

# Estudo Técnico Preliminar 72/2023

## 1. Informações Básicas

Número do processo: 01400.013417/2023-97

## 2. Descrição da necessidade

Estudo de eventual aquisição de Solução de detecção, análise, resposta e monitoramento de incidentes de segurança da informação, para a modernização dos recursos de segurança cibernética da rede de computadores do Ministério da Cultura.

### 2.1. Motivação/Justificativa

**2.1.1.** Por meio da publicação do Decreto nº 11.336, de 1º de janeiro de 2023, foi formalizado o desmembramento da Secretaria Especial de Cultura do Ministério do Turismo para a criação do Ministério da Cultura.

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

- I - política nacional de cultura e política nacional das artes;
- II - proteção do patrimônio histórico, artístico e cultural;
- III - regulação dos direitos autorais;
- IV - assistência ao Ministério do Desenvolvimento Agrário e Agricultura Familiar e ao Instituto Nacional de Colonização e Reforma Agrária nas ações de regularização fundiária, para garantir a preservação da identidade cultural dos remanescentes das comunidades dos quilombos;
- V - proteção e promoção da diversidade cultural;
- VI - desenvolvimento econômico da cultura e a política de economia criativa;
- VII - desenvolvimento e a implementação de políticas e ações de acessibilidade cultural; e
- VIII - formulação e implementação de políticas, de programas e de ações para o desenvolvimento do setor museal.

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

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

**2.1.5.** Assim, as ações de aquisições de equipamentos, de contratações de serviços e soluções de tecnologia da informação para atender as demandas do Ministério da Cultura

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

**2.1.6.** Cabe ressaltar que a partir da recriação do Ministério da Cultura, compromisso formalizado em campanhas eleitorais, a Pasta passou a receber grande visibilidade para os cidadãos, uma vez que a promessa de melhorias de atuação na gestão de políticas públicas de incentivo à cultura, trouxe para o cidadão a expectativa de novos investimentos na área e da criação de oportunidades de empregos e benefícios relacionados à economia criativa e atividades culturais no âmbito nacional.

**2.1.7.** Neste sentido, considerando que durante os últimos 6 (seis) anos não houveram investimentos relevantes em infraestrutura de tecnologia da informação no âmbito do Ministério da Cultura, é papel fundamental da área de tecnologia da informação desta Pasta, atuar na elaboração de projetos de soluções de tecnologia da informação que contemplem todo o cenário de recriação do Ministério com o foco no alcance das metas institucionais, principalmente aquelas relacionada à transformação digital, renovação do parque tecnológico, ampliação da rede de dados e otimização da infraestrutura de tecnologia da informação, com foco na implementação de soluções de segurança da informação e adaptação às normas. Estas atividades serão essenciais para garantir que o "*Novo Ministério da Cultura*" alcance o patamar dos outros órgãos centrais com importância similar a desta Pasta.

**2.1.8.** Em relação as questões de segurança da informação, é de conhecimento público que diversos órgãos brasileiros são alvos de constantes ameaças, a exemplo o recente ataque ao Ministério da Saúde, onde o hacker atingiu o principal sistema do Ministério; o ataque a Secretaria de Fazenda do Rio de Janeiro, onde foram vazados 420Gb de dados e o ataque ao Sebrae, onde as máquinas virtuais foram atacadas e criptografadas fazendo o site e sistema ficarem fora do ar por vários dias. Além destes, também foram alvo de ataques STF, STJ, TRF 3ª Região, Justiça Federal de SP e MS, etc.

**2.1.9.** Neste sentido, considerando que o Ministério da Cultura desenvolve um importantíssimo papel dentro do Governo Federal, sendo responsável pelo planejamento e pela execução das políticas nacionais de cultura e de artes, chegando a movimentar bilhões de reais em recursos públicos, verifica-se que a Pasta tende a ser alvo de criminosos e outros indivíduos que praticam crimes digitais.

**2.1.10.** Verifica-se ainda que o Ministério lida todos os dias com elevada troca de informações, além de um grande e complexo volume de dados sensíveis de milhares de cidadãos e empresas do Brasil.

**2.1.11.** Além disso, em 2020 um novo cenário surgiu em decorrência da Covid-19. Processos de transformação digital das organizações públicas acabou por forçar às organizações a expandir seu ambiente de trabalho em regime remoto. Dessa forma os ambientes das organizações tornaram-se mais visíveis e vulneráveis a ataques com roubo de informações além da possibilidade de comprometimento do ambiente, o que leva à conclusão da necessidade de que as instituições públicas tenham um altíssimo nível de segurança cibernética.

**2.1.12.** Nestes cenário em que há o avanço das ameaças cibernéticas, cada vez mais atuante no meio governamental, as ferramentas de segurança da informação também precisam se tornar cada vez mais diversas e sofisticadas no tratamento dos riscos de ocorrência de invasões da rede, fato que torna relevante a realização de investimentos em soluções de cibersegurança, fato que motiva a realização destes estudos, que visa a identificação de solução de segurança que possa apoiar o monitoramento da rede e controle de ações internas e identificação de situações suspeitas dentro da rede de computadores do Ministério da Cultura.

**2.1.13.** Considerando as características de recriação do Ministério da Cultura verifica-se que a estratégia da implementação da segurança da informações em camadas, é adequada, uma vez que consiste na disposição de várias etapas de proteção à operacionalidade da Pasta, de modo a blindar seus arquivos e dados mais sensíveis contra ataques cibernéticos desde a camada física de rede até a camada de aplicações, de forma que a metodologia adotada reforça as fronteiras digitais com vários muros de sustentação de forma gradativa.

**2.1.14.** Desta forma as camadas de segurança oferecem uma proteção maior, além de garantir que os criminosos tenham mais dificuldade na hora de tentar invadir um sistema, podendo até mesmo desestimular a tentativa, além disso a estratégia possibilita com que o Ministério possa efetuar a implementação gradativa por meio de contratações de soluções que exigem níveis variáveis de maturidade das equipes.

**2.1.15.** Neste sentido a Subsecretaria de Tecnologia da Informação e Inovação - STII, considerando a disponibilidade orçamentária e adotando as possibilidades previstas no arcabouço legislativo relacionado a licitações públicas, vem adotando a estratégia de promover os estudos de soluções de tecnologia da informação visando a disponibilização de uma série de registros de preços que será capaz de possibilitar com que o Ministério da Cultura possa adquirir equipamentos e soluções de segurança neste exercício e nos próximos até alcançar o nível de maturidade e proteção mais adequado a sua necessidade.

**2.1.16.** Diante destes apontamentos verifica-se que já foram elaborados os projetos voltados a modernização do parque tecnológico do Ministério, a exemplo de três projetos elencados a seguir:

- a) Projeto de aquisição de NG Firewall, que visa a aquisição de firewall de próxima geração com recursos SD-WAN para o edifício sede e para os sites conectados.
- b) Projeto de aquisição de solução de armazenamento de dados, com recursos de segurança da informação para implementação de ambientes de sustentação de sistemas críticos e para a implementação de repositórios de backup e uso de órgãos vinculados.
- c) Projeto de Modernização de ativos de rede, que visa a modernização de todos os switches do edifício sede e das unidades conectadas.

**2.1.17.** Desta forma, resta verificada a preocupação das equipes de tecnologia da informação desta Pasta em direcionar os investimentos de forma estratégica, promovendo a elevação gradativa dos níveis de segurança institucional e a maturidade das equipes técnicas de forma a alcançar vários benefícios, tais como:

- Proteção contra malwares, ransomware, wannacry, botnet entre outros;
- Proteção contra vazamentos de dados e phishing;
- Segurança ágil e dinâmica;

- Oferece proteção mais forte, multicamadas;
- Controle de ativos e
- Gerenciamento centralizados dos recursos de rede e segurança, dentre outros citados em cada projeto.

**2.1.18.** As camadas de segurança são fundamentais porque, caso uma das proteções falhe, a outra assume, mantendo os dados intactos. Uma só camada não é capaz de proteger toda a “superfície de ataque”, cada vez mais ampla. Neste sentido, a cada solução implementada é criada uma nova barreira, desta a implementação do firewall de rede posicionado na fronteira entre a rede interna e externa até a implementação de soluções de auditoria e monitoramento e controle de acessos.

**2.1.19.** Uma das primeiras camadas a se proteger é a camada de rede. Essa camada protege tanto contra ataques vindos de fora, que possuem o objetivo de descobrir sistemas vulneráveis com senhas fracas, para conseguirem informações privilegiadas; como também na saída de acessos, para que não seja realizado acesso a sites não permitidos, vazamento de informações, e consumo indevido de banda, o que atrapalha na produtividade e desempenho da rede. Além disso, com o novo cenário de trabalho remoto e híbrido, é necessário considerar também o monitoramento e proteção dos dispositivos móveis, ou seja, dos endpoints como os notebooks, os próprios aparelhos celulares e tablets trazidos pelas pessoas dentro das políticas de BYOD (Bring Your Own Device).

**2.1.20.** Nesse sentido, entendendo a grande importância que os sistemas e serviços de TI adquiriram para as organizações e que se observa a constante diversificação e desenvolvimento de novas ameaças cibernéticas, percebemos que o Firewall, que exerce a segurança de perímetro de Rede, protegendo o tráfego Norte-Sul de ataques conhecidos, embora possua grande importância para o Ministério da Cultura, não é o suficiente para bloquear ataques mais sofisticados, além de não suprir a proteção Leste-Oeste e de ataques desconhecidos na rede.

**2.1.21.** Verifica-se então, a necessidade da implementação de ferramenta que proteja também o tráfego Leste-Oeste de ameaças não conhecidas, dotada de inteligência artificial para estudar o comportamento da rede e, com isso, detectar comportamentos anômalos, até mesmo as menores e mais discretas tentativas do invasor fazendo a mitigação do ataque antes mesmo dele ocorrer, desta forma a ferramenta complementar a proteção garantida pelo Firewall na camada de rede.

**2.1.22.** A ação visa proteger a rede de ameaças desconhecidas externas, além das internas que podem ocorrer com máquinas infectadas vindo de trabalho híbrido/remoto ou de visitantes.

**2.1.23.** Assim, em continuidade as ações conduzidas em outros processos de contratação é importante a utilização de um sistema de detecção e respostas, com a finalidade de dar visibilidade, tratar incidentes e monitorar o tráfego de dados de todas as camadas de segurança adotando uma solução que possibilite o monitoramento e a gestão em interface centralizada otimizando assim o trabalho das equipes de suporte técnico e de segurança da informação do Ministério da Cultura.

**2.1.24.** Com o volume imenso de dados disponíveis e com a complexidade da rede de computadores do Ministério da Cultura, a análise minuciosa de tráfego de rede e demais recursos, utilizando inteligência artificial para estabelecer correlações e respostas

automáticas entre os vários alertas que estão em curso nas camadas de segurança é essencial para apoiar esta Pasta com os desafios de proteção de sistemas e serviços além da correta adequação a Lei Federal nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD).

### 3. Área requisitante

Área Requisitante	Responsável
Divisão de Segurança da Informação	Ramon Leonn Victor Medeiros

### 4. Necessidades de Negócio

**4.1.** As necessidades de negócio, também chamadas de requisitos do negócio, segundo o Corpo de Conhecimento de Análise de Negócios (Guia BABOK v. 2.0), são metas de mais alto nível, objetivos ou necessidades da organização. Descrevem as razões pelas quais um projeto foi iniciado, os objetivos que o projeto vai atingir e as métricas que serão utilizadas para medir o seu sucesso. Nesse sentido, a presente seção visa descrever as necessidades de negócios que conduzirão as análises de soluções e definição da solução mais adequadas a tais objetivos organizacionais, a saber:

- a) Proteção das informações sensíveis ao negócio do Ministério da Cultura;
- b) Aumentar a eficiência da segurança, proteção e autenticidade dos dados e acessos;
- c) Redução da probabilidade de ocorrência de incidentes de segurança;
- d) Controle da saída de dados sensíveis, seja via transferência de arquivos ou publicação em páginas da internet;
- e) Amplificação da camada de proteção e visibilidade de informações sensíveis;
- f) Fluxo automatizado de descoberta de informações sensíveis em todos os pontos do ambiente;
- g) Garantir a disponibilidade e continuidade dos serviços de TI

**4.2.** Incrementar e otimizar o gerenciamento, a eficiência e a proteção das informações do ambiente tecnológico do MinC.

**4.3.** Aprimoramento continuado das ações de Segurança da Informação, objetivando o atendimento à totalidade dos usuários do ambiente tecnológico do MinC.

**4.4.** Melhoramento da capacidade de detecção e prevenção de ameaças cibernéticas, comportamentos suspeitos dos usuários, mal-uso dos dados institucionais e vazamentos de dados sensíveis.

**4.5.** Atualização e modernização do ambiente tecnológico do MinC, mantendo assim a infraestrutura de rede segura, disponível e plenamente operacional para a disponibilidade de informações precisas e confiáveis à sociedade e aos diversos usuários de seus sistemas, assegurando deste modo o negócio do Ministério da Cultura.

**4.6.** Manutenção da integridade, confiabilidade e segurança do ambiente tecnológico do MinC, bem como disponibilizar equipamentos, bases de dados e informações precisas e confiáveis.

**4.7.** A iniciativa em questão está em conformidade e encontra-se alinhada ao Plano Diretor de Tecnologia da Informação – PDTIC do Ministério da Cultura, bem como ao Planejamento Institucional 2023 - 2027.

## **5. Necessidades Tecnológicas**

**5.1.** Para garantir a disponibilidade evitando-se que falhas em um equipamento cause a indisponibilidade dos serviços, a solução deverá ser baseada em hardware e software projetados especificamente para análise de comportamento anômalo da rede.

**5.2.** Os softwares e hardwares que contemplam a solução de TIC devem ser do mesmo fabricante ou, no caso de software de um outro fabricante/fornecedor, este deverá ser formalmente autorizada e homologada pelo fabricante do hardware.

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

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

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

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

**5.7.** Durante a vigência contratual e o prazo de garantia, o fabricante deve garantir a atualização de patches e softwares de todos os componentes que compõe a solução de TIC, de modo irrestrito e ilimitado.

**5.8.** A solução de proteção deve ser oferecida na última versão disponibilizada pelo fabricante; na data da proposta, nenhum dos softwares componentes da solução de proteção ofertados poderão estar listados pelo fabricante com data definida para fim de suporte (“end of support”) ou fim de vendas (“end of sale”).

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

**6.1.** Além dos requisitos de negócio e tecnológicos, a presente contratação destaca aqueles requisitos que devem ser considerados ao longo do planejamento da contratação para se assegurar o alcance dos objetivos pretendidos com a aquisição, conforme a seguir:

- a) A solução deverá ser compatível com as demandas previstas no PCA do MinC com vistas a facilitar e viabilizar a execução no Sistema PGC para o exercício de 2024;
- b) Observar aspectos de compatibilidade com o datacenter do Minc.

## **6.2. Requisitos de Garantia e Assistência Técnica**

6.2.1. Os equipamentos e demais componentes que fazem parte da solução, deverão possuir garantia on-site de, no mínimo, 36 (Trinta e seis) meses.

6.2.2. Disponibilizar recurso via site do próprio FABRICANTE (informar URL para comprovação) que faça a validação e verificação da garantia do equipamento através da inserção do seu número de série e modelo/número do equipamento;

6.2.3. Durante o prazo de garantia, a empresa CONTRATADA ou FABRICANTE terão a obrigação de substituir ou reparar, às suas expensas, qualquer equipamento, peça ou software que apresente defeito, mesmo que decorra do desgaste natural do produto;

6.2.4. A CONTRATADA deverá providenciar a troca de qualquer peça ou componente danificado por todo o período da garantia, nos casos de necessidade de substituição de peças ou componentes deverá, sempre que possível, realizar as substituições sem causar indisponibilidade dos serviços.

6.2.5. A garantia não será afetada caso a CONTRATANTE venha a instalar placas de expansão, tais como placa de rede, ou adicionar unidades de disco rígido ou SSD, bem como se alterar a capacidade de memória RAM do equipamento. Entretanto, a garantia desses opcionais será de total responsabilidade da CONTRATANTE;

6.2.6. Na reposição de qualquer equipamento homologado, durante a vigência da garantia, havendo a descontinuidade tecnológica do modelo fornecido, a CONTRATADA ou FABRICANTE deverão substituí-lo por um que atenda as especificações exigidas no edital ou superior;

6.2.7. Caso seja necessária a troca de quaisquer peças dos equipamentos, as peças substitutas deverão ser novas e de primeiro uso, devendo apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento, salvo nos casos fundamentados por escrito e aceitos pela CONTRATANTE;

6.2.8. A manutenção corretiva é aquela destinada a corrigir eventuais defeitos apresentados pelo equipamento ou software;

6.2.9. Os chamados poderão ser abertos através dos seguintes canais:

1. Telefone 0800 ou chamada com custo de ligação local em Brasília/DF;
2. E-mail; Página web (ou chat) mantida pela CONTRATADA ou pelo FABRICANTE do equipamento.

6.2.10. A assistência técnica dos produtos em garantia deverá ser prestada no local onde o equipamento estiver instalado (na modalidade on-site);

6.2.11. O prazo para resolução dos chamados será contado a partir do momento do registro do chamado, obedecendo a as regras de contagem previstos no Termo de Referência e demais documentos vinculados a este processo de contratação;

6.2.12. Poderão ser abertos chamados de consultas técnicas para sanar dúvidas, repassar conhecimentos ou obter melhores práticas;

6.2.13. Para cada chamado técnico, a CONTRATADA ou o FABRICANTE deverá informar um número de controle (protocolo) para registro, bem como manter histórico de ações e atividades realizadas;

6.2.14. O atendimento no período coberto pela garantia descrita acima inclui mão de obra, peças e, em caso de necessidade de manutenção fora das dependências do MinC, transportes e seguros também se aplicam à mesma garantia, sem nenhum ônus adicional para a CONTRATANTE.

### **6.3. Requisitos da Capacitação**

6.3.1. A CONTRATADA deverá repassar à CONTRATANTE todas as informações solicitadas e documentação da solução, além de disponibilizar treinamento conforme especificações a serem fornecidas no Termo de Referência

6.3.2. O treinamento será demandado à CONTRATADA pela CONTRATANTE após a efetiva implementação e estruturação da solução de segurança em seu parque tecnológico, quando acordarão cronograma para realização do treinamento;

6.3.3. O treinamento deverá ser em Brasília – DF, para a equipe técnica do CONTRATANTE.

6.3.4. Todos os custos relativos à realização do treinamento são de exclusiva responsabilidade da CONTRATADA.

6.3.5. O treinamento deverá capacitar as equipes técnicas do CONTRATANTE a operar, configurar, administrar e resolver problemas usuais na solução adquirida, englobando tanto os componentes de hardware quanto de software.

6.3.6. Deverá ser ofertada para 1 (uma) turma com no máximo 10 alunos e com carga horária mínima de 40 (quarenta) horas.

6.3.7. Deverá ser fornecido certificado de conclusão emitido pelo fabricante.

6.3.8. Os horários do curso deverão seguir a conveniência do CONTRATANTE, podendo sua realização ocorrer apenas em um dos períodos do dia (manhã ou tarde).

6.3.9. Deverá ser fornecido material didático completo e com conteúdo oficial do fabricante.

### **6.4. Requisitos Legais**

6.4.1. A contratação do objeto deste Estudo tem amparo legal nos seguintes dispositivos legais:

a) Lei 14.133, de 01 de abril de 2021.

b) Lei Complementar nº 123, de 14 de dezembro de 2006, que institui o Estatuto Nacional da microempresa e da Empresa de Pequeno Porte.

c) Instrução Normativa nº 05 do MPOG, de 26 de maio de 2017, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.

d) Instrução Normativa SGD/ME Nº 94, DE 23 DE DEZEMBRO DE 2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.



e) Instrução Normativa SEGES /ME nº 65, de 07 de julho de 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

6.4.2. A referida contratação deve assegurar os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), descritos no Artigo 6º. da Lei. Toda informação trafegada, por meio dos equipamentos de tecnologia da informação e comunicação, que fazem parte do objeto de contratação devem atender às exigências da Lei Geral de Proteção de Dados Pessoais.

## 6.5. Requisitos Temporais:

**6.5.1.** O prazo de vigência do contrato será de 36 (trinta e seis) meses, contados a partir da data da sua assinatura, podendo ser prorrogado, respeitada a vigência máxima decenal, desde que haja preços e condições mais vantajosas para a Administração, nos termos dos artigos 106 e 107 da Lei 14.133/2021.

**6.5.2.** A reunião inicial de alinhamento com a Contratada, deverá ocorrer em no máximo 10 (dez) dias corridos, posteriormente à assinatura do instrumento contratual.

**6.5.3.** Os serviços de fornecimento do objeto – isto é, a execução completa dos serviços e tarefas previstas objetivando a plena e efetiva operacionalização da solução no ambiente do MinC – deverão ser executados no prazo máximo de até 120 (cento e vinte) dias consecutivos a partir da assinatura da Ordem de Fornecimento ou Ordem de Serviço.

**6.5.4.** O Cronograma de Execução a seguir descreve os serviços e tarefas previstas por todas as etapas de trabalho:

ETAPA	DESCRIÇÃO	PRAZO
1	Planejamento da integração do serviço de detecção e resposta	15 dias após Reunião Inicial
2	Implantação dos casos de uso e fluxo de respostas	60 dias após Etapa 1
3	Planejamento e Implantação do serviço de investigação e Inteligência de ameaças	15 dias após Etapa 2
4	Gerenciamento de crises	15 dias após Etapa 3
5	Etapa Final	5 dias após Etapa 4

**6.5.5.** Alterações no cronograma poderão ser efetivadas desde que em comum acordo entre as partes, devendo os casos conflitantes serem solucionados pelo Gestor do Contrato.

## 6.6. Requisitos de Segurança:

**6.6.1.** A Contratada deverá conhecer todas as normas, políticas e procedimentos de segurança estabelecidos pelo MinC para execução do Contrato.

**6.6.2.** A Contratada deverá assinar Termo de Ciência e Termo de Confidencialidade e Sigilo.

**6.6.3.** Não será permitido, salvo justificado, que o ambiente seguro seja acessado por pessoas além daquelas necessárias para a prestação de serviços do objeto contratado.

**6.6.4.** O acesso dos profissionais da Contratada às dependências do MinC estará sujeito às suas normas referentes à identificação (crachá funcional), trajés, trânsito e permanência em suas dependências.

**6.6.5.** A Contratada responsabilizar-se-á integral e solidariamente pelos atos praticados de seus empregados e/ou prestadores de serviço nas dependências do MinC ou mesmo fora delas, que venham a causar danos ou colocar em risco o patrimônio do Ministério.

#### **6.7. Requisitos Sociais, Ambientais e Culturais:**

**6.7.1** Aderência aos padrões definidos pelo Modelo de Acessibilidade em Governo Eletrônico – e-MAG, conforme a Portaria Normativa SLTI nº 03, de 7 de maio de 2007, quando houver necessidades de acessibilidade ao aplicativo para solicitações de suporte técnico;

**6.7.2** Os serviços prestados pela Contratada deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e materiais consumidos bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pela Contratante; e

**6.7.3.** A Contratada deverá instruir os seus empregados quanto à necessidade de racionalização de recursos no desempenho de suas atribuições, bem como das diretrizes de responsabilidade ambiental adotadas pela Contratante, autorizando a participação desses em eventos de capacitação e sensibilização promovidos pela Contratante, quando for o caso.

#### **6.8. Requisitos de Arquitetura Tecnológica:**

**6.8.1.** Durante a implantação da solução, a Contratada deverá realizar, entre outras atividades: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, tuning, resolução de problemas e implementação de segurança.

**6.8.2.** Caberá à Contratada a disponibilização de todos os recursos necessários, tais como hardwares, softwares, recursos humanos necessários à instalação da solução.

**6.8.3.** Caberá à Contratada a disponibilização de ferramentas/scripts de retorno imediato ao estado original da estrutura da Contratada caso a instalação e migração dos produtos /softwares da Contratada apresente falha.

**6.8.4.** A Contratada realizará adequação/configuração da solução fornecida ao longo da etapa de migração e realização de novas configurações.

**6.8.5.** A Contratada deverá fornecer todas as licenças necessárias de todos os componentes da solução ofertada e dos elementos adicionais que se fizerem necessários à instalação /migração e à perfeita operação do ambiente de produção.

**6.8.6.** Mais detalhes técnicos acerca da Solução de TIC a ser contratada encontram-se no Anexo I - ESPECIFICAÇÃO TÉCNICA MÍNIMA DA SOLUÇÃO do presente documento.

#### **6.9. Requisitos de Projeto e Implementação:**

**6.9.1.** A solução de TIC deverá ser plenamente implementada pela Contratada no ambiente do MinC em no máximo 120 (cento e vinte) dias corridos, a partir da assinatura da Ordem de Fornecimento ou Ordem de Serviço.

**6.9.2.** Em caso de alterações necessárias nas especificações do projeto original durante a execução dos trabalhos, competirá à Contratada elaborar o projeto da parte a ser alterada e submetê-lo à aprovação do Fiscal, não podendo ocorrer, no entanto, alteração substancial das disposições gerais formuladas pelo projeto original.

#### **6.10 Requisitos de Implantação:**

**6.10.1.** Caberá à Contratada o irrestrito cumprimento das seguintes prerrogativas:

- a) responsabilizar-se pela completa implantação do projeto, ou seja, todos os custos necessários à operacionalização dos equipamentos;
- b) responsabilizar-se por todos os instrumentais necessários durante o período de implantação e testes de aceitação;
- c) instalar e configurar todos os produtos do fornecimento da solução;
- d) executar a integração de todos os produtos da solução, de modo a não prejudicar as atividades mantidas nos locais, podendo ser exigida a realização de algumas fases em horários noturnos e fins de semana para que seja cumprido o cronograma de entrega;
- e) elaborar a "Documentação e Finalização do Projeto", que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e/ou gerencial.

### **7. Estimativa da demanda - quantidade de bens e serviços**

**7.1** De forma a calcular o dimensionamento da demanda, foram levantadas as características da rede do Ministério da Cultura de modo a avaliar a capacidade de processamento e armazenamento necessária para lidar com o volume de tráfego da rede e para armazenar logs e dados de incidentes relevantes.

**7.2** Cabe ressaltar que o objetivo de uso da solução é a implementação de uma camada complementar de segurança da informação, desta forma o dimensionamento da solução considera que a solução possa se integrar de forma eficaz com outros sistemas de segurança cibernética e ferramentas de gerenciamento de rede já em uso, possibilitando-se assim com que não seja necessário, de início, que a solução suporte sozinha todo o tráfego da rede do Ministério da Cultura, mas que atue de forma a não comprometer o desempenho da rede.

**7.3** Para tanto, considerando o throughput da rede do Ministério da Cultura, verifica-se suficiente a instalação de um appliance conectado aos switches topo de racks instalados no Datacenter do Ministério da Cultura e também conectado ao Firewall.

**7.4** De modo a garantir a devida proteção ao investimento a ser realizado, será exigida a garantia de suporte técnico com reposição de peças e componentes além da atualização de todos os softwares que farão parte da solução por 36 (trinta e seis) meses, devendo portanto, ser fornecido com atualizações regulares de segurança e suporte técnico contínuo para garantir que o equipamento esteja sempre protegido contra as ameaças mais recentes.

**7.5** Para garantir a perfeita instalação da solução e de modo a possibilitar com que os colaboradores e servidores do Ministério da Cultura possam assumir a gerência da solução, fará parte da composição do fornecimento da solução a prestação dos serviços de instalação e transferência do conhecimento (treinamento), conforme itens ilustrados no quadro a seguir:

--	--	--	--

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE
1	Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação	Un	01
2	Serviço de Implantação	Un	01
3	Treinamento	Turma	01

**7.6.** O detalhamento da solução e demais especificações constam do Caderno de Especificações técnicas (documento anexo).

## 8. Levantamento de soluções

### 8.1. Identificação das Soluções

**8.1.1.** Os estudos elaborados pela Equipe de Planejamento da Contratação visam identificar, analisar e 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.

**8.1.2.** Dentre as opções disponíveis para atendimento da demanda, foram identificadas e analisadas as seguintes alternativas:

- **Solução 1:** Contratação de solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação em *appliance*.
- **Solução 2:** Contratação de solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação baseada em serviço (SaaS).
- **Solução 3:** Implantação de uma solução de software livre

## 9. Análise comparativa de soluções

### 9.1. Solução 1: Contratação de solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, em *appliance*.

**9.1.1 Descrição:** Este modelo prevê a aquisição dos equipamentos, softwares e treinamentos necessários à implantação da solução pela equipe do próprio MinC.

**9.1.2 Análise da Solução:** Nesta alternativa, todos os componentes da solução deverão ser adquiridos, estudados e operados pela equipe técnica do MinC.

**9.1.3** Sumariamente, a principal função de uma solução de detecção, análise e resposta (Network Detection and Response – NDR) é detectar tráfego suspeito na rede, abrangendo desde um usuário interno tentando acessar um sistema que não deveria, até uma tentativa criminosa de exfiltração de dados.

**9.1.4** Esse tipo de ferramenta coleta os dados da rede e aplica os recursos citados acima para identificar ameaças enquanto elas se movimentam entre um ponto e outro do ambiente de TIC.

**9.1.5** Comumente usa algoritmos especializados de inteligência artificial, de modo a assimilar o comportamento de todos os usuários internos, apontando anomalias causadas por roubo

de senhas, malware e movimento lateral, além de detectar e alertar sobre diversos tipos ataques cibernéticos.

**9.1.6** Esse tipo de solução de segurança é objeto de insights do Gartner, que a classifica assim: *"Os produtos de detecção e resposta de rede (NDR) detectam comportamentos anormais do sistema aplicando análises comportamentais aos dados de tráfego de rede. Eles analisam continuamente pacotes de rede bruto ou metadados de tráfego entre redes internas (leste-oeste) e redes públicas (norte-sul). O NDR pode ser entregue como uma combinação de dispositivos de hardware e software para sensores e um console de gerenciamento e orquestração na forma de um software no local ou SaaS". (tradução livre).*

**9.1.7** Para este cenário, foi efetuada pesquisa junto aos conteúdos divulgados pela Consultoria Gartner, onde foram identificados fabricantes que figuram como principais players do mercado na região da América Latina, conforme o quadro a seguir:

FABRICANTE	SOLUÇÃO
Darktrace	Darktrace DETECT/RESPONSE
Hillstone	Server Breach Detection System (sBDS)
Fortinet	FortiNDR
ExtraHop	ExtraHop Reveal(x)
ThreatBook	Threat Detection Platform (TDP)
Symantec	Symantec Security Analytics
IronNet	IronDefense
Gigamon	Gigamon ThreatINSIGHT
Stamus	Stamus Network Detection & Response (NDR)

Fonte: Gartner (<https://www.gartner.com/reviews/market/network-detection-and-response>)

**9.1.8** Oportuno ressaltar que inobstante a relevância da busca executada no site do Gartner na análise técnica para o presente Estudo Técnico, tal pesquisa tão somente exemplifica a variedade mercadológica de fornecedores na América Latina, não sendo utilizada como parâmetro exclusivamente para a escolha de soluções comerciais disponíveis, se prestando somente como base para compreensão das funcionalidades operacionais, cabendo aos licitantes participantes do certame apresentarem propostas em consonância com os requisitos estabelecidos no presente Estudo.

**9.1.9.** Entretanto, seguindo as boas práticas recomendadas pelo Tribunal de Contas da União, no sentido de aprimorar a transparência nos processos licitatórios, segue quadro com maior detalhamento das soluções que, em uma primeira análise, atendem às especificações exigidas pelo MinC:

FABRICANTE	MODELO/PART NUMBER
Trelix	XDR – TLXSUB-G
NetScout	Omnis® CyberStream and Omnis Cyber Intelligence
Hillstone	BDS-i2860-IN36/SG-6000-S3500-AD-IN36/SG-6000- ISC6305-SW-IN36
TrendMicro	Deep Discovery Inspector (DDI)

9.1.9.1. Importante destacar que o mercado de soluções é amplo, razão pela qual o termo de referência não limitou a oferta de soluções de um único fabricante. Nesse sentido, poderão participar da licitação empresas que ofertem outras soluções eventualmente não mapeadas, desde que atendam os requisitos técnicos mínimos exigidos pelo termo de referência.

## **9.2. Solução 2: Contratação de solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação, baseado em serviço (SaaS).**

**9.2.1 Descrição:** Este modelo prevê que a Contratada seja responsável por toda a operação.

**9.2.2 Análise da Solução:** Esta solução fundamenta-se na condução de toda a operação pela Contratada, ou seja, a Contratada fica responsável por operar em regime 24x7 (24 horas por dia, 7 dias por semana, 365 dias por ano).

**9.2.3** Neste modelo de contratação todos os equipamentos, licenças de software e profissionais qualificados devem ser providos pela Contratada, e devem ser capazes de atuar em todas as operações dentro do desempenho previsto.

**9.2.4** Esta solução é baseada na contratação de uma empresa prestadora de serviço, que será responsável por toda a plataforma operacional a ser integrada com o ambiente tecnológico do MinC, que deve prover e garantir a segurança de todos os ativos de TIC do Ministério.

**9.2.5** Nesta modalidade de solução, para assegurar tal proteção, a plataforma de serviço oferecida (Software as a Service – SaaS) deve ser totalmente integrada ao ambiente tecnológico do cliente, incluindo aí todos os módulos e componentes que a compõem, visando a instituição de um ambiente homogêneo de monitoração, prevenção, análise, investigação, inteligência, defesa e resposta a incidentes.

**9.2.6** O prestador do serviço obrigatoriamente opera em regime de 24 x 7 x 365, possuindo para isto processos, equipe de especialistas e ferramentas para o tratamento da segurança da informação, em conformidade com as boas práticas exercidas pela Administração e normativos legais vigentes que tratam do tema, como a ABNT ISSO/IEC 27001, as normas GSI/PR e a Lei Geral de Proteção de Dados (LGPD), dentre outros.

**9.2.7** Em geral, contratos deste tipo são baseados em SLA (Service Level Agreement), com um índice de disponibilidade dos serviços contratados de mínimo 99,7%.

## **9.3. Solução 3: Software Livre**

**9.3.1 Descrição:** Este modelo prevê que a utilização de softwares de código aberto.

**9.3.2 Análise da Solução:** Não há disponibilidade de solução de software livre capaz de atender aos requisitos técnicos nesse contexto. Esta solução apresenta alta complexidade, pois necessita de capacitação permanente da equipe de informática, falta de suporte técnico, baixa cobertura para malwares e não prevenção de novos incidentes de segurança. Além dessas dificuldades, o volume de tráfego de rede vem crescendo cada ano exigindo hardwares dedicados para essa função. Assim, esta opção está aos poucos sendo substituída por ferramentas pagas com suporte, gerenciamento unificado e garantia de funcionamento.

#### 9.4. Solução similar em outro órgão ou entidade da Administração Pública

##### 9.4.1. Pesquisa no Painel de Preços

**9.4.1.1.** Foi executada pesquisa de preços em Órgãos da Administração Pública, no site Painel de Preços (<https://paineldepregos.planejamento.gov.br/>) e complementarmente no Portal de Compras (<https://www.gov.br/compras/pt-br>), em conformidade com o disposto na legislação de regência (previsões legais que visam garantir a observância dos princípios da economicidade e eficiência nas contratações de soluções de TI), sob responsabilidade da Equipe de Planejamento da Contratação, a fim de averiguar a existência de contratações que englobassem aquisição de diversas soluções de detecção, análise e resposta de incidentes de segurança da informação, e cuja execução ou conclusão não tenha ultrapassado 1 (um) ano ao período da pesquisa. Cite-se, portanto, a pesquisa realizada, para fins de cumprimento da norma e verificação posterior da vantajosidade do procedimento de contratação escolhido pelo MinC.

UASG	ÓRGÃO	PREGÃO	OBJETO
	Secretaria de Fazenda de Pernambuco (SEFAZ/PE) <a href="https://www.peintegrado.pe.gov.br/Portal/Mural.aspx">https://www.peintegrado.pe.gov.br/Portal/Mural.aspx</a>	22/2022	Contratação de serviço especializado em segurança da informação, para realizar detecção, análise, resposta e restauração de incidentes de segurança da informação, com capacidade de tratar diariamente até 2.500 eventos por segundo (EPS).
010001	Câmara dos Deputados	33/2022	Prestação de serviços de monitoramento e apoio à resposta a incidentes de segurança cibernética, de varredura de vulnerabilidades e de inteligência contra ameaças cibernéticas, incluindo capacitação operacional, pelo período de 12 (doze) meses.).
	Banco do Brasil	2023/02544	Registro de Preços para aquisição de até 20 (vinte) equipamentos da solução física de Network Detection and Response (NDR), composta por um gerenciador centralizado, em que serão executadas as tarefas de administração, configuração e emissão de relatórios, com garantia técnica pelo período de 60 (sessenta) meses, conforme discriminado no ANEXO I do Edital que integra o instrumento convocatório da licitação em epígrafe

**9.4.1.2.** Examina-se na próxima seção, para cada solução, os aspectos previstos na IN SGD/ME nº 94/2022 que devem ser avaliados em uma contratação de TIC. Para efeito de estudo, foi realizada consulta ao catálogo de Software Público Brasileiro ([https://softwarepublico.gov.br/social/search/software\\_infos](https://softwarepublico.gov.br/social/search/software_infos)), onde efetivamente não foi possível identificar solução que pudesse vir a ser utilizada para atendimento às necessidades negociais do MinC, bem como aos requisitos tecnológicos identificados no presente Estudo Técnico, conforme observado nas figuras a seguir que apresenta o resultado da pesquisa no portal, utilizando como palavra-chave DETECÇÃO E RESPOSTA, TRÁFEGO DE REDE, PROTEÇÃO DESERVIDORES, NDR

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



A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 2			X
	Solução 3			X

**9.4.2.** Em conformidade com a Portaria STI/MP nº 46, de 28 de setembro de 2016, declara-se que a solução a ser contratada não se enquadra como Software Público Brasileiro.

## 10. Registro de soluções consideradas inviáveis

**Solução 2: Contratação da Solução como Serviço:** Conforme a análise nas contratações realizadas pela Administração, constantes no tópico “*Solução similar em outro órgão ou entidade da Administração Pública*”, somente uma parte da solução pode ser contratada como serviço – a prática adotada é a **aquisição** de solução composta por hardware e softwares específicos embarcados, com direito a suporte técnico.

Considerando que as atividades de monitoramento de rede e segurança são executadas pelas equipes técnicas da empresa contratada para sustentação de infraestrutura do Ministério da Cultura, uma eventual contratação de outros profissionais para a realização de serviços de forma a operar soluções de XDR e NDR poderia sombrear as atividades executadas pelos técnicos que atuam no contrato existente nesta Pasta.

**Solução 3: Software Livre:** Não foram identificadas soluções de software livre capazes de atender aos requisitos técnicos com a garantia de suporte em caso de falhas.

Além desse falto, verifica-se que devido a complexidade da solução, o uso de softwares livres requer aprendizagem contínua e maior tempo de atuação de especialistas para a realização de ajustes e customizações, neste sentido o uso de softwares livres não dispensaria o envolvimento de técnicos tanto na operação quanto a atualização dos softwares que serão utilizados.

Neste sentido a solução que apresenta alta complexidade, pois necessita de capacitação permanente da equipe de informática, poderá acarretar a falta de suporte técnico, baixa cobertura para malwares e não prevenção de novos incidentes de segurança. Além dessas dificuldades.

Considerando que as atividades de monitoramento de rede e segurança são executadas pelas equipes técnicas da empresa contratada para sustentação de infraestrutura do Ministério da Cultura, uma eventual contratação de outros profissionais para a realização de serviços de forma a operar soluções livres de XDR e NDR poderiam sombrear as atividades executadas pelos técnicos que atuam no contrato existente nesta Pasta.

## 11. Análise comparativa de custos (TCO)

**11.1.** Das três soluções apresentadas, a **Solução 1** - Contratação de Equipamentos e Softwares por appliance - foi considerada a melhor alternativa dentre as opções elencadas. Esta solução trata da aquisição dos equipamentos por meio de recursos orçamentários de investimentos com suporte e garantia.

**11.2.** O levantamento dos valores para a aquisição de bens e contratação de serviços em geral para os órgãos e entidades participantes do SISG - Sistema de Serviços Gerais, deve seguir os procedimentos administrativos definidos pela Instrução Normativa nº 65/2021 da Secretaria de

Gestão (SEGES) do Ministério da Economia. Este levantamento servirá para balizar a viabilidade financeira do projeto.

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

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

I - composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços em saúde, observado o índice de atualização de preços correspondente;

II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;

III - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;

IV - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou UASG 420001 Estudo Técnico Preliminar 3 /2023;

V - pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

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

**11.4.** Conforme orienta a referida Instrução Normativa e devidamente exposto no item 9.4.1.2 anterior, foi realizada pesquisa no Painel de Preços (disponível em <https://paineldepregos.planejamento.gov.br/>) no dia 19 de outubro de 2023 e verificou-se que três órgãos/entidades adquiriram bem similar ao objeto deste estudo, conforme segue:

ID	PREGÃO	FORNECEDOR	CONTRATANTE	DATA
1	22/2022	BID COMERCIO E SERVICOS EM TECNOLOGIA DA INFORMACAO LTDA	Secretaria de Fazenda de Pernambuco – SEFAZ-PE (926117)	05/08/2022
2	33/2022	ISH Tecnologia	Câmara dos Deputados (010001)	06/06/2022
3	02544 /2023	CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA	Banco do Brasil	Em andamento

**11.5.** Em que pesem os pregões encontrados, estes não servem como parâmetro válido pois os 2 primeiros tratam de contratação como serviço, (software as a service – SaaS) sem contemplar o fornecimento de hardware e software, e o ultimo (BB) contempla equipamentos bem maiores do que os aqui especificados, prejudicando a comparação.

**11.6.** Assim, dado o reduzido número de licitações encontradas, e a fim de se chegar ao valor estimado da contratação, foi também realizada pesquisa de preços com fornecedores do ramo, conforme segue:

ITEM	DESCRIÇÃO	UNID	QUANT	FORNECEDOR 1	FORNECEDOR 2	FORNECEDOR 3	FORNECEDOR 4
------	-----------	------	-------	-----------------	-----------------	-----------------	-----------------

1	Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	Un	01	4.245.000,00	4.439.680,00	5.204.900,00	4.219.420,00
2	Serviço de Implantação	Un	01	110.000,00	125.000,00	145.000,00	98.000,00
3	Treinamento	Turma	02	130.000,00	48.000,00	45.000,00	75.000,00
<b>VALOR TOTAL</b>				<b>4.615.000,00</b>	<b>4.660.680,00</b>	<b>5.439.900,00</b>	<b>4.467.420,00</b>

**11.7.** Assim, considerando o resultado das pesquisas elencadas no quadro anterior, temos os seguintes valores (médios) estimados para a presente contratação:

ITEM	DESCRIÇÃO	UNID	QUANT	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	Un	01	4.527.250,00	4.527.250,00
2	Serviço de Implantação	Un	01	119.500,00	119.500,00
3	Treinamento	Turma	02	74.500,00	149.000,00
<b>VALOR GLOBAL ESTIMADO DA CONTRATAÇÃO</b>					<b>4.795.750,00</b>

**11.8.** Registre-se, por oportuno, que para a obtenção do valor estimado de referência para a pretensa contratação, foi calculada a média simples dos valores obtidos na cotação com fornecedores do ramo.

**11.8.1** Conforme estabelece o parágrafo 2º do artigo 2º da Instrução Normativa nº 5/2014 – MP:

*“§2º Serão utilizados, como metodologia para obtenção do preço de referência para a contratação, a média, a mediana ou o menor dos valores obtidos na pesquisa de preços, desde que o cálculo incida sobre um conjunto de três ou mais preços, oriundos de um ou mais dos parâmetros adotados neste artigo, desconsiderados os valores inexequíveis e os excessivamente elevados. (Alterado pela Instrução Normativa nº 3, de 20 de abril de 2017)”*

**11.9.** Nessa linha, a definição do método para estabelecer o preço de referência para a aquisição /contratação é tarefa discricionária do gestor público. Esse foi o entendimento do Tribunal de Contas da União – TCU no Acórdão 4952/2012 – Plenário, que diz:

*“O menor preço deve ser utilizado apenas quando por motivo justificável não for mais vantajoso fazer uso da média ou mediana”.*

**11.10.** Esclarecemos:

**11.10.1** A média é a soma de todas as medições divididas pelo número de observações no conjunto de dado. Em razão de ser suscetível aos valores extremos, a média normalmente é utilizada quando os dados estão dispostos de forma homogênea.

**11.10.2** Já a mediana é o valor do meio que separa a metade maior da metade menor no conjunto de dados. Menos influenciada por valores muito altos ou muito baixos, a mediana pode ser adotada em casos onde os dados são apresentados de forma mais heterogênea e com um número pequeno que foge ao padrão.

**11.10.3.** Existem outras técnicas (média ponderada, média saneada e outras) que podem ser utilizadas desde que devidamente justificados pela autoridade competente. É importante ressaltar que o emprego de qualquer metodologia não pode resultar em equívoco ou levar a resultado diverso do fim almejado em lei.

**11.10.14** Pelo exposto, dado que os preços obtidos na cotação com fornecedores do ramo estão dispostos de forma homogênea (sem grandes distorções entre o maior e o menor valor encontrado), entende-se por correto o uso da média simples.

**11.10.15.** Ressalte-se por fim que, em obediência à norma de regência, o cálculo incidiu sobre um conjunto de quatro preços.

## 12. Descrição da solução de TIC a ser contratada

**12.1** Fornecimento e implantação de solução para realizar detecção, análise, resposta e monitoramento de incidentes de segurança da informação, com garantia de suporte técnico por 36 (trinta e seis) meses conforme detalhamento técnico constante no **Anexo I deste Estudo Técnico**.

## 13. Estimativa de custo total da contratação

**Valor (R\$):** 4.795.750,00

**13.1.** Assim, considerando o resultado das pesquisas elencadas no quadro anterior, temos os seguintes valores (médios) estimados para a presente contratação:

ITEM	DESCRIÇÃO	UNID	QUANT	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de monitoramento de comportamento anômalo da rede, detecção, análise, resposta e restauração de incidentes de segurança da informação.	Un	01	4.527.250,00	4.527.250,00
2	Serviço de Implantação	Un	01	119.500,00	119.500,00
3	Treinamento	Turma	02	74.500,00	149.000,00
VALOR GLOBAL ESTIMADO DA CONTRATAÇÃO					R\$ 4.795.750,00

## 14. Justificativa técnica da escolha da solução

**14.1.** Um dos pilares da área de segurança da informação é avaliar criticamente a cibersegurança do ambiente de TI, em particular os serviços disponibilizados na internet, por meio de monitoramento de diversas espécies de ameaças que incidem sobre os ativos que sustentam as operações das áreas de negócio, que agem com táticas e técnicas as mais variadas possíveis.

**14.2.** Já é de conhecimento público que diversos órgãos brasileiros são alvos de constantes ameaças, a exemplo o recente ataque ao Ministério da Saúde, onde o hacker atingiu o principal sistema do Ministério; o ataque a Secretaria de Fazenda do Rio de Janeiro, onde foram vazados 420Gb de dados e o ataque ao Sebrae, onde as máquinas virtuais foram atacadas e criptografadas fazendo o site e sistema ficarem fora do ar por vários dias. Além destes, também foram alvo de ataques STF, STJ, TRF 3ª Região, Justiça Federal de SP e MS, etc.

**14.3.** Por seu turno, o Ministério da Cultura desenvolve um importantíssimo papel dentro do Governo Federal, sendo responsável pelo planejamento e pela execução das políticas nacionais de cultura e de artes.

14.4. Com isso, o MinC lida todos os dias com elevada troca de informações, além de um grande e complexo volume de dados sensíveis de milhares de cidadãos do Brasil.

14.5. Além disso, em 2020 um novo cenário surgiu em decorrência da Covid-19. Processos de transformação digital das organizações públicas acabou por forçar às organizações a expandir seu ambiente de trabalho em regime remoto. Dessa forma os ambientes das organizações tornaram-se mais visíveis e vulneráveis a ataques com roubo de informações além da possibilidade de comprometimento do ambiente, o que leva à conclusão de que o MinC tenha um altíssimo nível de segurança cibernética.

14.6. Diante do avanço das ameaças cibernéticas, cada vez mais atuante no meio governamental, as ferramentas de segurança da informação também precisam se tornar cada vez mais diversas e sofisticadas no combate do avanço das invasões da rede.

14.7. Sendo assim, é de suma importância o investimento em soluções de Cibersegurança que compõe o ambiente, além da Segurança da Informação se fazer em camadas. A segurança em camadas consiste na disposição de várias etapas de proteção à operacionalidade da instituição, de modo a blindar seus arquivos e dados mais sensíveis contra ataques cibernéticos desde a camada física de rede até a camada de aplicações. Sendo assim, trata-se de uma metodologia que reforça as fronteiras digitais com vários muros de sustentação.

14.8. As camadas de segurança oferecem uma proteção maior, além de garantir que os criminosos tenham mais dificuldade na hora de tentar invadir um sistema, podendo até mesmo desestimular a tentativa.

14.9. Desta forma, apostar em estratégias de camadas de segurança traz diversos benefícios, tais como:

- i. Proteção contra malwares, ransomware, wannacry, botnet entre outros
- ii. Proteção contra vazamentos de dados e phishing
- iii. Segurança ágil e dinâmica
- iv. Oferece proteção mais forte, multicamadas

14.10. As camadas de segurança são fundamentais porque, caso uma das proteções falhe, a outra assume, mantendo os dados intactos. Uma só camada não é capaz de proteger toda a “superfície de ataque” cada vez mais ampla. Foi-se o tempo em que um firewall de rede posicionado na fronteira entre a rede interna e externa era suficiente para a proteção total.

14.11. A primeira camada a se proteger é a camada de rede. Essa camada protege tanto contra ataques vindos de fora, que possuem o objetivo de descobrir sistemas vulneráveis com senhas fracas, para conseguirem informações privilegiadas; como também na saída de acessos, para que não seja realizado acesso a sites não permitidos, vazamento de informações, e consumo indevido de banda, o que atrapalha na produtividade e desempenho da rede. Além disso, com o novo cenário de trabalho remoto e híbrido, é necessário considerar também o monitoramento e proteção dos dispositivos móveis, ou seja, dos endpoints como os notebooks, os próprios aparelhos celulares e tablets trazidos pelas pessoas dentro das políticas de BYOD (Bring Your Own Device).

14.12. Nesse sentido, entendendo a grande importância que os sistemas e serviços de TI adquiriram para as organizações e que se observa a constante diversificação e desenvolvimento de novas ameaças cibernéticas, percebemos que o Firewall, que exerce a segurança de perímetro de Rede, protegendo o tráfego Norte-Sul de ataques conhecidos, não é o suficiente para bloquear ataques mais sofisticados, além de não suprir a proteção Leste-Oeste e de ataques desconhecidos na rede.

14.13. Surge, então, a necessidade de uma ferramenta que proteja também o tráfego Leste-Oeste de ameaças não conhecidas. Ferramenta essa que usa inteligência artificial para estudar o comportamento da rede e, com isso, detectar comportamentos anômalos, até mesmo as menores e mais discretas tentativas do invasor fazendo a mitigação do ataque antes mesmo dele ocorrer. Essa ferramenta complementar o Firewall na proteção da camada de rede.

14.14. Dessa forma, o ambiente estará protegido de ameaças desconhecidas externas, além das internas que podem ocorrer com máquinas infectadas vindo de trabalho híbrido/remoto.

14.15. Assim, faz-se mister a utilização de um sistema de detecção e respostas, com a finalidade de tratar incidentes e garantir o prazo de reestabelecimento das operações e, consequentemente, a continuidade do serviço público.

14.16. Por fim, é necessário contextualizar que, com a vigência da Lei Federal nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD), a Autoridade Nacional de Proteção de Dados – ANPD, é competente para sancionar empresas e órgãos públicos envolvidos em incidentes que violam a privacidade de dados pessoais, o que impõe ao MinC, enquanto controlador desses dados, maior zelo e eficácia na vigilância de ameaças cibernéticas. segurança nos processos.

## **15. Justificativa econômica da escolha da solução**

**15.1.** Conforme demonstrado no item 11 - Análise comparativa de custos (TCO), só existe um tipo de solução viável.

**15.2.** Dado o reduzido número de licitações similares encontrado e a impossibilidade técnica de se aproveitar tais licitações para comparação e composição do valor estimada da aquisição pretendida, optou-se pela realização da pesquisa de mercado, em conformidade com a legislação de regência.

**15.3.** Desta forma, foram consultados 57 (cinquenta e sete) fornecedores do ramo. Destes, 04 (quatro) enviaram suas propostas comerciais e, a partir delas, apurou-se a média dos preços de mercado.

## **16. DO PARCELAMENTO DA CONTRATAÇÃO**

### **16.1. ASPECTOS TÉCNICOS**

**16.1.1.** Considerando o disposto no inciso I do §2º do art. 12 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, a Equipe de Planejamento da Contratação avaliou a viabilidade de *“realizar o parcelamento da solução de TIC a ser contratada, em tantos itens quanto se comprovarem tecnicamente viável e economicamente vantajoso”*.

**16.1.2.** O art. 40, inciso V, alínea “b” da Lei nº 14.133/2021, dispõe que:

*Art. 40 O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:*

*(...)*

*V - atendimento aos princípios:*

*(...)*

b) do parcelamento, quando for tecnicamente viável e economicamente vantajoso;

**16.1.3.** Similarmente, o Tribunal de Contas da União se manifestou sobre o tema através do disposto na Súmula n.º 247 de 2007: “É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade”

**16.1.4.** Todavia, nem sempre a licitação com o parcelamento do objeto é a mais eficiente em termos econômicos para a administração, especialmente quando considerados objetos de alta complexidade – o que é o caso da contratação em tela – cite-se como exemplo o Acórdão nº 3.140/2006 – TCU – 2ª Câmara, cujo trecho inerente está transcrito a seguir:

*“Cabe considerar, porém, que o modelo para a **contratação parcelada adotado nesse parecer utilizou uma excessiva pulverização dos serviços**. Para cada um de cinco prédios, previram-se vários contratos (ar-condicionado, instalações elétricas e eletrônicas, instalações hidrossanitárias, civil). Esta exagerada divisão de objeto pode maximizar a influência de fatores que contribuem para tornar mais dispendiosa a contratação (...) embora as estimativas numéricas não mostrem consistência, não há nos autos nenhuma evidência no sentido oposto, de que o parcelamento seria mais vantajoso para a Administração. Ao contrário, os indícios são coincidentes em considerar a licitação global mais econômica” (Acórdão nº 3140/2006 do TCU).*

**16.1.5.** Deste modo, para a pretendida aquisição se faz necessário a contratação de **solução única de TIC**, considerando questões técnicas, bem como o ganho de economia em escala, sem prejuízo à ampla competitividade, uma vez que existem no mercado várias empresas com capacidade de fornecer soluções que, não obstante possuírem características distintas, atendem ao mesmo objetivo. O agrupamento encontra ainda justificativa em decisões já deliberadas pelo TCU sobre a matéria, tais como, o Acórdão nº 5.260/2011 – TCU – 1ª Câmara, de 28/06/2011, que decidiu que *“Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si”*.

**16.1.6.** Ademais, em termos administrativos, a adjudicação do objeto desta contratação à Contratadas distintas, além de aumentar o custo administrativo (em ofensa aos princípios da economicidade, razoabilidade e eficiência), oportuniza que as eventuais Contratadas, eventualmente deixem de prestar o serviço contratado, alegando que a falha de um componente sob sua responsabilidade foi causada por falha de componente sob responsabilidade de outra Contratada, originando deste modo uma série de possibilidades e brechas para inconformidades, incongruências e desentendimentos.

**16.1.7.** De modo a impedir que esse cenário se torne realidade, comprometendo a disponibilidade dos serviços de TIC do MinC para com a sociedade brasileira, é fundamental que o objeto desta contratação seja adjudicado a uma única licitante.

**16.1.8.** Neste sentido, conforme exposto, a Equipe de Planejamento da Contratação optou pelo não parcelamento do objeto, e sim pela contratação de solução única, tendo em vista a garantia que a separação em itens distintos compromete técnica e administrativamente a aquisição e gestão do objeto, sendo deste modo estritamente necessária a aquisição de elementos de forma agrupada, não cabendo assim, o desmembramento do fornecimento.

## **16.2. ASPECTOS ECONÔMICOS**

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

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

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

## **17. JUSTIFICATIVA PARA REGISTRO DE PREÇOS**

**17.1.** A presente contratação é uma demanda oriunda da Lei nº 13.709, de 14 de agosto de 2018 – a Lei Geral de Proteção de Dados Pessoais (LGPD), que estabelece diretrizes para a regulamentação, tratamento e segurança de dados pessoais, por todas as entidades ou aqueles que, de alguma forma, captam informações sensíveis sobre os indivíduos, seja no meio digital ou não.

**17.2.** Como tal, as diretrizes oriundas da LGPD são de observância obrigatória para União, Estados, DF e Municípios. Nessa esteira, a Fundação Cultural Palmares manifestou interesse na aquisição da solução ora pretendida, conforme Ofício nº 212/2024/COP-Tecnologia da Informação /CGI/PR-FCP (SEI nº 1999070), constantes do processo SEI nº 01400.013417/2023-97.

**17.3.** Diante de tal situação, a adoção do Sistema de Registro de Preços (SRP) no presente caso vai ao encontro do que preconiza o inciso III do art. 3º, do Decreto 11.462/2023, que estabelece hipóteses em que a Administração Pública Federal pode utilizar a adoção do SRP, a saber:

*Art. 3º O SRP poderá ser adotado quando a Administração julgar pertinente, em especial:*

*(...)*

*III - quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas;*

**17.4.** Cabe ressaltar que a existência de preços registrados não obriga a Administração a firmar as contratações que deles poderão advir, ficando facultada a realização de licitação específica para aquisição, sendo assegurada ao beneficiário do registro a preferência de fornecimento em igualdade de condições.

### **17.5. Vigência do Registro de Preços**



1. O prazo de vigência da ata de registro de preços será de um ano, e poderá ser prorrogado por igual período, desde que comprovado que o preço é vantajoso, conforme dispõe o art. 22 do Decreto nº 11.462/2023.

#### **17.7. Da Adesão à Ata de Registro de Preços**

1. A Ata de Registro de Preços, durante sua validade, poderá ser utilizada por órgãos que não se manifestaram na Intenção de Registro de Preços e, conseqüentemente, não partícipes do certame licitatório.

### **18. Da Subcontratação**

- 18.1. Não será admitida a subcontratação.

### **19. Da Prova de Conceito**

- 19.1. A licitante classificada provisoriamente em primeiro lugar que tiver sua proposta de preços aceita e a documentação de habilitação aprovada poderá, a critério do MinC, ser convocada para executar prova de conceito, conforme as regras estabelecidas no **ANEXO II** deste documento.

### **20. Benefícios a serem alcançados com a contratação**

- 20.1. Entre os principais resultados e benefícios a serem obtidos com a implantação da solução a ser contratada, destacam-se:

1. Possibilitar o atendimento aos controles e diretrizes previstas na LGPD;
2. Mitigação de riscos de segurança da informação associados à exposição, perdas, violações e /ou vazamentos de dados intencionais ou não por usuários do MinC;
3. Diminuição de falsos positivos e negativos;
4. Diminuição do tratamento manual de incidentes;
5. Aumentar a taxa de automatização de detecção e respostas
6. Melhoria da qualidade dos serviços de TIC prestados pelo MinC à sociedade, com adoção das melhores práticas de mercado relativas à segurança da informação e comunicação;
7. Prevenir a ocorrência de incidentes cibernéticos que podem causar impactos à imagem e reputação do MinC, inclusive o que dispõe a Lei de Proteção de Dados Pessoais;
8. Alinhamento estratégico ao PDTIC, garantindo a entrega de valor para que as áreas finalísticas logrem alcançar seus objetivos específicos no âmbito da Missão Institucional do MinC;
9. Ampliar o índice de confiabilidade dos usuários em relação aos serviços prestados pela área de TIC do MinC, tendo em vista a garantia de segurança destes serviços com a implantação da solução;
10. Mitigar internamente os riscos de falhas na segurança dos dados institucionais, bem como identificar, investigar e tratar ocorrências, tendo em vista que a perda, roubo e/ou vazamento de dados do Órgão podem propiciar inúmeros inconvenientes e prejuízos financeiros tanto ao próprio MinC quanto aos usuários de seus sistemas.

## 21. Providências a serem Adotadas

### 21.1. Infraestrutura Tecnológica

1. Disponibilizar conexões físicas e lógicas destinadas ao equipamento a ser instalado.
2. Disponibilizar pontos de rede no switch-core para o appliance.

### 21.2 Infraestrutura Elétrica

1. Verificar disponibilidade de pontos da rede elétrica para ligação do equipamento.

## 22. Declaração de Viabilidade

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

### 22.1. Justificativa da Viabilidade

Em atendimento ao art. 11, Inciso V, § 1º e 3º, da Instrução Normativa SGD/ME nº 94/2022, a equipe de elaboração entende que o estudo de soluções viáveis para esta demanda está de acordo com as necessidades do MinC. Portanto, o presente Estudo Técnico Preliminar é justificadamente **viável** quanto aos requisitos de negócios, administrativos e técnicos a serem alcançados.

## 23. Responsáveis

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

Despacho: Portaria SPOA/MINC nº 230 (1959891)

**RAMON LEONN VICTOR MEDEIROS**

Integrante Requisitante



Assinou eletronicamente em 25/11/2024 às 18:38:38.

Despacho: Portaria SPOA/MINC nº 230 (1959891)

**FREDERICO GUIMARAES CARDOSO**

Integrante Administrativo



Assinou eletronicamente em 25/11/2024 às 17:59:01.

**WALLACE MOREIRA BASTOS**

Autoridade competente



*Assinou eletronicamente em 25/11/2024 às 17:53:20.*

Despacho: Portaria SPOA/MINC nº 230 (1959891)

**MARIA APARECIDA GOMES**

Integrante Técnico



*Assinou eletronicamente em 25/11/2024 às 17:53:32.*