS/DDoS e serviços agregados

**Ministério da Educação**

**Secretaria Executiva**

**Subsecretaria de Tecnologia da Informação e Comunicação**

**Brasília/DF, 18 de outubro de 2021.**

# Índice

# Anexos

# 1 Objetivo

O Estudo Técnico Preliminar da Contratação é documento que descreve as análises realizadas em relação às condições da contratação em termos de necessidades, requisitos, alternativas, escolhas, resultados pretendidos e demais características, e que demonstra a viabilidade técnica e econômica da contratação e integra a fase de Planejamento da Contratação de Soluções de Tecnologia da Informação e Comunicação - conforme regulamentado pela Instrução Normativa n° 01, de 04 de abril de 2019[1], da Secretaria de Governo Digital do Ministério da Economia, e suas atualizações.

No presente documento, a Equipe de Planejamento da Contratação - ora designada pelo Ofício nº 117/2021/GAB/CGLC/SAA-MEC, de 06 de maio de 2021 - dedica-se a analisar aspectos fundamentais relacionados à demanda em questão, tais como: adequação técnica; funcionalidades e requisitos; adequação às normas vigentes; modelos de execução; capacidade do mercado; estimativa preliminar de custos e viabilidade econômico-financeira do objeto.

| Versionamento | | |
|---|---|---|
| **Versões** | **Descrição** | **Data** |
| 1.0 | Primeira versão consolidada pela Equipe de Planejamento da Contratação | 18/10/2021 |

# 2 Descrição da demanda

Trata-se de demanda da Coordenação-Geral de Infraestrutura e Segurança da Informação - CGIS para Aquisição de solução para a mitigação de ataques de Negação de Serviços (DoD/DDoS) para o centro de processamento de dados do Ministério da Educação – conforme detalhado no Documento de Oficialização da Demanda (2474971 - Processo 23000.002559/2021-11). A Equipe de Planejamento da Contratação (EPC) foi instituída pelo Ofício nº 117, não sendo verificada a acumulação de papéis e nem a participação da autoridade de TIC em sua composição de Serviços de Tecnologia da Informação.

## 2.1 Identificação das necessidades de negócio

A segurança da informação está entre os principais itens de discussão das organizações governamentais, motivados, essencialmente, pelo crescente número de diferentes ataques cibernéticos destinados a portais e serviços entregues pelo Governo Brasileiro.

As corporações que fazem uso ou oferecem serviços através da Internet ou por outras redes parceiras devem ter um extremo cuidado com esse canal, pois apesar dos grandes benefícios, permitindo conectividade em abrangência global, representa também, em contrapartida, risco potencial para infestações e recebimentos de artefatos desnecessários, maliciosos e mal-intencionados.

Por sustentar os principais sistemas educacionais do país, o ambiente de TIC do MEC é altamente crítico, para tanto é fundamental manter a infraestrutura necessária para desenvolver com segurança e confiabilidade as atividades deste Ministério.

Com foco na melhoria da segurança dos serviços tecnológicos prestados a entidades internas e externas, visando propiciar à Administração Pública uma consecução mais econômica e vantajosa de seus fins, além do contínuo aperfeiçoamento de Governança de TI no setor público, especificamente a assuntos referentes a segurança da informação, o MEC aponta como essencial

Atualmente o MEC possui uma solução de AntiDDoS adquirida por meio do contrato nº 17/2017 (SEI 23000.042716/2016-55) e que se encontra instalada e em produção em seu datacenter. Esta solução possui como características a combinação de técnicas de detecção de ameaças e mitigação de ataque DDoS para bloqueá-lo e também para manter o time de segurança/rede informado sobre o tráfego malicioso. Em razão do final da garantia e suporte desta solução e, ainda, considerando a defasagem tecnológica da atual solução propõe-se nova contratação visando manter e atualizar esse tipo de proteção. Vale ressaltar que o fim dessa cobertura da garantia e do suporte deixa o ambiente tecnológico do MEC vulnerável a ataques cibernéticos, sem rastreabilidade e sem contramedidas.

Essas questões influenciam na capacidade de gestão e resposta a eventos de Segurança da Informação visto que o MEC é custodiante de uma extensa base de dados de terceiros e que a luz da LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em setembro de 2020 e do PDA – Plano de Dados Abertos e a lei n° 12.965/2014 - Marco Civil da Internet, o MEC, no caso concreto, deve seguir para se evitar o acesso a informações pessoais e ao uso indevido dessas informações.

A exemplo temos o recente caso da identificação dos responsáveis pelo desvio (fraude) da ordem de 1 bilhão de reais no sistema FIES pelo FNDE e que foi amplamente noticiado na mídia jornalística:

- https://veja.abril.com.br/educacao/esquema-de-fraude-no-mec-envolveu-invasao-e-espionagem/
- https://veja.abril.com.br/educacao/a-fraude-de-r-1-bilhao-no-fies/
- https://www.metropoles.com/brasil/educacao-br/mec-suspeita-que-fraude-no-fies-pode-ser-maior-que-r-1-bilhao
- https://www.correiobraziliense.com.br/euestudante/ensino-superior/2021/02/4906339-mec-solicita-investigacao-a-cgu-e-policia-federal-acerca-de-fraudes-no-fies.html

[1] Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/instrucao-normativa-sgd-me-no-1-de-4-de-abril-de-2019-versao-compilada

- https://agenciabrasil.ebc.com.br/educacao/noticia/2021-02/ministerio-da-educacao-anuncia-investigacao-de-fraudes-no-fies
- https://g1.globo.com/educacao/noticia/2021/02/12/fraudes-no-fies-sao-investigadas-diz-ministerio-da-educacao.ghtml

O processo está referenciado no Plano Diretor de Tecnologia da Informação e Comunicações – PDTIC conforme abaixo:

| Plano Diretor de Tecnologia da Informação (PDTIC 2021 - 2023) | |
|---|---|
| **Objetivo(s) estratégico(s)** | **Necessidade(s) vinculada(s)** |
| Iniciativa Estratégica 4D - Prover soluções adaptativas de segurança da informação Evoluir a arquitetura e as soluções de segurança da informação de forma adaptativa ao nível de ameaças – através de processos de previsão, prevenção, detecção e resposta | Aquisição de Solução de Segurança contra ataques do Tipo DDoS (Distributed Denial of Service |

Podemos descrever que o MEC tem como necessidade de negócio garantir um controle eficiente na gestão de incidentes de segurança, com origem em eventos de plataformas de segurança já contratadas (Se estendendo também a novas contratações). A ferramenta deverá prover meios para coleta, armazenamento, correlacionamento e contextualização de todos os incidentes de segurança gerados no ambiente, contando também com validação contínua de efetividade de controles de segurança, permitindo a realização de testes automáticos e contínuos quanto à postura das soluções de segurança e contra ataques cibernéticos reais.

Tecnicamente, pelo cenário complexo atual no que tange segurança cibernética e orientações gerais do governo federal, a cada dia que passa surgem inúmeros artefatos maliciosos, vulnerabilidades conhecidas, técnicas comuns de ataque, entre outros. Na medida que os avanços tecnológicos fornecem novos incríveis meios de realizar/facilitar atividades cotidianas, pessoas mal-intencionadas trabalham para explorar e se aproveitar de brechas que surgem e muitas das vezes não são notadas. Baseado nisso o MEC busca soluções de eficiência comprovada, provendo a integração eficiente entre todos os itens necessários para funcionamento adequado.

Apenas acrescentando informações referenciadas em um normativo recente e importante, seguem alguns trechos do Decreto nº 10.222, de 5 de fevereiro de 2020[2]:

> *1.2. INTRODUÇÃO*
>
> *Em decorrência da presente Estratégia, recomenda-se que cada órgão do setor público e do setor privado, planeje e realize gestões no sentido de colocar em prática os aspectos que lhe cabem e que estão estabelecidos nas ações estratégicas, em um esforço conjunto e dedicado, em prol do pleno alcance dos objetivos estratégicos do País, no crítico e atual tema da segurança cibernética nacional.*
>
> *2.3. AÇÕES ESTRATÉGICAS*
>
> *2.3.3. Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade. Promover um ambiente participativo, colaborativo e seguro, entre as organizações públicas, as instituições privadas, a academia e a sociedade, por meio do acompanhamento contínuo e proativo das ameaças e dos ataques cibernéticos, com o objetivo de:*
>
> *- realizar exercícios cibernéticos com participação de múltiplos atores;*
>
> *- fortalecer o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov e mantê-lo atualizado em pessoal e material;*
>
> *- ressaltar o papel dos Centros de Tratamento e Resposta a Incidentes Cibernéticos - CSIRTs nacionais;*
>
> *- aperfeiçoar a infraestrutura nacional de investigação de crimes cibernéticos;*
>
> *- incentivar a criação e a atuação de equipe de tratamento e resposta aos incidentes cibernéticos - ETIRs, com ênfase no uso de tecnologias emergentes;*
>
> *- emitir alertas e recomendações;*
>
> *2.3.4. Elevar o nível de proteção do Governo*
>
> *Elevar o nível de proteção do Governo, por meio de ações no campo cibernético, a exemplo de:*
>
> *- aperfeiçoar e manter atualizados os sistemas informacionais, as infraestruturas e os sistemas de comunicação dos órgãos públicos, em relação aos requisitos de segurança cibernética;*

[2] Disponível em https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419

*- elaborar requisitos específicos de segurança cibernética relativos ao uso de endpoints nas organizações públicas, aqui entendidos, em suma, como equipamentos finais conectados a um terminal de alguma rede ou a algum sistema de comunicação;*

*- monitorar a implementação dos requisitos mínimos de segurança cibernética pelos fornecedores que integram a cadeia de suprimentos.*

*2.3.5. Elevar o nível de proteção das Infraestruturas Críticas Nacionais*

*Proporcionar às infraestruturas críticas, maior resiliência que possibilite a contínua prestação de serviços essenciais, por meio das seguintes ações:*

*- incentivar que essas organizações implementem políticas de segurança cibernética, que contemplem, dentre outros aspectos, métricas, mecanismos de avaliação, e de revisão periódica;*

*- incentivar a constituição de ETIRs;*

*- estimular que as infraestruturas críticas notifiquem o CTIR Gov dos incidentes cibernéticos; e*

*- incentivar a participação das infraestruturas críticas em exercícios cibernéticos.*

*2.3.6. Aprimorar o arcabouço legal sobre segurança cibernética*

*Para aprimorar o arcabouço legal sobre segurança cibernética, revisar e atualizar os normativos existentes, abordar novas temáticas e elaborar novos instrumentos. Nesse sentido, podem ser adotadas as seguintes ações como:*

*- identificar e abordar temas ausentes na legislação vigente;*

*- criar políticas de incentivo para contratação de mão de obra especializada em segurança cibernética;*

*- definir requisitos de segurança cibernética nos programas de trabalho remoto;*

*2.3.10. Elevar o nível de maturidade da sociedade em segurança cibernética*

*Elevar o nível de maturidade em segurança cibernética da sociedade, com o fim de ensejar a compreensão das ameaças e dos riscos no espaço cibernético, e possibilitar às pessoas o uso adequado e oportuno de procedimentos e de ferramentas em prol da utilização segura do ambiente digital. Nesse sentido, identificam-se como iniciativas:*

*- incentivar a formação de profissionais para atuar no combate aos crimes cibernéticos;*

*PARTE I*

*DIAGNÓSTICO*

*[...] Ao todo, 57,4% dos ataques foram realizados por meio de phishing, enquanto, em segundo plano, ficaram os golpes com publicidade suspeita, que somaram 19,2% dos casos.*

*Os dados dessa pesquisa demonstram que as empresas brasileiras, principalmente aquelas consideradas como infraestruturas críticas, precisam considerar a segurança cibernética como ação prioritária de investimentos, elaborar planos de gestão de riscos e de tratamento e resposta a incidentes, assim como planejar orçamento adequado para combater os incidentes de segurança. Em mais da metade das empresas ouvidas no levantamento da Tempest/EZ-Security15, o orçamento anual de segurança da informação representa até 2% do faturamento anual. Em 34,5% dessas empresas, esse percentual não ultrapassa 1%, de acordo com a mesma pesquisa.*

*Um ataque cibernético de grande envergadura, caso não seja adequadamente tratado, pode afetar profundamente a reputação da organização, ocasionar perda de receitas, levar a prejuízos operacionais com a paralização dos serviços, resultar em perda de informações e ainda levar à aplicação de sanções legais e administrativas.*

*PARTE II*

*ANÁLISE DOS EIXOS TEMÁTICOS*

*Com vistas a auxiliar a formulação das ações estratégicas, foram analisados, primeiramente, os eixos temáticos que pertencem à área de proteção e de segurança, que são: a governança da segurança cibernética nacional, o universo subconectado e seguro, a prevenção e mitigação de ameaças cibernéticas, e a proteção estratégica. Em seguida, foram abordados os eixos temáticos transformadores, assim denominados pelo potencial que possuem em modificar, de forma decisiva e estruturante, os temas por*

*eles influenciados. São eles: a dimensão normativa, a pesquisa, desenvolvimento e inovação, a dimensão internacional e parcerias estratégicas, e a educação.*

*1.3. Proteção Estratégica*

*"O País encontra-se em pleno processo de digitalização de serviços públicos, o que confere progressiva criticidade às redes e aos sistemas de governo, que apoiam a prestação desses serviços ao cidadão. Observa-se o mesmo processo com relação às estruturas de comunicação entre os entes governamentais, cujo nível de proteção deve ser adequado e proporcional à sua relevância."*

*"Para dar suporte efetivo à E-Digital e ao mesmo tempo conferir proteção cibernética aos sistemas de gestão e aos sistemas utilizados pelas repartições públicas, é necessário reduzir a vulnerabilidade das organizações governamentais contra qualquer tipo de ameaça cibernética, ao proporcionar à administração pública níveis adequados de segurança e de resiliência contra ataques cibernéticos."*

*"Em relação à proteção das redes e dos sistemas governamentais, em virtude da crescente integração de serviços, de bases de dados e de plataformas digitais, nota-se o aumento das vulnerabilidades, que podem ser exploradas por hackers. Nesse sentido, destaca-se que o Governo deve empregar recursos para que a segurança cibernética seja implementada e adequada à proteção de suas estruturas computacionais, para que a prestação de serviços ao cidadão não sofra solução de continuidade. Ressalta-se que esses recursos devem compor um conjunto estruturado de investimentos em conhecimento, em políticas, em profissionais e em tecnologias, dentre outros."*

*"Os dispositivos móveis funcionais, conectados à internet e utilizados com frequência por autoridades públicas, podem ser alvos de ilícitos cibernéticos, e merecem atenção, especialmente no caso dos órgãos que permitem, em suas políticas de segurança, a utilização desses equipamentos na modalidade conhecida como BYOD, sigla de Bring Your Own Device ou traga seu próprio dispositivo, em que o administrador do sistema permite a conexão, à rede do órgão, de um equipamento particular.*

*Nesse ponto, considera-se vital a segurança de endpoints, nome pelo qual são conhecidos, na área de rede de computadores, os dispositivos finais que estão conectados em um terminal de rede. Trata-se, portanto, de qualquer dispositivo que esteja conectado em uma rede, interna ou externa."*

*"Por isso, esses endpoints devem ser escopo de um conjunto de medidas que visem bloqueá-los contra ameaças cibernéticas e mantê-los livres de ataques. Ao bloquear os terminais de rede, a segurança de endpoint impede que brechas e vulnerabilidades dos dispositivos conectados sejam utilizadas por hackers para invadir e roubar dados corporativos."*

*"A preocupação e as ações de proteção voltadas aos endpoints são plenamente justificáveis, dado o crescimento de ameaças cibernéticas sobre eles. Segundo o AVTEST, mais de nove milhões de novos casos de malware são observados por mês, tendo por alvo não apenas os sistemas Windows®, mas também o macOS®, o Linux e o Android®."*

*"Outro ponto que se tem destacado dentre as preocupações de segurança cibernética do Governo refere-se aos ataques sofisticados e direcionados às cadeias de suprimentos. Um ataque à cadeia de suprimentos (Supply Chain Attack, em Inglês), ocorre quando há infiltração em um sistema por meio de um fornecedor, de uma empresa parceira ou de um provedor externo com acesso a sistemas e a dados. Esse tipo de ataque, em geral, causa perdas financeiras e reflete negativamente na imagem dos fornecedores, de forma a levar à perda de confiança e a afetar profundamente os negócios."*

*"A proteção às infraestruturas críticas, por sua relevância, merece abordagem específica. Segundo o estudo "2018 Cost of Data Breach Study: Global Overview", realizado pela IBM em parceria com o Instituto Ponemon, observou-se, em 2018, um aumento de 350% em ataques de ransomware, verificou-se uma expansão de 250% em ataques de spoofing ou de comprometimento de e-mail comercial e constatou-se um acréscimo de 70% em ataques de spear-phishing nas empresas de modo geral."*

*"Por isso, essas organizações necessitam de meios para identificar, proteger, detectar, avaliar, responder, recuperar e assim gerenciar o risco das ameaças cibernéticas, e também de ferramentas de automação de segurança que usam inteligência artificial e aprendizado de máquina, que permitam analisar, identificar e conter os ataques cibernéticos."*

*"Os principais tipos de ameaças contra as infraestruturas críticas são ataques de phishing, negação de serviço em larga escala, vazamentos de informações privadas ou institucionais, espionagem cibernética e a interrupção de serviços."*

O objeto desse Estudo Técnico, conforme já informado anteriormente, visa adquirir solução para a mitigação de ataques de Negação de Serviços (DoS/DDoS) para o centro de processamento de dados do Ministério da Educação. Esse Estudo atende ao decreto citado acima que estabelece a estratégia nacional de segurança cibernética, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e, ainda, contribuindo também para um avanço muito grande para a estratégia de ampliação de maturidade de segurança da informação do MEC e disponibilidade/qualidade dos serviços de tecnologia ofertados.

Dessa forma a pretendida contratação visa gerar insumos para suprir as necessidades expostas nestas perguntas de forma com que a maturidade de segurança da informação do MEC possa crescer dia após dia, ampliando o nível de estabilidade e confiabilidade de todos os serviços tecnológicos disponibilizados, assumindo uma postura proativa e não reativa quanto ao cenário de ameaças cibernéticas atual.

## 2.2 Identificação das necessidades tecnológicas e Análise do Cenário Atual

Conforme bem descrito no item 2.1 desse estudo, mesmo sendo um grande custodiante de informações sensíveis de terceiros, o MEC não possui uma solução de correlacionamento de eventos e gestão. Cabe destacar que além da custódia dessas informações o MEC possui, em seu portfólio de serviços disponíveis para a sociedade, 4 (quatro) grandes sistemas tratados como programas. São eles: o Sistema Nacional de Seleção Unificado - SISU, que tem por objetivo selecionar os candidatos às vagas das instituições públicas de ensino superior que utilizarão a nota do Exame Nacional do Ensino Médio (ENEM) como critério para o processo seletivo, o Programa Universidade para Todos - PROUNI, que tem por objetivo a concessão de bolsas de estudo integrais e parciais em cursos de graduação e sequenciais de formação específica, em instituições privadas de educação superior, o Programa de Financiamento Estudantil – FIES, destinado a financiar a graduação na educação superior de estudantes matriculados em cursos superiores não gratuitos na forma da Lei 10.260/2001 e o Sistema Nacional de Informações da Educação Profissional e Tecnológica - SISTEC. Esses sistemas são os grandes consumidores dos dados sensíveis de terceiros e que, por uma característica própria, são utilizados seja na validação de dados, seja na inclusão/atualização desses mesmos dados. Cabe para o MEC manter esses sistemas e base de dados em ambiente restrito e protegido, com vistas a possibilitar a rastreabilidade de acesso a essas informações.

Estes programas têm sua dinâmica de uso fortemente ligada à infraestrutura tecnológica uma vez que o principal meio de interação com a população se dá por meio de portais e sistemas acessíveis via internet. Tal disposição de acesso traz os inúmeros benefícios de disponibilidade e facilidade de acesso que somente sistemas disponibilizados via internet trazem ao processo, no entanto, com a facilidade e dinamicidade trazidas pelo acesso online, são gerados também riscos cibernéticos que variam do acesso indevido à informações restritas ou ainda de indisponibilidade dos sistemas devido à eventos adversos que podem ser gerados à partir de ações orquestradas de entidades maliciosas, como hackers ou grupos com interesses diversos que divergem das políticas públicas implantadas pelo Ministério da Educação.

Nesse contexto, como a base de funcionamento desses sistemas são dados pessoais de terceiros, dentre outros tipos de dados, as questões relacionadas a proteção desses dados torna o desafio ainda maior. Não obstante, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em setembro de 2020, o PDA – Plano de Dados Abertos e a lei n° 12.965/2014 - Marco Civil da Internet, são os instrumentos legais que buscam estabelecer regras para acesso a informações pessoais e ao uso indevido dessas informações. Esses normativos foram aprimorando os regramentos anteriores trazendo para os tempos atuais as regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas. Aquelas instituições que não cuidam dos dados estão suscetíveis a sanções que podem variar podendo chegar a multas pesadíssimas. Dessa forma, como o objetivo de proteger os dados pessoais dos usuários da Rede MEC e, ainda, atender ao disposto nos dispositivos legais supra é preciso investir em ferramentas e recursos tecnológicos para segurança da informação.

Ao contrário do que parece, a LGPD não se aplica apenas a empresas do segmento de tecnologia, mas a qualquer uma, tanto no setor público quanto no privado, desde que haja manipulação de dados de usuários, esta Lei se aplica. No MEC, por exemplo, todo corpo docente, discente e administrativo possui cadastro de seus dados pessoais para uso nos diversos sistemas do Ministério. A base LDAP e o Active Directory alimentam os principais sistemas, ali, concentra informações que vão desde o nome completo, e-mail, telefone, endereço, matrícula, data de nascimento e outras diversas informações importantes para o Ministério. Em outro eixo temos as cargas completas das bases de CPF e CNPJ oriundas das bases da Receita Federal.

Um simples vazamento de informações pessoais de qualquer usuário, por exemplo, pode acarretar severas sanções administrativas e/ou criminais que não é favorável para a imagem desta instituição.

E é fato que atualmente existe uma crescente ação de usuários mal-intencionados que visam acessos indevidos a dados para obter informações privilegiadas. No MEC, casos de ataques de negação de serviço, tentativas de interrupção de sistemas e indisponibilizar a infraestrutura são frequentes e devem ser mitigados.

Por essa razão a aquisição de uma solução que possibilite gerir e bloquear as ações de tentativa de negação de serviço (DoS/DDoS) é de grande relevância para o MEC.

O MEC possui uma solução que atende a essa necessidade, contrato nº 19/2018, porém sem cobertura contratual que proporcione suporte técnico e atualização.

## 2.3 Identificação dos requisitos necessários e suficientes à escolha da solução

São requisitos mínimos necessários à escolha da solução, aqui consideradas como premissas da área requisitante:

- Prover solução de segurança da informação moderna e eficiente;
- Prover solução de segurança que disponibilize as condições plenas para a execução das ações do MEC embasadas em Tecnologia da Informação, com performance, segurança e disponibilidade adequadas, garantindo à infraestrutura de TI a capacidade adequada para melhor atender as necessidades de negócio do Ministério da Educação;
- Prover solução de segurança da informação capaz de detectar, bloquear e notificar tráfego malicioso para os administradores da rede;
- Prover solução de segurança robusta, capaz de atender as demandas sazonais do negócio;
- Prover solução de segurança que permita a criação de serviços de segurança da informação que suportem os programas e políticas do Ministério.

## 2.4 Estimativa do volume de bens e/ou serviços da demanda

Esse tipo de solução é composta por hardware e software **entregues em appliances** (servidores de processamento dedicados) além de suporte técnico especializado para atualização, suporte e garantia para 60 (sessenta) meses. Abaixo a volumetria necessária para sustentar o ambiente do MEC.

| Descrição | Quantidade |
|---|---|
| Quantidade de tráfego SUJO a ser mitigado pela solução | 40 Gbps ou 27M PPS |
| Quantidade de tráfego LIMPO a ser encaminhado pela solução | 10 Gbps |
| Quantidade de links de 10 Gbps a serem protegidos pela solução | 2 |

Cumpre esclarecer que o serviço de Operação Assistida é de fundamental importância para o MEC em virtude do calendário anual dos programas críticos (SISU, PROUNI e FIES). Sempre que se abrem as inscrições e outras atividades relacionadas à disponibilização desses sistemas para a população é preciso um acompanhamento presencial em virtude da quantidade de problemas relacionados a ataques de indisponibilidades, falsos positivos e outras ocorrências que podem interferir seriamente na disponibilidade desses sistemas. Para solicitar a demanda pela operação assistida é preciso emitir um Ordem de Serviço detalhando a necessidade.

Para se definir o volume de horas necessárias para o serviço de operação assistida levantamos todas as OS de demanda de Operação Assistida do **contrato nº 19/2018**, conforme abaixo:

| Ano | Quantidade | Valor Unitário | Valor Total | Nº Os | Nº Sei |
|---|---|---|---|---|---|
| 2018 | 156 | 378 | 58968 | 1 | 23000.020138/2018-68 |
| 2019 | 150 | 378 | 56700 | 2 | 23000.001253/2019-14 |
| 2019 | 200 | 378 | 75600 | 3 | 23000.014399/2019-20 |
| 2020 | 150 | 378 | 56700 | 4 | 23000.001672/2020-90 |
| 2020 | 50 | 378 | 18900 | 76 | 23000.019221/2020-17 |
| 2021 | 100 | 378 | 37800 | 01/2021 | 23000.000471/2021-56 |
| 2021 | 24 | 378 | 9072 | 02/2021 | 23000.011536/2021-99 |
| 2021 | 72 | 378 | 27216 | 03/2021 | 23000.017590/2021-48 |

Desta forma, considerando o exercício de 2021, foi adicionada uma Ordem de Serviço de Operação Assistida relacionada com o calendário PROUNI Remanescentes (OS 02/2021).

Considerando, então, que em 2019, maior utilização de horas, 350 horas (OSs 2 e 3) utilizamos essa estimativa 350 horas e acrescentamos mais 14% como uma folga de eventual crescimento. Como se trata de quantidade anual chegamos a possibilidade de demandar um total de 400 horas anuais. Cumpre destacar que a utilização dessas horas é estimativa podendo ou não serem utilizadas em sua totalidade.

# 3 Identificação e análise de soluções

A análise comparativa de soluções, nos termos do inc. II do art. 11 da IN-01/2019/SGD, visa a elencar as alternativas de atendimento à demanda considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

Durante o levantamento de possíveis soluções foram identificados 2 (duas) alternativas para a contratação em tela:

| Mapa comparativo da análise de custos totais de propriedade | | |
|---|---|---|
| **Alternativa** | **Descrição da alternativa ou cenário identificado** | **Item** |
| A | Substituição da solução implantada | 3.1.1 |
| B | Extensão da garantia, manutenção e suporte técnico para a solução vigente | 3.1.2 |

## 3.1 Análise comparativa das alternativas para o atendimento da demanda

Para o atendimento da demanda em estudo foram identificadas as alternativas levantadas no item anterior, abaixo segue análise qualitativa e técnica.

### 3.1.1 Alternativa A: Substituição da solução implantada

Nesta alternativa consideramos a substituição da solução implantada, com o intuito de atualizar o parque tecnológico do MEC com uma solução mais robusta, compreendendo a garantia e suporte técnico da mesma, zelando-se pela disponibilidade contínua dos serviços ofertados pela Secretaria de Tecnologia da Informação (STIC) para todo o Ministério da Educação. Desta forma, propomos a aquisição de novos equipamentos, em linha de produção do fabricante, com garantia pelo período de 60 (sessenta) meses. Esta opção permite ao MEC fazer a gestão autônoma da plataforma de mitigação de ataques do tipo DoS/DDoS, sincronizando a detecção de ameaças da mesma com equipamentos semelhantes de fornecedores externos, que disponibilizam links de acesso à internet para este Ministério em contratos vigentes. Esta gestão granular da solução permite um maior refinamento das políticas e regras de detecção de ameaças e uma gestão proativa de possíveis incidentes de segurança da informação.

Cabe ressaltar que nesta opção não buscamos apenas a substituição displicente da solução vigente, mas também a atualização dos recursos disponíveis. Por exemplo, os modelos 2600/2800 implementados no MEC utilizam uma tecnologia de PCI e barramento de 2015. Na atualização dessas especificações a tecnologia de barramento, PCI, drivers e comutadores de tráfego usam a versão 2020. Ou seja, é a evolução natural da tecnologia de motherboard, discos e processadores.

Destacamos também que o equipamento atual (AED 2800) possui um Maximum DDoS Flood Prevention Rate de 28.8 Mpps enquanto a nova contratação apresenta um limite de 38.9Mpps. A nova contratação prevê o suporte a interfaces de 40Gbps com bypass integrado enquanto o equipamento atual possui interfaces de 10Gbps. O equipamento especificado nesta contratação suporta 40 Gbps de ataque independente da licença atribuída, e o atual equipamento do MEC possui o limite de 10Gbps.

Além dos aspectos em nível de hardware a nova solução propõe a adição de novas funcionalidades e assinaturas se comparado ao modelo atual. Essas novas funcionalidades acompanham às mais recentes técnicas utilizadas para promover ataques DDoS.

Por se tratar de uma solução semelhante à **ALTERNATIVA B**, as vantagens e desvantagens aqui descritas estão restritas a esta forma de aquisição.

| VANTAGENS | DESVANTAGENS |
|---|---|
| ▪ Substituição da solução com serviços de atualização, suporte e garantia;<br>▪ Operada e gerenciada pela força de trabalho existente no MEC (servidores efetivos e terceiros oriundos contrato de nº 03/2020/MEC com a empresa Globalweb);<br>▪ Não existe a necessidade de adequação de espaço físico para recebimento de equipe externa;<br>▪ Em comparação à alternativa "B" esse modelo demanda menos esforço de fiscalização de gestão contratual;<br>▪ Menor custo a longo prazo. | ▪ A curto prazo o valor empregado na contratação é maior; |

Diante do exposto, e visto que essa alternativa supre a principal motivação da contratação, qual seja: gerir e bloquear as ações de tentativa de negação de serviço (DoS/DDoS), garantindo assim a segurança e a disponibilidade dos serviços e da infraestrutura tecnológica do MEC por meio de nova solução para a mitigação de ataques de Negação de Serviços (DoD/DDoS), entendemos que esta alternativa é tecnicamente viável.

### 3.1.2 Alternativa B: Extensão da garantia, manutenção e suporte técnico para a solução vigente

Nesta alternativa vislumbramos a possibilidade de renovação do serviço de suporte técnico e garantia, por determinado período, para os atuais equipamentos implantados no Datacenter do MEC. Estes equipamentos foram adquiridos por meio do contrato nº 19/2018 (SEI nº 23000.042716/2016-55), e os serviços adjacentes findaram em agosto de 2021. Desta forma, a solução implantada atualmente não possui mais o suporte técnico da contratada e a garantia do fabricante, criando-se desta forma um risco crítico na infraestrutura de TIC do Ministério da Educação. Importante ressaltar neste ponto que a solução atual também encontra-se obsoleta, já que está classificada como "EoS - End of Sale" pelo fabricante. Além disto, estes equipamentos utilizam tecnologia de barramento de comunicação PCI Express v4, datado de 2015 e já ultrapassado. De maneira simplificada, um barramento pode ser definido como um conjunto de linhas de comunicação que permitem a interligação entre dispositivos, como a CPU, a memória RAM e outros periféricos de um computador, caracterizando-se como linhas de transmissão capazes de trocar informações entre estes componentes. Desta forma, quanto maior a capacidade de transmissão de um barramento, melhor será o desempenho geral dos equipamentos. A última versão estável desta tecnologia é a PCI Express v5, anunciada em Maio de 2019, com capacidade de largura de banda, em modo full duplex, de até 128Gb/s. Desta forma, como a demanda de processamento e transmissão de dados do Datacenter do MEC é cada vez maior, com a agregação constante de novos serviços, é necessário que as ferramentas subjacentes acompanhem esta demanda. A seguir apresentamos as vantagens e desvantagens desta alternativa:

| VANTAGENS | DESVANTAGENS |
|---|---|
| ▪ Manter os mesmos equipamentos já instalados no Datacenter do MEC;<br>▪ Curva de aprendizagem na solução baixo; | ▪ Alto custo apenas com renovação da garantia e do suporte se comparado a aquisição de nova solução, Alternativa A, com 5 anos de garantia e suporte.<br>▪ Manter em produção uma solução defasada tecnologicamente;<br>▪ Equipamento já listado como EoS (End of Sales) pelo Fabricante; |

A proposta de contratação de suporte e manutenção para solução implantada foi identificada com uma das alternativas para se manter a continuidade da solução de mitigação de ataques do tipo DDoS, da Central de Processamento de Dados do MEC, com garantia e suporte técnico, entretanto, a presente solução não demonstra ser viável, posto que os equipamentos em uso no MEC, já possuem mais de 3 (três) anos e meio de utilização, ou seja, já estão em fase inicial de obsolescência, considerando o ciclo de vida de 5 (cinco) anos, conforme orientação da Secretaria de Logística e Tecnologia da Informação do MPOG, atual Secretaria de Governo Digital, por meio da **Portaria nº 20/2016**, que dispõe sobre orientações para contratação de soluções de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional.

Assim, quando os equipamentos chegam na fase de fim do ciclo de vida devem ser observados os seguintes pontos críticos:

- A probabilidade de defeitos é elevada, causando indisponibilidades e prejudicando as atividades diárias da instituição;
- O fornecedor poderá ter dificuldade de provimento de peças de reposição, aumentando o risco descumprir os níveis de serviço exigidos para reparo dos equipamentos;
- O fabricante deixa de liberar quaisquer versões de manutenção de software finais ou correções de bugs;
- O fabricante deixa de analisar falhas de rotina que podem ser realizados para determinar a causa da falha do produto de hardware ou defeito;
- Ajuste de SLA para o reparo ou substituição de ativo antigo, em decorrência da dificuldade de se conseguir peças.

De forma geral a contratação 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. Assim, os contratos de manutenção têm seus custos elevados na medida em que os bens 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 de o fornecedor descumprir os níveis de serviço exigidos para reparo desses equipamentos.

Assim, diante do exposto observa-se que de acordo com os pontos levantados a escolha de manter os equipamentos atuais com uma contratação de manutenção e suporte apresentam sérios riscos ao negócio, demonstrando ir na contramão dos princípios balizadores das contratações públicas, quais sejam: eficiência, eficácia e economicidade.

Pelo exposto, não seria conveniente ou oportuna a manutenção da solução implantada, cujo contratos de suporte técnico e garantia já estão vencidos. Em vista disso, principalmente pelos fatos de não proporcionar a evolução tecnológica, expor a infraestrutura de rede a maior risco de indisponibilidade e ir de encontro às orientações do SISP, conclui-se que a presente alternativa não é tecnicamente adequada, apesar de ser viável.

## 3.2 Alternativas para o modelo de contratação

### 3.2.1 Estratégia A: realização de licitação própria

Considerando as alternativas elencadas nos itens 3.1.1 e 3.1.2 a demanda da área requisitante pode ser atendida através da realização de procedimento licitatório para contratação da solução pretendida, de acordo com as disposições da IN-01/2019/SGD, da

Lei 8.666/1993 e demais instrumentos legais aplicáveis. A consecução dessa estratégia envolve três etapas: o planejamento da contratação, a seleção do fornecedor e a execução contratual.

### 3.2.2 Estratégia B: contratação conjunta ou mediante sistema de registro de preços

Quanto à adoção do SISTEMA DE REGISTRO DE PREÇOS, A Lei n° 8.666/1993, em seu inc. II do art. 15, estabelece que "as compras, sempre que possível, deverão ser processadas através de sistema de registro de preços" – assim definido como o "conjunto de procedimentos para registro forma de preços relativos à prestação de serviços e aquisição de bens para contratações futuras" (Decreto n° 7.892/2013, art. 1°, I). À luz do princípio da eficiência, o SRP tem por escopo instrumentalizar meios para aquisição parcelada de bens e serviços pela Administração Pública, sendo, portanto, compatível com a modalidade Pregão Eletrônico (Lei nº 10.520/02, art. 11). Ainda, de acordo com o disposto no Decreto n° 7.892/2013, a utilização do Sistema de Registro de Preços enquadra-se nas seguintes hipóteses:

> *"Art. 3- O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:*
> *I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;*
> *II – quando o for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;*
> *III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo: ou*
> *IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.*
> *Por outro lado, de acordo com o art. 16 do Decreto nº 7.892/2013, a existência de preços registrados não obriga a Administração Pública a contratar, facultando-se a realização de licitação específica para a aquisição pretendida, assegurada preferência ao fornecedor registrado em igualdade de condições."*

Dessa forma, após análise das especificações técnicas e realização de pesquisa de preços de mercado, consideramos ADEQUADA a estratégia de utilização do Sistema de Registro de Preços, já que a aquisição dos bens e serviços previstos neste estudo, poderão ocorrer em momentos distintos, de acordo com a disponibilidade orçamentária.

## 4 Análise comparativa de custos

A análise comparativa de custos foi elaborada considerando apenas as soluções técnica e funcionalmente viáveis, nos termos do inc. III art. 11 da IN-01/2019/SGD, e inclui:

a) comparação de custos totais de propriedade (*Total Cost Ownership* – TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia, manutenção; e

b) memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados.

O detalhamento dos cálculos realizados está contido no documento de pesquisa de preços, que segue incorporado ao processo administrativo 23000.002559/2021-11, sendo também referenciado no **ANEXO B**.

**Mapa comparativo da análise de custos totais de propriedade**

| Alternativa | Descrição da alternativa ou cenário identificado | TCO global |
|---|---|---|
| A | Substituição da solução implantada | R$ 5.002.409,33 |
| B | Extensão da garantia, manutenção e suporte técnico para a solução vigente | R$ 4.554.693,83 |

### 4.1 Memória de cálculo das soluções viáveis

### 4.1.1 Alternativa A: Substituição da solução implantada

Para viabilizar o cálculo comparativo dos custos totais de propriedade utilizamos como referência principal a cotação de valores com o mercado especializado no fornecimento de soluções desta natureza. Esse fato deu-se principalmente pela ausência de preços públicos na ferramenta Painel de Preços, dentro dos moldes propostos nesta alternativa, de acordo com os parâmetros de pesquisa utilizados. Desta forma, a parcela relevante da contratação (item 1) foi determinada primordialmente por preços privados, respeitando-se as previsões contidas no Inc. IV Do Art. 5° Da In-73/2020/Seges. Para os demais itens (2 e 3), foram considerados preços públicos e privados. O quadro abaixo apresenta a tabela resumo com o TCO para a alternativa em análise:

| TCO - Alternativa A | | | | | |
|---|---|---|---|---|---|
| **Item** | **Descrição** | **Métrica** | **Quantidade** | **Valor unitário** | **Total global** |
| 1 | Solução de mitigação de ataques de negação de serviço (DoS/DDoS) | Unidade | 1 | R$ 4.765.229,95 | R$ 4.765.229,95 |
| 2 | Serviço de implantação, instalação, configuração e transferência de conhecimento | Unidade | 1 | R$ 91.218,49 | R$ 91.218,49 |
| 3 | Serviço de operação assistida | Horas | 400 | R$ 364,90 | R$ 145.960,89 |
| | | | | **Total Global Estimado:** | **R$ 5.002.409,33** |

### 4.2 Alternativa B: Extensão da garantia, manutenção e suporte técnico para a solução vigente

De maneira semelhante à alternativa anterior, para viabilizar o cálculo comparativo dos custos totais de propriedade para esta alternativa, utilizamos como referência principal a cotação de valores com o mercado especializado no fornecimento de soluções desta natureza, sendo encontrado apenas um preço público compatível com a alternativa. Destacamos, porém, que em ambos os casos (preços públicos e privados), os valores dos itens 1 e 2 contêm o prazo de garantia e suporte limitado ao período de 36 (trinta e seis) meses apenas e não 60 (sessenta) meses, conforme necessidade primária do projeto. Isto ocorre porque a extensão da garantia e suporte técnico da solução aqui analisada está limitada a este período pelo fabricante, uma vez que a mesma já encontra-se em fase de "end-of-sale", conforme aludido no item 3.1.2 deste estudo técnico. Desta forma, para que fosse possível realizar uma comparação adequada com a alternativa A, projetamos o valor dos itens 1 e 2, para 60 meses, como forma de exercício dos valores estimados, mesmo que este prazo de garantia e suporte já não seja possível, devido à restrição citada.

No que tange à contratação pública utilizada como parâmetro de referência para compor o preço de cada item, deve-se considerar que os valores refletem exclusivamente as condições conhecidas no edital, não sendo possível afirmar que tanto os equipamentos descritos, quanto o volume de serviços, sejam plenamente compatíveis com aqueles aqui almejados, assim como não é possível compreender, através da pesquisa de preços, o cenário interno e as necessidades específicas do Órgão contratante. Portanto, considerando que as diversas soluções podem variar em termos de especificações, os valores devem ser entendidos como simples estimativas utilizadas para a construção de cenários hipotéticos.

O quadro abaixo apresenta a tabela resumo com o TCO para a alternativa em análise:

| TCO - Alternativa B | | | | | |
|---|---|---|---|---|---|
| **Item** | **Descrição** | **Métrica** | **Quantidade** | **Valor unitário** | **Total global** |
| 1 | Subscrição de garantia e suporte para a solução Arbor Edge Defense, por 60 meses<br>Modelo: Netscout Arbor AED APS 2800 –10 S/N CG23726010HA | Unidade | 1 | R$ 3.589.023,97 | R$ 3.589.023,97 |
| 2 | Suporte técnico especializado mensal para a solução Arbor Edge Defense, por 60 meses | Unidade | 1 | R$ 819.708,98 | R$ 819.708,98 |
| 3 | Serviço de operação assistida | Horas | 400 | R$ 364,90 | R$ 364,90 |
| | | | | **Total Global Estimado:** | **R$ 4.554.693,83** |

### 4.3 Registro das soluções inviáveis

De acordo com o presente estudo, todas as alternativas elencadas foram consideradas tecnicamente viáveis, sendo calculado seus respectivos custos totais de propriedade, conforme previsão contida no inciso III, Art. 11 da Instrução Normativa nº 01 de 04 de Abril de 2019.

## 5 Descrição e justificativas da solução escolhida

Após a análise comparativa das soluções identificadas a alternativa viável, economicamente mais vantajosa para a Administração e recomenda pela equipe de planejamento da contratação, é a seguinte:

*Alternativa A - aquisição de nova solução para mitigação de ataques de negação de serviço (DoS/DDoS) e serviços agregados de implantação, instalação, configuração, operação assistida, garantia e suporte técnico dos equipamentos – de acordo com as especificações técnicas e condições previstas no Termo de Referência.*

## 5.1 Composição da solução

Para atendimento da necessidade a presente contratação deverá ser composta pelos bens e serviços descritos na tabela a seguir:

| Composição da solução | | | | |
|---|---|---|---|---|
| **Item** | **Descrição** | **Unidade** | **Catmat/Catser** | **Estimativa de volume** |
| 1 | Solução de mitigação de ataques de negação de serviço (DoS/DDoS) | Unidade | 133132 | 1 |
| 2 | Serviço de implantação, instalação, configuração e transferência de conhecimento | Unidade | 27111 | 1 |
| 3 | Serviço de operação assistida | Horas | 26999 | 400 |

## 5.2 Justificativa da escolha da solução

Uma vez que buscamos uma solução que, além de garantir a economicidade, reduza a indisponibilidade e garanta a eficiência dos serviços disponibilizados pela STIC, ao Ministério da Educação, a extensão da garantia, suporte técnico e manutenção para solução implantada atualmente, não se configura como uma escolha tecnicamente vantajosa, tendo em vista os riscos apontados na análise da solução no item 3.1.2, bem como o fato de ser um opção que usualmente é mais onerosa para a Administração, não apenas em termos econômicos, quando comparada à aquisição do ativo com garantia e suporte técnico adequados, dentro do seu prazo de vida útil.

Neste momento é importante salientar que, de acordo com os valores apresentados no TCO de cada alternativa, é possível verificar sob a ótica meramente de custos que a ALTERNATIVA B seria a melhor opção para a Administração, já que a mesma apresenta uma variação percentual a menor, de aproximadamente 9%, quando compara à ALTERNATIVA A, implicando em uma possível economia na ordem de R$ 447.715,49 (quatrocentos e quarenta e sete mil, setecentos e quinze reais e quarenta e nove centavos). Citamos, entretanto, que não buscamos apenas a solução mais barata, mas aquela que, a longo prazo, atenderá as necessidades deste Ministério, em termos de atualização tecnológica, disponibilidade e escalabilidade.

Ressaltamos ainda o fato de que a composição da estimativa de preços das alternativas foi determinada primordialmente por preços cotados com fornecedores, dada a ausência de contratações públicas recentes, nos modelos propostos neste estudo. Desta maneira, como forma de exercitar os preços de soluções similares da Administração Pública, para fins de comparação hipotética, elencamos os contratos destacados no quadro abaixo, contendo aquisições realizadas nos mesmos moldes da alternativa A, incluindo alguns contratos do próprio MEC. Apesar da vigência da maioria destes já ter expirado, o que torna as referências inválidas, considerando as disposições contidas no inciso II do Art. 5° da Instrução Normativa nº 73, de 5 de agosto de 2020, atualizamos os valores dos contratos de acordo com a variação do dólar para o período analisado, para fins de comparação.

Mesmo considerando este fator, a aquisição de uma solução atualizada tecnologicamente ainda caracteriza-se como vantajosa para a Administração, visto que a variação percentual de valor para soluções semelhantes, adquiridas em editais passados, não representam um grande "gap de fuga" dos preços estimados para a ALTERNATIVA A, que apresenta um menor valor na quase totalidade das ocorrências. O detalhamento da projeção do valor dos contratos abaixo, em dólares, pode ser verificado no **ANEXO D.**

| Órgão | Contrato | Projeção do Valor Estimado da Solução | Variação % em relação à Alternativa A |
|---|---|---|---|
| Ministério de Minas e Energia | 08-2013 | R$ 4.952.887,29 | -1% |
| Inep | 12-2018 | R$ 5.913.758,59 | 15,41% |
| Inep | 16-2015 | R$ 5.677.247,49 | 11,89% |
| Inep | 34-2017 | R$ 5.945.821,14 | 15,87% |
| Ministério da Educação | 67-2014 | R$ 6.714.188,15 | 25,49% |
| Ministério da Educação | 19-2018 | R$ 5.515.850,61 | 9,31% |

Além dos aspectos elencados acima, utilizados como critério de escolha da melhor solução, também citamos as disposições contidas no item **1.2, *"aquisição de ativos com garantia versus contratação de serviços de manutenção"***, do documento de **boas**

**práticas, orientações e vedações para contratação de ativos de TIC - versão 4**[3], do MP/STI, anexo da Portaria MP/STI nº 20/2016, que prevê o seguinte:

> *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 manutenidos 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 de o 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. (grifo nosso)*

O referido documento tem força normativa legal, estando vinculado à **Portaria MP/STI nº 20, de 14 de junho de 2016**, na forma de anexo, tendo sido assinado, em sua última versão, pelo então Secretário de Tecnologia da Informação do Ministério do Planejamento, Desenvolvimento e Gestão em 22/03/2017 e publicado em 23/03/2017.

Em contrapartida, na Alternativa A, buscamos a substituição da solução implantada com a aquisição de um novo produto. Esta proposta, além de atender às recomendações legais, estabelece padrões de qualidade, com vistas ao ganho na eficiência e economicidade para a Administração Pública. Desta forma, buscando-se realizar o melhor atendimento possível às necessidades tecnológicas do MEC, considerando a situação crítica do Órgão em relação aos aspectos até então apresentados, o Guia de Boas Práticas de Contratação de Ativos de TI, e o fato de que os equipamentos atuais já encontram-se fora da garantia, na iminência do fim de sua vida útil, optamos neste estudo pela **Alternativa A**, concluindo-se que esta opção será aquela que melhor atenderá os requisitos da contratação, sendo técnica e economicamente vantajosa para a Administração.

## 5.3 Garantia técnica

Esse requisito tem por finalidade central buscar garantir que a empresa contratada entregue serviços com alto nível de qualidade, uma vez que ela própria será responsável por corrigir todas as falhas em seus produtos enquanto perdurar sua relação contratual com a área requisitante. A CONTRATADA deverá prestar a GARANTIA TÉCNICA pelo prazo de **60 (sessenta) meses**, para equipamentos, itens 1, 2 e 3, a contar da data do Termo de Recebimento Definitivo. A identificação e a comunicação de defeitos dos produtos deverão ser efetuadas dentro do período de GARANTIA TÉCNICA, devendo a totalidade dos defeitos reportados ser corrigida pela CONTRATADA, ainda que a conclusão do serviço extrapole esse período.

## 5.4 Enquadramento legal e normativo

A natureza do objeto a ser adquirido enquadra-se na classificação de bens comuns, nos termos do parágrafo único do art. 1° da Lei 10.520, de 2002. Classifica-se o objeto deste Termo de Referência, também, como bens ou serviços de informática, nos termos do Decreto nº 7.174/2010, para fins de definição dos critérios de sua aceitação quando da fase externa da licitação.

## 5.5 Da Vigência contratual

Considerando as características de cada grupo/lote da contratação, a respectiva vigência contratual está fixada de acordo com o seguinte:

A vigência inicial do CONTRATO será de **12 (doze) meses**, contados a partir da data de assinatura, com previsão de prorrogação apenas para os serviços de operação assistida (**item 3**), por iguais e sucessivos períodos de 12 (doze) meses até o limite de 60 (sessenta) meses, conforme art. 57, inciso II, da Lei n° 8.666/1993.

O término da vigência do contrato não exonera a CONTRATADA de sua responsabilidade em promover e assegurar a assistência técnica da garantia, estando sujeita, na hipótese do descumprimento da responsabilidade assumida e mesmo depois de expirada a vigência do contrato, às penalidades previstas neste Termo de Referência, sem prejuízo de eventual responsabilidade civil e penal.

### 5.5.1 Das alterações contratuais

Nos termos da legislação em vigor, durante a fase de execução da prestação dos serviços, o CONTRATO poderá ser alterado, desde que justificadamente, na forma e nos limites previstos no art. 65 da Lei nº 8.666, de 1993. As alterações contratuais devem ser

[3] Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/orientacoes_ativos-de-tic-v-4.pdf

promovidas mediante celebração de termo aditivo, que deverá ser submetido à prévia aprovação da consultoria jurídica do CONTRATANTE.

Considerando o disposto no Orientação Normativa AGU nº 50 (atualizada pela Portaria nº 140, de 26 de abril de 2021[4]), os acréscimos e as supressões do objeto contratual devem ser sempre calculados sobre o valor inicial do contrato atualizado, aplicando-se de forma isolada os limites percentuais previstos em lei ao conjunto de acréscimos e supressões, vedada a compensação de acréscimos e supressões entre itens distintos, não se admitindo que a supressão de quantitativos de um ou mais itens seja compensada por acréscimos de itens diferentes ou pela inclusão de novos itens.

No âmbito do mesmo item, o restabelecimento parcial ou total de quantitativo anteriormente suprimido não representa compensação vedada, desde que sejam observadas as mesmas condições e preços iniciais pactuados, não haja fraude ao certame ou à contratação direta, jogo de planilha, nem descaracterização do objeto, sendo juridicamente possível, além do restabelecimento, a realização de aditamentos para novos acréscimos ou supressões, observados os limites legais para alterações do objeto em relação ao valor inicial e atualizado do contrato.

### 5.6 Especificação técnica da solução

As especificações técnicas, os requisitos da contratação, o modelo de execução e os requisitos dos serviços, estão descritos na minuta de TERMO DE REFERÊNCIA, que integra o presente processo de planejamento da contratação.

### 5.7 Justificativa do quantitativo a ser contratado

Os quantitativos definidos para cada item da contratação foram definidos de acordo com o quadro abaixo:

| Item | Descrição | Qtde. | Justificativa |
|---|---|---|---|
| 1 | Solução de mitigação de ataques de negação de serviço (DoS/DDoS) | 1 | Necessidade de substituir o atual equipamento |
| 2 | Serviço de implantação, instalação, configuração e transferência de conhecimento | 1 | Serviços necessários para a implantação da solução |
| 3 | Serviço de operação assistida | 400 horas | Considerando o histórico de demandas do contrato vigente, conforme apontado no item 2.4 deste estudo, estimou-se uma média de 350 horas de serviço técnico, acrescentando-se uma folga de 14% sobre este valor. Destacamos que a utilização destas horas é estimativa e não representa obrigatoriedade de consumo por parte da Administração |

### 5.8 Parcelamento ou não parcelamento da solução

A equipe de planejamento da contratação avaliou a viabilidade de realizar o parcelamento da solução de TIC a ser contratada, porém, tal parcelamento não se mostrou técnica e economicamente viável. Uma vez que, dentre outros aspectos detalhados no Estudo Técnico Preliminar, o agrupamento de elementos que compõem a mesma solução representa a melhor estratégia da Administração quando a adjudicação de itens isolados onera o "o trabalho da administração pública, sob o ponto de vista do emprego de recursos humanos e da dificuldade de controle, colocando em risco a economia de escala e a celeridade processual", vide o ACÓRDÃO Nº 5301/2013 – TCU – 2ª Câmara, além de representar risco à integração da solução e ao atingimento dos benefícios da contratação. Diante de todo o exposto, fica assegurado o interesse público e justifica-se a inviabilidade do parcelamento do objeto.

### 5.9 Escolha do regime de execução

A equipe de planejamento da contratação entender ser a **EMPREITADA POR PREÇO GLOBAL** o regime de execução mais adequado para o objeto pretendido e o tipo e critério de julgamento da futura licitação, o **MENOR PREÇO** por lote, para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratações de bens e serviços de informática.

De acordo com o Art.1º do Decreto nº10.024/2019, a futura licitação deverá ser realizada na modalidade de Pregão, preferencialmente na sua forma eletrônica, com julgamento pelo critério de menor preço por lote. A fundamentação pauta-se na premissa de que a aquisição dos bens e a prestação dos serviços elencados neste estudo, baseiam-se em padrões de desempenho e qualidade claramente definidos por meio de especificações usuais de mercado, havendo diversos fornecedores capazes de fornecê-los e prestá-los, caracterizando-os como "bens e serviços comuns", de acordo com a previsão contida no Art. 9º, §2º do Decreto 7.174/2010.

O processo licitatório NÃO será destinado exclusivamente à participação de microempresas e empresas de pequeno porte, conforme preceitua o art. 6º do Decreto nº 8.538, de 6 de outubro de 2015, que regulamenta o tratamento favorecido, diferenciado e simplificado para estas entidades, pois o valor estimado para o lote pretendido é superior a R$ 80.000,00 (oitenta mil reais), também não aplicando-

[4] Disponível em: https://www.in.gov.br/web/dou/-/portaria-agu-n-140-de-26-de-abril-de-2021-316016680

se o benefício referente à cota exclusiva para microempresas e empresas de pequeno porte, pois o lote se trata de uma única solução, sendo impossível subdividi-la, devido à necessidade de compatibilização de todos os seus componentes/serviços.

### 5.10 Classificação dos bens e/ou serviços a serem contratados

No que concerne os bens e serviços que compõe a solução, em conformidade com o art. 1° da LEI N° 10.520/2002, para fins de avaliação da aplicabilidade do DECRETO N° 10.024/2019, o objeto pretendido enquadra-se como **BEM E/OU SERVIÇO COMUM** por apresentar, independentemente de sua complexidade, "padrões de desempenho e qualidade objetivamente definidos em edital, por meio de especificações usuais no mercado".

De acordo com os entendimentos estabelecidos na Nota Técnica n° 02/2008 SEFTI/TCU, "devido à padronização existente no mercado, os bens e serviços de tecnologia da informação geralmente atendem a protocolos, métodos e técnicas pré-estabelecidos e conhecidos e a padrões de desempenho e qualidade que podem ser objetivamente definidos por meio de especificações usuais no mercado. Logo, via de regra, esses bens e serviços devem ser considerados comuns para fins de utilização da modalidade Pregão" [...] "Em geral, nem a complexidade dos bens ou serviços de tecnologia da informação nem o fato de eles serem críticos para a consecução das atividades dos entes da Administração descaracterizam a padronização com que tais objetos são usualmente comercializados no mercado. Logo, nem essa complexidade nem a relevância desses bens e serviços justificam o afastamento da obrigatoriedade de se licitar pela modalidade Pregão".

### 5.11 Forma de seleção do fornecedor

Considerando a natureza dos bens e/ou serviços pretendidos, o disposto no §1° do art. 1° do DECRETO N° 10.024/2019 e o disposto no § único do art. 26 da INSTRUÇÃO NORMATIVA SGD/ME N° 01, de 04 de abril de 2019, a licitação será realizada na modalidade **PREGÃO ELETRÔNICO** do tipo **MENOR PREÇO GLOBAL** observando, como critério de julgamento, o valor por **LOTE/GRUPO**. Quanto aos modos de disputa, assim define o art. 31 do Decreto n° 10.024/2019:

> *Art. 31. Serão adotados para o envio de lances no pregão eletrônico os seguintes modos* de disputa:
> *I - aberto - os licitantes apresentarão lances públicos e sucessivos, com prorrogações, conforme o critério de julgamento adotado no edital; ou*
> *II - aberto e fechado - os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado, conforme o critério de julgamento adotado no edital.*
> *Parágrafo único. No modo de disputa aberto, o edital preverá intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.*

Assim, embora ressalvada a competência da área administrativa para decidir sobre tal ponto, recomendamos que seja adotado o **modo de disputa aberto**, uma vez que em nossa visão este propicia maior grau de disputa:

> *Art. 32. No modo de disputa aberto, de que trata o inciso I do caput do art. 31, a etapa de envio de lances na sessão pública durará dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.*
> *§ 1º A prorrogação automática da etapa de envio de lances, de que trata o caput, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive quando se tratar de lances intermediários.*
> *§ 2º Na hipótese de não haver novos lances na forma estabelecida no caput e no § 1º, a sessão pública será encerrada automaticamente.*
> *§ 3º Encerrada a sessão pública sem prorrogação automática pelo sistema, nos termos do disposto no § 1º, o pregoeiro poderá, assessorado pela equipe de apoio, admitir o reinício da etapa de envio de lances, em prol da consecução do melhor preço disposto no parágrafo único do art. 7º, mediante justificativa.*

#### 5.11.1 Requisitos de qualificação técnica do fornecedor

Para efeito de qualificação técnica, a LICITANTE deve demonstrar sua aptidão e capacidade técnico-operacional para a execução do OBJETO mediante comprovação de prestação bem-sucedida de serviços em características e quantidades compatíveis com a presente licitação, mediante apresentação de um ou mais **ATESTADO (S) DE CAPACIDADE TÉCNICA** que deverão comprovar o atendimento aos seguintes requisitos:

Comprovação de aptidão para o fornecimento de bens em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

A critério do CONTRATANTE, nas situações em que julgar necessário, poderão ser realizadas inspeções e diligências com a finalidade de entender, esclarecer e/ou comprovar as informações contidas no (s) **ATESTADO (S) DE CAPACIDADE TÉCNICA** entregue (s) – nos termos do §3°do art. 43 da Lei n° 8.666/1993. Assim como poderão ser solicitadas cópias de documentos complementares

como contratos, notas fiscais e notas de empenho. Porém, não serão executadas diligências para acrescentar informações obrigatórias ausentes no (s) atestado (s) apresentado (s).

A eventual recusa do (s) emitente (s) do (s) ATESTADO (S) em prestar esclarecimentos e/ou fornecer documentos comprobatórios, ou sofrer diligências, ou a constatada inexatidão das informações atestadas, desconstituirá o (s) ATESTADO (S) – o que poderá, inclusive, configurar prática criminosa, ensejando comunicação ao Ministério Público Federal e abertura de Processo Administrativo Disciplinar, conforme o caso, para fins de apuração de responsabilidades.

No caso de atestados emitidos por empresas privadas, **não serão admitidos** aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial[5] da empresa proponente. São consideradas como pertencentes ao mesmo grupo empresarial as empresas controladas ou controladoras da CONTRATADA proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócia ou possua vínculo com a empresa emitente. Ainda, com respeito aos ATESTADOS DE CAPACIDADE TÉCNICA:

a) Devem estar relacionados ao objeto da licitação;
b) Devem ser pertinentes e compatíveis às características, quantidades e prazos exigidos na licitação;
c) Poderão ser fornecidos por pessoas jurídicas de direito público ou privado, com correta identificação do emissor;
d) Devem ser emitidos sem rasuras, acréscimos ou entrelinhas;
e) Devem estar assinados por quem tenha competência para expedi-los, tais como representantes legais do órgão/empresa, diretores, gerentes e representantes formais das áreas técnica ou demandante (sem se limitar a esses);
f) Devem conter identificação clara e suficiente do Atestante;
g) Devem apresentar redação clara, sucinta e objetiva que demonstre de forma inequívoca o atendimento ao objeto da requisição.

Convém destacar que, na análise dos atestados de capacidade técnica, o CONTRATANTE primará pela finalidade precípua da exigência, qual seja: a demonstração de que os licitantes possuem condições técnicas para executar o objeto pretendido pela Administração caso venha a sagrar-se vencedor da licitação. Assim, preservada a aderência aos ditames legais e constitucionais fundamentais, o exame documental balizar-se-á nos princípios da razoabilidade, da proporcionalidade e do formalismo moderado – o que, por óbvio, não significa que serão admitidos quaisquer informalismos.

### 5.11.2 Requisitos da garantia contratual

O adjudicatário prestará GARANTIA DE EXECUÇÃO DO CONTRATO, nos moldes do art. 56 da Lei nº 8.666/1993, com validade durante a execução do CONTRATO e por 90 (noventa) dias após o término da vigência contratual, em valor correspondente a 5% (CINCO POR CENTO) do valor total do CONTRATO.

No prazo máximo de 10 (DEZ) DIAS ÚTEIS, prorrogáveis por igual período, a critério do CONTRATANTE, contados da assinatura do CONTRATO, a CONTRATADA deverá apresentar comprovante de prestação de GARANTIA, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

A inobservância do prazo fixado para apresentação da GARANTIA acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autoriza a ADMINISTRAÇÃO CONTRATANTE a promover a rescisão do CONTRATO por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n. 8.666 de 1993.

A validade da GARANTIA, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o término da vigência contratual, conforme item 3.1 do Anexo VII-F da IN SEGES/MP nº 5/2017. A GARANTIA assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

a) prejuízos advindos do não cumprimento do objeto do CONTRATO e do não adimplemento das demais obrigações nele previstas;

b) prejuízos diretos causados à ADMINISTRAÇÃO CONTRATANTE decorrentes de culpa ou dolo durante a execução do CONTRATO;

c) multas moratórias e punitivas aplicadas pela ADMINISTRAÇÃO CONTRATANTE à CONTRATADA; e

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

A modalidade SEGURO-GARANTIA somente será aceita se contemplar todos os eventos indicados acima, observada a legislação que rege a matéria. A GARANTIA em dinheiro deverá ser efetuada em favor da CONTRATANTE, em conta específica na CAIXA ECONÔMICA FEDERAL, com correção monetária.

Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo BANCO CENTRAL DO BRASIL, e avaliados pelos seus valores

[5] Grupo de empresas mantido sob a direção, controle ou administração de outra, embora tendo, cada uma delas, personalidade jurídica própria e autonomia individual, constituindo grupo industrial, comercial ou de qualquer outra atividade econômica.

econômicos, conforme definido pelo Ministério da Fazenda. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

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

Se o valor da GARANTIA for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 10 (DEZ) DIAS ÚTEIS, contados da data em que for notificada. A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

Será considerada extinta a GARANTIA:

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

b) no prazo de 90 (noventa) dias após o término da vigência do CONTRATO, caso a ADMINISTRAÇÃO não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea "h2"do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017.

O garantidor não é parte para figurar em processo administrativo instaurado pela contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada. A CONTRATADA autoriza a contratante a reter, a qualquer tempo, a GARANTIA, na forma prevista no EDITAL e no CONTRATO.

## 5.12 Benefícios identificados

Em termos de eficiência, eficácia, efetividade e economicidade, busca-se alcançar os seguintes benefícios com a contratação:

- Mitigar riscos pela falta de suporte e manutenção técnica especializada à solução de segurança de rede;
- Prover melhorias no gerenciamento dos níveis de serviço, com o necessário uso de equipamentos de segurança de rede atualizados;
- Manter plenamente funcionais os recursos operacionais de prevenção de ameaças e ataques a rede de TI do MEC;
- Preservar investimentos já realizados na infraestrutura e serviços de TI do MEC, sem a realização de novos dispêndios de recursos em outros equipamentos;
- Disponibilizar com segurança os recursos para atender a crescente demanda de serviços de TI;
- Possibilitar a realização de operação assistida e suporte técnico especializado localmente sempre que necessário e atualização tecnológica dos equipamentos;
- Prover os serviços do MEC aos usuários de forma eficaz, eficiente e segura;
- Prover infraestrutura tecnológica para que a STIC tenha condições de garantir as atividades finalísticas do MEC, através do emprego de recursos necessários para garantir a segurança das informações digitais de propriedade ou sob custódia do MEC;
- Garantir a capacidade dos componentes e serviços no atendimento das necessidades do MEC;
- Manter e disponibilizar acesso às informações que gerem valor ao negócio;
- Prover condições de disponibilizar dinamicamente e rapidamente as informações, com a performance proporcional à demanda manifestada pelos clientes do MEC.

## 5.13 Aplicabilidade de normas específicas

### 5.13.1 Instrução Normativa SGD n° 02, de 04 de abril de 2019

A Instrução Normativa SGD/ME n° 02, de 11 de janeiro de 2021, “regulamenta o art. 9º-A do Decreto nº 7.579, de 11 de outubro de 2011, e o art. 22, § 10 do Decreto nº 7.892, de 23 de janeiro de 2013, e dispõe sobre a composição e as competências do Colegiado Interno de Referencial Técnico”.

A INSTRUÇÃO NORMATIVA SGD/ME Nº 5, DE 11 DE JANEIRO DE 2021, que atualizou a Instrução Normativa SGD n° 02, de 04 de abril de 2019, regulamenta os requisitos e procedimentos para aprovação de contratações ou de formação de atas de registro de preços, a serem efetuados por órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, relativos a bens e serviços de tecnologia da informação e comunicação – TIC, de acordo com o art. 9º-A do Decreto nº 7.579, de 11 de outubro de 2011, e o art. 22, § 10 do Decreto nº 7.892, de 23 de janeiro de 2013. A norma, em seu art. 2°, estabelece o seguinte:

> *Art. 2º Os órgãos e as entidades previstos no art. 1º deverão submeter à Secretaria de Governo Digital do Ministério da Economia solicitação para aprovação de:*
>
> *I - contratações relativas a bens e serviços de TIC, para efeito do disposto no art. 9º-A do Decreto nº 7.579, de 11 de outubro de 2011, com valor global estimado do objeto superior a 20 (vinte) vezes o previsto no art. 23, inciso II, alínea "c", da Lei nº 8.666, de 21 de junho de 1993; e*

*II - formação de atas de registro de preços de serviços de TIC passíveis de adesão por parte de órgãos ou entidades não participantes, para efeito do disposto no art. 22, § 10, inciso II, do Decreto nº 7.892, de 23 de janeiro de 2013.*

*§ 1º Para contratações no sistema de registro de preços, o valor global estimado que trata o inciso I deverá contemplar o montante das demandas dos órgãos participantes da licitação, incluindo os volumes previstos para possíveis utilizações da ata de registro de preços por órgão ou entidade não participante, e considerar a revisão dos valores na forma do art. 120 da Lei nº 8.666, de 1993.*

*§ 2º Para efeitos do valor referenciado no inciso I considerar-se-ão os valores estimados para a primeira vigência do(s) contrato(s).*

Por sua vez, a alínea "c" do inc. II do art. 23 da Lei 8.666/1993 estabelece:

*Art. 23. As modalidades de licitação a que se referem os incisos I a III do artigo anterior serão determinadas em função dos seguintes limites, tendo em vista o valor estimado da contratação: [...]*

*II - Para compras e serviços não referidos no inciso anterior: [...]*

*c) concorrência - acima de R$ 650.000,00 (seiscentos e cinquenta mil reais).*

Ocorre que esses valores foram atualizados pelo Decreto n° 9.412/2018, da seguinte forma:

*Art. 1º Os valores estabelecidos nos incisos I e II do caput do art. 23 da Lei nº 8.666, de 21 de junho de 1993, ficam atualizados nos seguintes termos: [...]*

*I - Para obras e serviços de engenharia: [...]*

*II - Para compras e serviços não incluídos no inciso I: [...]*

*a) na modalidade concorrência - acima de R$ 1.430.000,00 (um milhão, quatrocentos e trinta mil reais).*

Assim, o limite estabelecido no art. 2° Instrução Normativa SGD/ME n° 02, de 04 de abril de 2019 é de 20 vezes o valor estabelecido na alínea "c" do art. 1° do Decreto n° 9412/2018, ou seja, R$28.600.000,00. Assim, considerando o valor estimado global de R$ 4.584.117,34 a referida norma não se aplica à presente pretensão contratual.

### 5.13.2 Portaria STIC nº 6.432, de 11 de julho de 2018

A Portaria STIC n° 6.432, de 11 de julho de 2018[6], "dispõe sobre a aplicação do Índice de Custos de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional e dá outras providências".

Considerando a aplicabilidade, o índice de reajuste a ser adotado para o CONTRATO será o ICTI - Índice de Custos de Tecnologia da Informação.

### 5.13.3 Portaria STI n° 04, de 6 de março de 2017

A Portaria STI n° 04, de 6 de março de 2017[7], "dispõe sobre recomendações técnicas para mensuração de software ou de resultados de serviços de desenvolvimento, manutenção e sustentação de software no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, e dá outras providências.

A contratação em questão não envolve serviços de desenvolvimento e/ou manutenção de software, logo não se aplica o normativo acima.

### 5.13.4 Portaria STI nº 20, de 14 de junho de 2016

A Portaria STI n° 20, de 14 de junho de 2016[8], "dispõe sobre orientações para contratação de soluções de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional e dá outras providências".

Quanto ao normativo acima, foram consideradas tanto as recomendações de caráter geral quanto as recomendações específicas contidas no Guia de Boas Práticas, Orientações e Vedações para Contratação de Ativos de TIC – Versão 4, anexo da norma, disponível no seguinte sítio eletrônico: https://www.gov.br/governodigital/pt-br/contratacoes/orientacoes_ativos-de-tic-v-4.pdf.

O referido guia prevê o seguinte ciclo de vida para ativos de TIC:

*De forma geral, o ciclo de vida dos ativos de TI obedece a quatro fases, a saber:*
*Fase 1: Lançamento.*
*Nesta fase, os ativos de TI são naturalmente mais caros por representarem produtos recentemente lançados no mercado e que*

[6] Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=13/07/2018&jornal=515&pagina=96

[7] Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&data=08/03/2017&pagina=147

[8] Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&data=15/06/2016&pagina=52

*encontram-se na vanguarda da tecnologia. Normalmente há poucas opções de fornecedores disponíveis no mercado e alguma dificuldade na manutenção e reposição.*

*A aquisição de ativos de TI nesta fase do ciclo de vida deve pautar-se na justificativa da necessidade de provimento de serviços altamente diferenciados em desempenho e/ou capacidade e que não possam ser providos por ativos que se encontrem na fase de Menor Custo ou alternativamente na fase de Seleção.*

*Fase 2: Seleção.*

*Este documento de Boas práticas, Orientações e Vedações tem força normativa legal, estando vinculado à Portaria MP/STI nº 20, de 14 de junho de 2016, na forma de anexo, tendo sido assinado, em sua última versão, pelo Secretário de Tecnologia da Informação do Ministério do Planejamento, Desenvolvimento e Gestão em 22/03/2017 e publicado em 23/03/2017.*

*Fase imediatamente posterior à de Lançamento, na qual os ativos de TI têm menor custo se comparados à fase anterior, alta capacidade de customização e níveis crescentes de padronização e de suporte de mercado.*

*A estratégia de aquisição dos ativos de TI deve contemplar, via de regra, os bens que estejam compreendidos na fase Menor Custo ou alternativamente nesta fase, levando-se em consideração as necessidades de desempenho e/ou capacidade, a vida útil prevista para o equipamento, entre outros.*

*Fase 3: Menor Custo.*

*Fase imediatamente posterior à Seleção, neste momento os ativos de TI estão altamente comoditizados, atingindo seu menor custo de comercialização, tanto para aquisição como para manutenção, possuem alta capacidade de customização, alta padronização e adequado suporte de mercado.*

*A estratégia de aquisição dos ativos de TI deve contemplar, preferencialmente, os bens que estejam compreendidos nesta fase de melhor relação custo / capacidade ou alternativamente na fase Seleção, levando-se em consideração as necessidades de desempenho e/ou capacidade, a vida útil prevista para o equipamento, entre outros.*

*Fase 4: Substituição.*

*Fase imediatamente posterior a Menor Custo, representa a última no ciclo de vida dos bens de TI. Normalmente, os ativos de TI nesta fase têm baixa comercialização e alto custo de manutenção. São compostos normalmente pelos ativos que fazem parte do legado tecnológico da instituição.*

*A estratégia de aquisição dos ativos de TI deve ser trabalhada de forma a implementar uma política de substituição e descarte, conforme item 1.3 deste documento, visando não incorrer em custos elevados de manutenção de tecnologia já obsoleta.*

Desta forma, como a solução de mitigação de ataques do tipo DoS/DDoS implantada na central de processamento de dados do MEC, já estão em fase de obsolescência (correspondente à fase 4 descrita acima), considerando o tempo de vida de 5 (cinco) anos para estes equipamentos, decidiu-se, como proposta de planejamento, a aquisição de novos equipamentos e não a renovação da garantia dos mesmos.

Em relação à definição das especificações técnicas para ativos de TIC, foram consideradas as seguintes previsões do guia:

*1.5.2. Para a correta especificação dos requisitos dos ativos de TI, é primordial que o gestor busque conhecimento técnico adequado do objeto a ser adquirido e se atenha exclusivamente à necessidade da Administração, evitar especificações excessivas, irrelevantes ou desnecessárias que limitem ou frustrem o caráter competitivo da licitação e não observem os padrões de mercado.*

## 5.14 Estimativa do custo total da contratação

A estimativa do custo global da contratação é de R$ 4.894.784,12 (quatro milhões oitocentos e noventa e quatro mil setecentos e oitenta e quatro reais e doze centavos). A definição do preço considerou os critérios contidos na Instrução Normativa SEGES n° 73, de 5 de agosto de 20209, e as disposições aplicáveis às soluções de Tecnologia da Informação e Comunicação da Instrução Normativa SGD n° 01, de 04 de abril de 2019, cujo resultado encontra-se consolidado no documento **PESQUISA DE PREÇOS**, anexo a este **ESTUDO TÉCNICO PRELIMINAR**.

Ainda, na forma do art. 21 da Instrução Normativa SGD/ME n° 01/2019, a adequação orçamentária e o cronograma físico-financeiro contêm a estimativa do impacto econômico-financeiro no orçamento do órgão ou entidade, com indicação das fontes de recurso e o

[9] Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=06/08/2020&jornal=515&pagina=19

cronograma de execução física e financeira, contendo o detalhamento das etapas ou fases da Solução a ser contratada, com os principais serviços ou bens que a compõe, e a previsão de desembolso para cada uma delas:

| Ação | Plano Orçamentário | PTRES | Fonte | PI |
|---|---|---|---|---|
| 2000 | 0001 | 169152 | 8186 | VKK01N0100N |

| Item | Descrição | Catmat/Catser | Natureza da Despesa | Estimativa de Volume |
|---|---|---|---|---|
| 1 | Solução de mitigação de ataques de negação de serviço (DoS/DDoS) | 133132 | 44.90.52-35 | 1 |
| 2 | Serviço de implantação, instalação, configuração e transferência de conhecimento | 27111 | 33.90.40-22 | 1 |
| 3 | Serviço de operação assistida | 26999 | 33.90.40-11 | 400 |

| Natureza Da Despesa | Exercício | Anual Estimado |
|---|---|---|
| 44.90.52-35 [item 1] | 2021 | R$ 4.765.229,95 |
| **Natureza Da Despesa** | **Exercício** | **Anual Estimado** |
| 33.90.40-22 [item 2] | 2021 | R$ 91.218,49 |
| **Natureza Da Despesa** | **Exercício** | **Anual Estimado** |
| 33.90.40-11 [item 3] | 2021 | R$ 29.192,18 |
| | 2022 | R$ 29.192,18 |
| | 2023 | R$ 29.192,18 |
| | 2024 | R$ 29.192,18 |
| | 2025 | R$ 29.192,18 |
| | **Valor Global Estimado:** | **R$ 5.002.409,33** |

## 5.15 Análise de necessidades de adequação do ambiente

### 5.15.1 Identificação de recursos tecnológicos e materiais necessários à execução do objeto

Para viabilizar a execução contratual será necessária a realização das seguintes adequações ambientais:

a) Disponibilização de mobiliário (mesas e cadeiras) para a equipe de implantação da solução;
b) Disponibilização de instalações elétricas para energização dos equipamentos na sala cofre;
c) Disponibilização de espaço nos racks onde serão instalados os equipamentos;
d) Disponibilizar cabeamento lógico.

### 5.15.2 Identificação de recursos humanos necessários à execução do objeto

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

- **Gestor do Contrato**: servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente;
- **Fiscal Técnico**: servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato;
- **Fiscal Requisitante**: servidor representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista funcional da Solução de Tecnologia da Informação; e
- **Fiscal Administrativo**: servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos.

Atualmente, a área requisitante dispõe de servidores em quantidade e capacidade suficientes para a fiscalização de todos os controles, acompanhamento processual e demais atividades necessárias à aferição das exigências contratuais.

### 5.16 Análise da estratégia de continuidade

Recomendamos que a vigência do CONTRATO seja fixada em 12 (doze) MESES, podendo ser prorrogado por períodos sucessivos de 12 (doze) meses até o limite de 60 (sessenta) meses, apenas para o item 3 do objeto, conforme disciplinado no art. 57 da Lei n° 8.666/1993. Com relação à manutenção das condições iniciais de habilitação técnica, a equipe de fiscalização deve atentar-se ao cumprimento do disposto no inc. V do art. 33 da IN-01/2019/SGD:

> *Art. 33 O monitoramento da execução deverá observar o disposto no Modelo de Gestão do Contrato, e consiste em: [...]*
>
> *V - Verificação da manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica, a cargo dos Fiscais Administrativo e Técnico do Contrato.*

A área requisitante deverá realizar contínuo monitoramento da execução contratual, com o objetivo de garantir a continuidade dos serviços e evitar sua interrupção de forma não programada. Além disso, deverá atuar no sentido de manter sob seu controle o conhecimento do serviço e dos processos de execução de modo a reduzir o risco de dependência em relação ao fornecedor. Todos os eventos da execução contratual deverão ser apontados em registro histórico adequado. Os **RISCOS** mapeados estão listados no **MAPA DE GERENCIAMENTO DE RISCOS**.

## 6 Declaração de viabilidade da contratação

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

## 7 Aprovação

Nos termos do §2° do art. 11 da IN-01/2019/SGD, o presente Estudo TÉCNICO PRELIMINAR da Contratação é aprovado e assinado pelos Integrantes TÉCNICO e REQUISITANTE da Equipe de Planejamento da Contratação e pela AUTORIDADE MÁXIMA da Área de TIC.

| APROVADO E ASSINADO ELETRONICAMENTE – PROCESSO SEI 23000.002559/2021-11 | |
|---|---|
| **INTEGRANTE(S) REQUISITANTE(S)** | **INTEGRANTE(S) TÉCNICO(S)** |
| Álvaro da Costa Rondon Neto - 1774842 | Alonso Cláudio Pereira da Silva Brito - 1087782 |
| **AUTORIDADE DE TIC** | |
| **André Henrique dos Santos Castro**<br>Subsecretário de Tecnologia da Informação e Comunicação | |

## ANEXO A ANÁLISE COMPARATIVA DAS ALTERNATIVAS IDENTIFICADAS

| Análise comparativa das alternativas identificadas | | | | | | |
|---|---|---|---|---|---|---|
| SOLUÇÃO [ALTERNATIVA DE MERCADO] | ADOÇÃO E/OU DISPONIBILIDADE EM OUTROS ÓRGÃOS | ADOÇÃO E/OU DISPONIBILIDADE NO PORTAL DO SOFTWARE PÚBLICO | ADERÊNCIA ÀS POLÍTICAS, PADRÕES E MODELOS DE GOVERNO | NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE | ESPECIFICAÇÃO, COMPOSIÇÃO E/OU CARACTERÍSTICAS | FORMA DE AQUISIÇÃO |
| Alternativa A (Item 3.1.1) | Sim | Não se aplica | Não se aplica | Há necessidade de adequação | Solução composta por aquisição de produtos e serviços | Nova contratação (Licitação) |
| Alternativa B (Item 3.1.2) | Sim | Não se aplica | Não se aplica | Não há necessidade de adequação | Solução composta por serviços | Nova contratação (Licitação) |

## ANEXO B RESUMO DA ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

| ALTERNATIVA A - SUBSTITUIÇÃO DA SOLUÇÃO IMPLANTADA | | | | | | Média | | Mediana | | Menor | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Lote | Item | Descrição | Catmat/Catser | Unidade | Qtde. | Valor Unitário | Valor Total | Valor Unitário | Valor Total | Valor Unitário | Valor Total |
| 1 | 1 | Solução de mitigação de ataques de negação de serviço (DoS/DDoS) | 133132 | Unidade | 1 | R$ 4.765.229,95 | R$ 4.765.229,95 | R$ 4.839.143,62 | R$ 4.839.143,62 | R$ 4.535.079,24 | R$ 4.535.079,24 |
| | 2 | Serviço de implantação, instalação, configuração e transferência de conhecimento | 27111 | Unidade | 1 | R$ 91.218,49 | R$ 91.218,49 | R$ 27.875,00 | R$ 27.875,00 | R$ 2.231,73 | R$ 2.231,73 |
| | 3 | Serviço de operação assistida | 26999 | Horas | 400 | R$ 364,90 | R$ 145.960,89 | R$ 350,00 | R$ 140.000,00 | R$ 147,00 | R$ 58.800,00 |
| | | | | | Valor Global Estimado >>> | | R$ 5.002.409,33 | | R$ 5.007.018,62 | | R$ 4.596.110,97 |

| ALTERNATIVA B - EXTENSÃO DA GARANTIA, MANUTENÇÃO E SUPORTE TÉCNICO PARA A SOLUÇÃO VIGENTE | | | | | | Média | | Mediana | | Menor | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Lote | Item | Descrição | Catmat/Catser | Unidade | Qtde. | Valor Unitário | Valor Total | Valor Unitário | Valor Total | Valor Unitário | Valor Total |
| 1 | 1 | Subscrição de garantia e suporte para a solução Arbor Edge Defense, por 60 meses<br>Modelo: Netscout Arbor AED APS 2800 –10 S/N CG23726010HA | 133132 | Unidade | 1 | R$ 3.589.023,97 | R$ 3.589.023,97 | R$ 3.552.428,33 | R$ 3.552.428,33 | R$ 3.500.000,00 | R$ 3.500.000,00 |
| | 2 | Suporte técnico especializado mensal para a solução Arbor Edge Defense, por 60 meses | 27111 | Unidade | 1 | R$ 819.708,98 | R$ 819.708,98 | R$ 861.978,14 | R$ 861.978,14 | R$ 668.046,25 | R$ 668.046,25 |
| | 3 | Serviço de operação assistida | 26999 | Horas | 400 | R$ 364,90 | R$ 145.960,89 | R$ 350,00 | R$ 140.000,00 | R$ 147,00 | R$ 58.800,00 |
| | | | | | Valor Global Estimado >>> | | R$ 4.554.693,83 | | R$ 4.554.406,48 | | R$ 4.226.846,25 |

## ANEXO C SÉRIE DE PREÇOS COLETADA

| SÉRIE DE PREÇOS COLETADA | | | | | ID FONTES CONSULTADAS | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Alternativa A - Aquisição de nova solução de mitigação de ataques DoS/DDoS e serviços agregados** | | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| **LOTE** | **ITEM** | **DESCRIÇÃO** | **CATMAT/CATSER** | **UNIDADE** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** |
| 1 | 1 | Solução de mitigação de ataques de negação de serviço (DoS/DDoS) | 133132 | Unidade | - | - | - | - | - | - | - | - | - | - | - | R$ 4.535.079,24 | R$ 4.839.143,62 | R$ 4.921.467,00 |
| | 2 | Serviço de implantação, instalação, configuração e transferência de conhecimento | 27111 | Unidade | R$ 7.877,00 | R$ 2.231,73 | R$ 8.500,00 | R$ 30.000,00 | R$ 25.750,00 | - | - | - | - | - | - | R$ 189.900,00 | R$ 234.300,10 | R$ 231.189,05 |
| | 3 | Serviço de operação assistida | 26999 | Horas | - | - | - | - | - | R$ 190,00 | R$ 234,00 | R$ 250,00 | R$ 147,00 | R$ 350,00 | R$ 530,00 | R$ 498,00 | R$ 530,00 | R$ 555,12 |

| SÉRIE DE PREÇOS COLETADA | | | | | ID FONTES CONSULTADAS | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Alternativa B - Extensão da garantia, manutenção e suporte técnico para a solução vigente** | | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| **LOTE** | **ITEM** | **DESCRIÇÃO** | **CATMAT/CATSER** | **UNIDADE** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** | **R$ UNIT** |
| 1 | 1 | Renovação de garantia e suporte 60 meses<br>Modelo: Netscout Arbor AED APS 2800 –10 S/N CG23726010HA | 133132 | Unidade | - | - | - | - | - | - | - | - | - | - | R$ 2.100.000,00 | R$ 2.250.743,52 | R$ 2.100.000,00 | R$ 2.162.914,00 |
| | 2 | Suporte técnico especializado mensal para a solução Arbor Edge Defense, por 60 meses | 27111 | Unidade | - | - | - | - | - | - | - | - | - | - | R$ 400.827,75 | R$ 532.100,03 | R$ 514.213,15 | R$ 520.160,62 |
| | 3 | Serviço de operação assistida | 26999 | Horas | - | - | - | - | - | R$ 190,00 | R$ 234,00 | R$ 250,00 | R$ 147,00 | R$ 350,00 | R$ 530,00 | R$ 498,00 | R$ 530,00 | R$ 555,12 |

## ANEXO D PROJETOS SIMILARES EXECUTADOS POR OUTROS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA

| Órgão | UASG | Edital | Processo SEI | Contrato | Data de Assinatura | Ata Registro de Preço | Valor de Contrato <Todos os Itens> | Valor do Contrato <Solução AntiDDOS + Serviços de Implantação> | Cotação do Dólar <Data de Assinatura> | Projeção do Valor da Contratação <Em Dólares> | Cotação do Dólar <Vigente em 28/10/21> | Projeção do Valor Estimado da Solução <Considerando a Cotação Vigente do Dólar> |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ministério de Minas e Energia | 320004 | 03/2013 | 48000.001883/2012-43 | 08-2013 | 19/04/2013 | 03-2013 MME | Itens 1, 2, 3 e 4 (R$ 1.733.740,00)<br>Item 5 Operação (R$ 360,00) | R$ 1.733.740,00 | R$ 1,96 | U$ 882.490,07 | R$ 5,61 | R$ 4.952.887,29 |
| Inep | 153978 | 21/2020 | 23036.002739/2020-04 | 01-2021 | 04/01/2021 | 13-2020 INEP | Itens 1 e 2 (R$ 2.500.827,75)<br>Item 3 Operação (R$ 530,00) | R$ 2.500.827,75 | R$ 5,15 | U$ 485.852,34 | R$ 5,61 | R$ 2.726.797,67 |
| Inep | 153978 | - | 23036.001587/2017-19 | 12-2018 | 28/03/2018 | 10-2017 INEP | Itens 1 e 2 (R$ 3.517.234,37)<br>Item 3 Operação (R$ 378,00) | R$ 3.517.234,37 | R$ 3,34 | U$ 1.053.695,14 | R$ 5,61 | R$ 5.913.758,59 |
| Inep | 153978 | - | 23036.000494/2014-24 | 16-2015 | 15/06/2015 | 08-2014 INEP | Itens 1, 2 e 3 (R$ 3.139.460,00) | R$ 3.139.460,00 | R$ 3,10 | U$ 1.011.554,32 | R$ 5,61 | R$ 5.677.247,49 |
| Inep | 153978 | 17/2017 | 23036.001587/2017-19 | 34-2017 | 26/12/2017 | 10-2017 INEP | Itens 1 e 2 (R$ 3.517.234,37)<br>Item 3 Operação (R$ 378,00) | R$ 3.517.234,37 | R$ 3,32 | U$ 1.059.407,94 | R$ 5,61 | R$ 5.945.821,14 |
| Inep | 153978 | 22/2014 | 23036.000494/2014-24 | 39-2014 | 05/09/2014 | 08-2014 INEP | Itens 1, 2, 4, 5 e 8 (R$ 4.263.460,00) | R$ 4.263.460,00 | R$ 2,24 | U$ 1.901.971,81 | R$ 5,61 | R$ 10.674.626,56 |
| Ministério da Educação | 150002 | - | 23000.013106/2014-82 | 67-2014 | 22/12/2014 | adesão a ARP 08-2014 INEP | Itens 1, 3 e 5 (R$ 3.173.460,00) | R$ 3.173.460,00 | R$ 2,65 | U$ 1.196.313,19 | R$ 5,61 | R$ 6.714.188,15 |
| Ministério da Educação | 150002 | - | 23000.013106/2014-82 | 56-2015 | 09/10/2015 | adesão a ARP 08-2014 INEP | Item 7 Operação (R$ 380,00) | - | R$ 3,74 | U$ 0,00 | R$ 5,61 | R$ 0,00 |
| Ministério da Educação | 150002 | - | 23000.042716/2016-55 | 19-2018 | 08/05/2018 | adesão a ARP 10-2017 INEP | Itens 1 e 2 (R$ 3.517.234,37)<br>Item 3 Operação (R$ 378,00) | R$ 3.517.234,37 | R$ 3,58 | U$ 982.797,13 | R$ 5,61 | R$ 5.515.850,61 |