SPOA/SE/MINC

Estudo Técnico Preliminar 35/2025

1. Informações Básicas

Número do processo: 01400.017979/2025-71

2. Descrição da necessidade

Contratação de Serviços Especializados de Tecnologia da Informação

2.1. Considerando a nova Estrutura Regimental do Ministério da Cultura, por meio do Decreto n° 11.336, de 1° de janeiro de 2023, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Cultura e remaneja cargos em comissão e funções de confiança, e considerando ainda a necessidade de se prover os devidos recursos tecnológicos para o ambiente de forma adequada, eficiente e segura, será realizado um estudo visando adquirir serviços técnicos especializados de Tecnologia da Informação e Comunicação. Estas soluções devem posicionar o MinC em conformidade com os padrões estabelecidos para os órgãos integrantes da Administração Pública Federal, observando a legislação vigente, em especial a Lei nº 14.133/2021 e a Instrução Normativa SGD/ME nº 94/2022, sem prejuízo da observância das diretrizes consolidadas na Instrução Normativa SGD/ME nº 01/2019, quando aplicáveis.

2.1.1 Delimitação do Objeto

O presente Estudo Técnico Preliminar tem por objeto a avaliação da contratação de serviços especializados de Tecnologia da Informação e Comunicação, de natureza continuada, estruturados de forma integrada e orientados a resultados, com vistas a ampliar a capacidade operacional, a segurança cibernética, a interoperabilidade, a governança de dados e a continuidade dos serviços digitais do Ministério da Cultura.

O objeto será organizado em macrocomponentes técnicos interdependentes, cuja execução integrada se justifica pela necessidade de interoperabilidade, gestão unificada de riscos, centralização de responsabilidades e mitigação de falhas de coordenação, conforme detalhado nas seções subsequentes.

2.1.2 Organização do Escopo em Macrocomponentes Técnicos

Para fins de planejamento da contratação, análise comparativa de alternativas tecnológicas e gerenciamento de riscos, as necessidades institucionais do Ministério da Cultura foram organizadas em macrocomponentes técnicos interdependentes.

Esses macrocomponentes representam conjuntos de capacidades essenciais para a sustentação, evolução e segurança dos serviços digitais culturais, não se confundindo com soluções específicas, marcas, fornecedores ou modelos contratuais.

A organização em macrocomponentes permite estruturar o objeto de forma lógica, coerente e aderente às diretrizes da Instrução Normativa SGD/ME nº 94/2022, possibilitando a avaliação integrada das necessidades institucionais, dos riscos, dos impactos técnicos e dos custos associados à contratação, em consonância com os princípios da Lei nº 14.133/2021.

De forma complementar, consideram-se as diretrizes consolidadas na Instrução Normativa SGD/ME nº 01/2019, no que couber, especialmente quanto às boas práticas de planejamento e organização de soluções de TIC.

Os macrocomponentes identificados são:

I – Conectividade e comunicação de dados;
II – Continuidade de serviços, backup e recuperação de desastres;
III – Segurança cibernética, gestão de identidades e resposta a incidentes;
IV – Infraestrutura computacional e serviços de nuvem;
V – Governança de dados, plataformas analíticas e interoperabilidade;
VI – Inteligência geoespacial e imageamento;
VII – Serviços transversais de gestão, capacitação e evolução tecnológica.

2.2. A Subsecretaria de Tecnologia da Informação e Inovação - STII executa competências com suporte em um considerável volume de serviços e recursos de infraestrutura tecnológica que, ao longo dos anos, tem sido sustentada, atualizada e evoluída de forma contínua, de modo a suportar as demandas de negócio. Essa variedade de soluções é composta por diversas tecnologias, que vão desde softwares prontos, soluções customizadas, aplicativos mobile, sites e portais, painéis e estruturas de análise de dados, estruturas de interoperabilidade, dentre outros.

2.3. É compreensível que o atendimento à demanda por serviços de TIC para uma organização de grande porte, como é o caso do Ministério da Cultura, requeira a adoção e manutenção de uma extensa diversidade de soluções, tecnologias e estratégias que habilitam a entrega de serviços com a qualidade requerida para todas as suas áreas demandantes.

2.4. Nesse contexto, de forma geral, as demandas a serem atendidas com a pretensão contratual dizem respeito às seguintes necessidades:

- A disponibilização de serviços voltados ao desenvolvimento e à manutenção de soluções de software, de modo a atender, por meio da área demandante, as solicitações do MinC;
- A oferta de serviços de suporte e continuidade das soluções de software, atendendo às exigências do Ministério, também por intermédio da área solicitante;
- O fortalecimento técnico-gerencial no que se refere ao planejamento, execução, acompanhamento, suporte e evolução dos sistemas e soluções de software utilizados pelo MinC;
- O aperfeiçoamento dos mecanismos de controle e conformidade relacionados aos serviços, resultados, processos e contratos da área de tecnologia da informação do MinC;
- O desenvolvimento da capacidade organizacional e o aumento da maturidade institucional nas práticas de engenharia de software.
- A implementação de serviço contínuo de análise e gestão de vulnerabilidades de segurança cibernética, capaz de identificar, classificar, priorizar e apoiar o tratamento tempestivo de fragilidades existentes em ativos de TIC do MinC, incluindo servidores, dispositivos de rede, estações de trabalho, aplicações, serviços em nuvem e ambientes de missão crítica, de forma aderente às diretrizes da IN SGD/ME nº 94/2022, da Portaria SGD/MGI nº 5.950/2023 e às políticas internas de segurança da informação.

2.5. Além disso, é imprescindível que a STII disponha de uma infraestrutura tecnológica eficiente, escalável e capaz de oferecer acesso ágil aos sistemas que sustentam as Políticas Públicas do Ministério da Cultura.

2.6. No entanto, na busca por atendimento às demandas de forma tempestiva e eficaz, a STII enfrenta alguns desafios:

2.6.1. Integração de sistemas heterogêneos

2.6.1.1. Ao longo dos anos, as soluções tecnológicas desenvolvidas no âmbito do Ministério da Cultura resultaram de esforços pontuais voltados ao atendimento imediato de demandas específicas das políticas públicas culturais. Essa abordagem gerou um ecossistema composto por sistemas diversos, com tecnologias e arquiteturas heterogêneas e, muitas vezes, sem integração entre si.

2.6.1.2. Tais soluções foram criadas com base nas necessidades e recursos disponíveis à época, sem um planejamento estruturado voltado para interoperabilidade, arquitetura em microserviços ou implantação em ambientes de nuvem.

2.6.1.3. A limitação da capacidade contratual atual compromete a atuação simultânea nas frentes de manutenção dos sistemas legados e de modernização tecnológica, dificultando a construção de uma plataforma integrada e interoperável para a gestão cultural.

2.6.2. Crescimento e dispersão dos dados culturais

2.6.2.1. A formulação de políticas culturais baseadas em evidências demanda um aumento substancial na coleta, estruturação e análise de dados culturais.

2.6.2.2. O setor cultural brasileiro é marcado por sua diversidade e descentralização, envolvendo entes federativos, instituições públicas e privadas, artistas, coletivos, espaços culturais independentes, entre outros. Contudo, ainda há carência de plataformas que facilitem a integração e o intercâmbio de dados entre esses atores. Em muitos casos, os registros culturais ainda são realizados de forma manual ou fragmentada, dificultando sua consolidação e análise.

2.6.2.3. Além do desafio tecnológico, é fundamental assegurar a proteção de dados pessoais de agentes culturais, especialmente em processos de fomento, cadastramento e difusão cultural.

2.6.3. Complexidade do ecossistema cultural

2.6.3.1. A complexidade das políticas culturais está associada à ampla diversidade de públicos, linguagens, territórios, expressões artísticas e estruturas organizacionais.

2.6.3.2. As soluções tecnológicas devem atender desde grandes instituições culturais até pequenos coletivos e iniciativas comunitárias, abrangendo equipamentos públicos (museus, centros culturais, bibliotecas), espaços independentes e iniciativas informais.

2.6.3.3. O público-alvo é igualmente plural: produtores, artistas, técnicos, gestores públicos e privados, além da população beneficiária das ações culturais. Deve-se ainda garantir a acessibilidade para pessoas com deficiência, respeitando as diretrizes de inclusão e equidade.

2.6.3.4. As estratégias de governo digital, como a ENGD e a EFGD, reforçam a necessidade de serviços públicos centrados no cidadão, interoperáveis e acessíveis, com foco na usabilidade e no reuso inteligente de dados existentes.

2.6.4. Infraestrutura tecnológica desatualizada

2.6.4.1. O avanço das políticas públicas digitais exige revisão dos modelos tradicionais de infraestrutura. Após um período de forte investimento em datacenters próprios e posterior migração parcial para ambientes de nuvem pública, o Governo Federal tem direcionado esforços à avaliação e ao fortalecimento de modelos de infraestrutura baseados em nuvem, incluindo iniciativas relacionadas à chamada nuvem soberana, a serem consideradas na análise comparativa de alternativas tecnológicas, à luz de critérios de segurança, conformidade normativa, custo, capacidade operacional e integração com o ecossistema governamental.

2.6.4.2. Entretanto, a infraestrutura tecnológica do MinC encontra-se defasada e vulnerável, resultado de um histórico de investimentos insuficientes e da falta de atualização contínua de seus ambientes computacionais, o que compromete a segurança, escalabilidade e inovação dos serviços digitais prestados à sociedade.

2.6.5. Segurança cibernética

2.6.5.1. O aumento da incidência e da sofisticação dos ataques cibernéticos a instituições públicas tem exigido ações proativas e contínuas de proteção da informação. A utilização de tecnologias como Inteligência Artificial por agentes maliciosos tem elevado o grau de risco e exigido maior vigilância e capacitação técnica.

2.6.5.2. O fator humano – servidores, terceirizados e dirigentes – continua sendo uma vulnerabilidade crítica, especialmente diante da falta de treinamento contínuo e da prática de utilização de dispositivos pessoais para fins profissionais.

2.6.5.3. A proteção dos dados sob custódia do Ministério da Cultura – incluindo cadastros de agentes culturais, dados de editais, políticas de fomento e obras protegidas por direitos autorais – é essencial para garantir a confiabilidade institucional e o cumprimento da LGPD.

2.6.5.4. Além disso, os longos prazos dos processos licitatórios retardam a adoção de soluções, ampliando o tempo de exposição a vulnerabilidades.

2.6.5.5. Considerando o aumento da superfície de ataque do Ministério da Cultura, aliado à elevada sofisticação das ameaças cibernéticas direcionadas à Administração Pública Federal, torna-se indispensável incorporar, como serviço complementar obrigatório da presente contratação, uma solução de gestão contínua de vulnerabilidades, capaz de identificar, classificar, priorizar e apoiar o tratamento tempestivo de fragilidades existentes em ativos de TIC.

2.6.5.6. Tal serviço permitirá a realização de varreduras automatizadas e sob demanda em servidores, dispositivos de rede, endpoints, aplicações, ambientes virtualizados e serviços críticos hospedados em infraestrutura própria ou contratada, com análise baseada em frameworks amplamente reconhecidos (CVSS, NIST, MITRE ATT&CK).

2.6.5.7. Ausência de estrutura formal e automatizada de Resposta a Incidentes e Forense Digital: a inexistência de uma frente institucionalizada, estruturada e padronizada de Resposta a Incidentes e Forense Digital compromete gravemente a capacidade do MinC de identificar rapidamente ataques, compreender sua extensão, delimitar responsabilidades, avaliar impactos, iniciar contramedidas e realizar restauração segura dos serviços afetados. Sem essa capacidade:

a) a detecção de incidentes ocorre tardiamente, em geral após danos significativos;

b) não há reconstrução precisa da linha de tempo dos fatos, dificultando o entendimento da causa raiz;

c) evidências digitais tornam-se inadmissíveis por falta de cadeia de custódia;

d) a resposta é reativa, fragmentada e com alto grau de dependência de terceiros;

e) riscos jurídicos aumentam, incluindo sanções LGPD, responsabilização administrativa e perdas patrimoniais;

f) o tempo médio de resposta (MTTR) se torna elevado, ampliando impacto institucional.

2.6.5.7.1 Assim, faz-se indispensável a implementação de uma solução avançada e integrada de Resposta a Incidentes e Forense Digital, alinhada às melhores práticas internacionais.
As capacidades de Resposta a Incidentes e Forense Digital descritas observam os princípios e diretrizes da Política Nacional de Segurança da Informação, instituída pelo Decreto nº 9.637/2018, bem como as Normas Complementares do Gabinete de Segurança Institucional da Presidência da República, no que se refere à detecção, resposta, registro, custódia de evidências e recuperação de incidentes de segurança da informação.

2.6.5.8. Exposição crescente a ransomware, ataques inteligentes e campanhas direcionadas (APT): a ausência de mecanismos especializados para prevenção e resposta a ransomware e ameaças avançadas (APT) expõe o Ministério da Cultura a riscos severos, em um cenário em que agentes maliciosos têm direcionado, de forma recorrente, suas campanhas a órgãos públicos, explorando fragilidades de infraestrutura, processos e pessoas.

2.6.5.8.1. Os ataques contemporâneos caracterizam-se por:

a) direcionamento a infraestruturas públicas essenciais, visando alto impacto e poder de pressão;
b) exploração de ambientes mistos (nuvem + legado + edge), tirando proveito de configurações complexas e, por vezes, heterogêneas;
c) foco em dados pessoais e culturais sensíveis, que possuem valor estratégico, econômico e simbólico;
d) uso de inteligência artificial, machine learning e polimorfismo para alterar dinamicamente o comportamento do malware;
e) adoção de técnicas de criptografia rápida (flash encryption) para reduzir o tempo de reação da equipe técnica;
f) utilização de modelos de extorsão dupla e tripla, envolvendo criptografia dos dados, ameaça de vazamento de informações sensíveis e chantagem sobre a indisponibilidade prolongada de serviços essenciais.
g) Essa lacuna de proteção específica contra ransomware e ameaças avançadas coloca o Ministério em situação de risco quanto a:

- indisponibilidade prolongada de sistemas críticos, com impacto direto na entrega de serviços à sociedade;

- paralisia sistêmica de sistemas de políticas públicas culturais, editais, fomento e gestão de acervos;
- violação de dados pessoais, com consequências no âmbito da LGPD, inclusive quanto à necessidade de comunicação à ANPD e aos titulares;
- perda ou comprometimento de acervo cultural digital, com danos muitas vezes irreversíveis;
- responsabilização administrativa, civil e penal de gestores e da instituição;
- gastos emergenciais elevados para reconstrução de ambientes, restauração de dados, contratação de consultorias de crise e comunicação institucional.

2.6.5.8.2. Diante desse cenário, a adoção de solução de Defesa contra Ransomware e Ameaças Avançadas deixa de ser um mecanismo opcional de reforço e passa a constituir condição indispensável para a sustentabilidade operacional, a resiliência cibernética e o cumprimento dos princípios de continuidade do serviço público, eficiência, economicidade e segurança da informação.

As capacidades e funcionalidades descritas nos itens anteriores não implicam, neste momento, a definição de solução tecnológica específica, fabricante, modelo de licenciamento ou arquitetura contratual, constituindo-se em requisitos funcionais e não funcionais mínimos, destinados a subsidiar a análise comparativa de alternativas tecnológicas a ser realizada nas seções subsequentes deste Estudo Técnico Preliminar, em observância aos princípios da competitividade, isonomia, planejamento, economicidade e motivação dos atos administrativos, conforme disposto na Lei nº 14.133/2021.

2.6.5.9. Limitação estrutural decorrente da inexistência de plataforma de Enterprise Security Management (ESM):

2.6.5.9.1. A atual inexistência de uma plataforma integrada de Enterprise Security Management (ESM) constitui vulnerabilidade estrutural que compromete de forma significativa a postura de segurança cibernética do Ministério da Cultura.

2.6.5.9.2. Sem um mecanismo centralizado de coleta, processamento, correlação, priorização e resposta a eventos de segurança:

a) não é possível estabelecer visibilidade única e contínua das superfícies de ataque que hoje se distribuem entre sistemas legados, nuvem pública, nuvem privada, edge, appliances, ambientes de terceiros e infraestrutura distribuída pelo território nacional;

b) a gestão de incidentes permanece fragmentada, dificultando a adoção efetiva de modelos como Zero Trust Architecture (ZTA), Defesa em Profundidade, Monitoramento Contínuo, ou Resposta Orquestrada a Incidentes (SOAR);

c) o MinC fica exposto a riscos elevados de lateralização de ameaças, escalonamento de privilégios, exploração de vulnerabilidades não corrigidas e ataques direcionados com uso de IA;

d) o cumprimento das obrigações legais (LGPD, E-Cyber, PPSI/MGI), bem como das normas internas de segurança, torna-se mais oneroso, demorado e sujeito a falhas;

e) informações estratégicas — incluindo dados pessoais sensíveis, bases de editais, registros culturais e ativos de valor histórico — permanecem sem mecanismo adequado de rastreabilidade e detecção precoce de acessos indevidos.

2.6.5.9.3. Assim, a implantação de ESM é condição indispensável para elevar o nível de maturidade em segurança cibernética e mitigar riscos de forma proativa e sustentada.

2.6.5.9.4. A ausência de mecanismos contínuos de auditoria e governança de dados aumenta o risco de manipulação indevida, acessos não autorizados, exclusões acidentais e fragilidades de integridade, comprometendo a confiabilidade institucional e a conformidade com a LGPD. A presente contratação deve mitigar esse risco mediante solução integrada de monitoramento, logging avançado, trilhas de auditoria e governança dos dados estratégicos do MinC.

A adoção das capacidades descritas alinha-se às diretrizes estratégicas vigentes do Governo Federal, em especial ao Plano Plurianual, à Lei de Diretrizes Orçamentárias e à Lei Orçamentária Anual aplicáveis ao exercício, bem como às

diretrizes internas de planejamento de TIC do Ministério da Cultura, não representando desvio de finalidade nem criação de despesa sem amparo no planejamento institucional.

2.6.5.9.5. A solução deve assegurar visão integrada e em tempo quase real do risco cibernético institucional, provendo relatórios executivos e técnicos, dashboards dinâmicos e mecanismos de correlação de vulnerabilidades com ameaças ativas. Seu objetivo primário é reduzir a janela de exposição, apoiar o saneamento de fragilidades estruturais e fornecer subsídios técnicos às equipes internas da STII para priorização de correções, hardening e mitigação de riscos, em atendimento às diretrizes da Portaria SGD/MGI nº 5.950/2023, da IN SGD nº 94/2022 e das políticas de segurança vigentes no Ministério da Cultura.

2.6.5.9.6. O serviço de análise de vulnerabilidades não altera a métrica contratual (USC/USI/USB/USE/USN), pois se caracteriza como requisito complementar obrigatório para fortalecer a proteção dos ambientes computacionais do MinC, garantindo aderência às boas práticas de segurança e resiliência operacional exigidas para sistemas críticos, sem gerar duplicidade de escopo ou sobreposição com as soluções já previstas no presente Estudo Técnico.

A definição do modelo de mensuração, estimativa de custos e impactos financeiros decorrentes da incorporação dos requisitos descritos será realizada em seção própria deste Estudo Técnico Preliminar, em conformidade com a Instrução Normativa SEGES/ME nº 65/2021, não implicando, neste momento, comprometimento orçamentário ou definição de valores.

2.6.5.9.7. Fragilidades no ciclo de vida de identidades e acessos: a inexistência de solução unificada de IAM expõe o Ministério da Cultura a um conjunto de fragilidades estruturais no ciclo de vida de identidades e acessos, que impactam diretamente a segurança cibernética, a continuidade dos serviços e a conformidade legal:

a) Contas órfãs e privilégios sem governança: ex-servidores, bolsistas, colaboradores temporários, terceirizados e prestadores de serviço podem manter acessos ativos mesmo após o encerramento de seus vínculos, em razão da ausência de processos automatizados de desprovisionamento. Isso resulta em contas órfãs, perfis não revistos e privilégios desnecessários, que podem ser explorados por atacantes ou utilizados indevidamente, ampliando o risco de acesso não autorizado a sistemas e dados sensíveis.

b) Falta de MFA em sistemas críticos: grande parte dos acessos a sistemas críticos ainda se apoia, predominantemente, em mecanismos de autenticação baseados apenas em usuário e senha, frequentemente frágeis e reutilizados em múltiplos serviços. Essa realidade torna o ambiente vulnerável a ataques de força bruta, campanhas de phishing, credential stuffing e reutilização de senhas vazadas, reduzindo significativamente a resiliência do Ministério frente a ameaças cibernéticas modernas.

c) Escalonamento lateral facilitado por credenciais comprometidas: na ausência de uma plataforma IAM que aplique políticas de menor privilégio, segregação de funções e monitoramento rigoroso de acessos privilegiados, credenciais comprometidas podem ser utilizadas para movimentação lateral em ambientes híbridos (datacenter, nuvem, SD-WAN, edge), permitindo que atacantes ampliem seu alcance, elevem privilégios e impactem múltiplos sistemas, bases de dados e serviços de missão crítica.

d) Inexistência de SSO e automação de provisionamento/desprovisionamento: a criação, alteração e exclusão de acessos é realizada de forma manual e fragmentada, com múltiplos pontos de solicitação e aprovação, o que aumenta a probabilidade de erros operacionais, atrasos na concessão ou revogação de permissões, inconsistências entre sistemas e dificuldade de rastrear quem autorizou cada acesso. A ausência de SSO também induz os usuários a manterem diversas senhas, muitas vezes inseguras.

e) Inconsistência das trilhas de auditoria de acesso: sem um repositório central que concentre logs de autenticação, autorização, elevação de privilégio e uso de credenciais, o MinC não dispõe de registro unificado e íntegro de todos os acessos realizados aos seus sistemas. Isso dificulta a reconstrução de cadeias de eventos em caso de incidente, prejudica a atuação de equipes de forense digital, fragiliza a prestação de informações a órgãos de controle e compromete a capacidade de demonstrar conformidade com a LGPD e com a PPSI/MGI.

f) Não aderência plena aos referenciais nacionais de segurança: LGPD, E-Cyber, PPSI/MGI, normas GSI/PR e as diretrizes internas de segurança da informação exigem governança de privilégios, segregação de funções, registro íntegro de acesso e mecanismos de prevenção e detecção de incidentes. A ausência de uma solução

IAM/IDMaaS impede o atendimento adequado a esses referenciais, expondo o Ministério ao risco de sanções regulatórias, recomendações de órgãos de controle e fragilização de sua imagem institucional.

As fragilidades descritas nos itens 2.6.5.5 a 2.6.5.8.7 constituem insumos diretos para a Matriz de Gerenciamento de Riscos da presente contratação, nos termos da Instrução Normativa SEGES/MP nº 05/2017 e do art. 20 da Lei nº 14.133/2021, considerando seus impactos potenciais sobre a continuidade do serviço público, a segurança da informação, a proteção de dados pessoais e a responsabilização institucional.

2.6.5.9.8. A inexistência de uma solução estruturada de PAM expõe o Ministério da Cultura a fragilidades graves na gestão e no uso de contas privilegiadas, dentre as quais destacam-se:

- Compartilhamento informal de credenciais administrativas: contas de administração de domínio, servidores, bancos de dados, aplicações e dispositivos de rede tendem a ser compartilhadas entre analistas e prestadores, sem registro individualizado, o que torna impossível identificar com precisão quem executou cada ação.
- Armazenamento inseguro de senhas críticas: sem cofre central, senhas privilegiadas tendem a ser mantidas em planilhas locais, arquivos de texto, sistemas não seguros ou até anotações físicas, constituindo vetor de risco significativo para uso indevido, vazamento e exploração por agentes maliciosos.
- Ausência de gravação e monitoramento de sessões privilegiadas: atualmente, ações de administração em sistemas críticos muitas vezes não são gravadas nem monitoradas em tempo real, o que compromete a capacidade de auditoria, dificulta a perícia digital e limita a responsabilização em casos de incidente ou mau uso.
- Rotação insuficiente de senhas privilegiadas: senhas privilegiadas tendem a permanecer ativas por longos períodos, às vezes por anos, inclusive após mudanças na equipe técnica, entrada de novos prestadores ou desligamento de colaboradores, aumentando a probabilidade de uso indevido ou continuidade de acesso por pessoas não autorizadas.
- Dificuldade de aplicar princípios de menor privilégio e just-in-time: sem um mecanismo de concessão temporária e controlada de privilégios, é comum que usuários permaneçam com acesso administrativo permanente a sistemas que não exigem tal nível de privilégio na rotina, ampliando o impacto potencial de credenciais comprometidas.
- Alto impacto de ataques de ransomware e APT com credenciais elevadas: em cenários de ransomware e ameaças avançadas (APT), a captura de credenciais privilegiadas permite ao atacante ampliar rapidamente o alcance do ataque, desabilitar controles, apagar logs, criptografar múltiplos servidores e comprometer backups, gerando risco elevado à continuidade dos serviços digitais culturais e à integridade de dados pessoais e do acervo cultural.

2.6.6. Sustentabilidade financeira das ações de TIC

2.6.6.1. A atual dotação orçamentária destinada à área de Tecnologia da Informação e Inovação do MinC está aquém das necessidades reais, cobrindo apenas uma fração da demanda anual. Frequentemente, é necessário buscar complementação orçamentária ao longo da execução.

2.6.6.3. Diretrizes emanadas do Ministério da Gestão e da Inovação em Serviços Públicos indicam a necessidade de avaliação de alternativas tecnológicas que envolvam a utilização de soluções providas por empresas públicas de TIC, no contexto de iniciativas como a Nuvem Soberana e a Infraestrutura Nacional de Dados, hipótese que poderá implicar, a depender da alternativa selecionada após análise comparativa, em otimização de custos e melhor alocação de recursos orçamentários..

2.6.7. Déficit de equipes técnicas especializadas

2.6.7.1 A baixa atratividade dos cargos de TI no governo federal tem resultado na redução do quadro de servidores efetivos, dificultando a manutenção de uma força de trabalho qualificada e estável nas áreas de tecnologia.

2.6.7.2. Para suprir essa lacuna, a alternativa tem sido a contratação de terceirizados, muitas vezes por meio de contratos com foco no menor preço, o que compromete a retenção de talentos e a formação continuada das equipes.

2.6.7.3. Essa realidade impacta diretamente na capacidade de planejamento, inovação e execução de projetos estratégicos de TIC no âmbito do Ministério da Cultura.

2.6.7.4. A atual capacidade operacional da Subsecretaria responsável por TIC encontra-se limitada em razão da escassez de servidores especializados, aliada à crescente complexidade técnica e administrativa envolvida na gestão, fiscalização e monitoramento de múltiplos contratos de tecnologia da informação. Tal cenário compromete a execução plena das atividades de planejamento, acompanhamento qualitativo, melhoria contínua de processos e governança das soluções de TIC, restringindo a atuação da equipe a atividades operacionais essenciais.

2.6.7.5. Em decorrência dessa limitação, a atuação da equipe técnica concentra-se predominantemente na verificação do atendimento aos requisitos mínimos contratuais, em detrimento de análises mais aprofundadas sobre a efetiva qualidade dos serviços prestados, oportunidades de aprimoramento, otimização de desempenho e produção sistemática de informações gerenciais e técnicas que subsidiem a tomada de decisão estratégica. Nesse contexto, a contratação de serviços especializados apresenta-se como alternativa necessária para ampliar a eficiência operacional, fortalecer a governança das soluções de TIC e assegurar a melhoria contínua do atendimento aos usuários dos serviços digitais do Ministério da Cultura.
A limitação de capacidade interna descrita não implica, por si só, a definição antecipada da forma de contratação ou do modelo de solução, constituindo-se em elemento técnico a ser considerado na análise comparativa de alternativas, incluindo a reorganização de processos internos, redistribuição de demandas, capacitação, automação e eventual contratação de serviços, conforme diretrizes da Instrução Normativa SGD/ME nº 01/2019 e da Lei nº 14.133/2021.

A insuficiência de capacidade técnica e operacional interna configura risco relevante à efetividade da contratação e à continuidade dos serviços digitais, devendo ser considerada na Matriz de Gerenciamento de Riscos do presente Estudo Técnico Preliminar.

2.6.8. Adaptação às novas tecnologias e demandas da sociedade

2.6.8.1. O avanço contínuo da tecnologia e sua ampla difusão na sociedade têm elevado as expectativas quanto à qualidade e à acessibilidade dos serviços públicos digitais.

2.6.8.2. O setor cultural, intensamente impactado pelas transformações tecnológicas, demanda soluções atualizadas, interoperáveis, interativas e adaptáveis a diferentes perfis sociais e regionais.

2.6.8.3. O público cultural – especialmente jovens, artistas e produtores independentes – está cada vez mais conectado e engajado com ferramentas digitais, exigindo do Estado respostas compatíveis com a linguagem, os meios e os canais contemporâneos.

2.6.8.4. Isso impõe ao MinC o desafio de inovar continuamente, promovendo o acesso à cultura também no ambiente digital, com equidade, inclusão e respeito à diversidade cultural.

2.7. Assim, a contratação de Serviços Especializados de Tecnologia da Informação visa ampliar a capacidade operacional do MinC, assegurando a oferta de serviços tecnológicos interoperáveis, estáveis e disponíveis de forma ininterrupta (24 horas por dia, 7 dias por semana) aos usuários da Pasta e à sociedade brasileira, promovendo o acesso contínuo às Políticas Públicas Culturais.

2.8. Diante das necessidades do Ministério da Cultura, que envolvem o fortalecimento das políticas públicas culturais por meio da digitalização de processos, da ampliação do acesso à cultura e da valorização da diversidade cultural brasileira, o Governo Federal tem promovido diversas iniciativas de modernização da administração pública. Essas ações visam fomentar a eficiência, a inclusão, a transparência, a celeridade e a entrega de valor ao cidadão, na construção de um Estado mais proativo, participativo e sustentável.

2.9. Nesse contexto, destaca-se a Estratégia Nacional de Governo Digital (ENGD), que tem como um de seus pilares a viabilização de uma Infraestrutura Pública Digital (IPD). Essa infraestrutura, quando implementada de forma integrada, permite a criação de plataformas digitais acessíveis, capazes de suportar serviços interconectados e uma gestão eficiente de dados públicos — elementos fundamentais para o planejamento, a execução e o monitoramento de políticas públicas culturais mais assertivas, descentralizadas e inclusivas.

2.10. A ENGD apresenta diretrizes estratégicas voltadas à articulação das iniciativas de governo digital em todos os entes federativos, com o propósito de ampliar e simplificar o acesso da população aos serviços públicos. Por meio de

um framework digital, busca-se otimizar e transformar digitalmente os serviços, tornando-os mais acessíveis, responsivos e alinhados às reais necessidades da sociedade — inclusive no campo da cultura, onde o acesso equitativo a bens, serviços e oportunidades culturais é um direito fundamental.

2.11. Essa estratégia visa consolidar um ecossistema de serviços públicos digitais interconectados, no qual a transformação digital se estabelece como base estruturante das políticas públicas. Para o avanço dessa visão, é imprescindível dispor de uma IPD sólida e eficaz, capaz de sustentar uma variedade de ferramentas e soluções digitais voltadas à gestão cultural, ao fomento, ao mapeamento de agentes e espaços culturais, à preservação do patrimônio e à difusão de conteúdos artísticos e culturais em ambiente digital.

2.12. Outro destaque relaciona-se à expertise das empresas públicas na disponibilização de produtos, infraestrutura, tecnologias, nuvem e ferramentas robustas e modernas que fomentam e desenvolvem o parque tecnológico sem a necessidade de replicação de estruturas locais para gestar e operacionalizar uma grande carga de dados, acessos que a demanda solicita, promovendo a ampliação da capacidade operacional do MinC em prover serviços de tecnologia interoperáveis, resilientes e disponíveis 24 horas x 7 dias para a sociedade brasileira, garantindo o acesso da população às Políticas Públicas Culturais.

2.13. Neste sentido, a presente contratação de Serviços Especializados de Tecnologia da Informação considera, entre as alternativas tecnológicas admissíveis, a possibilidade de utilização de soluções providas por empresas públicas federais de tecnologia, a ser avaliada comparativamente com outras opções, em consonância com os princípios da competitividade, economicidade e motivação dos atos administrativos, subsidiando, por meio do acesso aos dados por agentes decisores, a tomada de decisão para criação e aperfeiçoamento de políticas culturais.

2.14. As necessidades de cada solução a ser contratada estão especificadas abaixo, de forma justificada e detalhada.

2.15. Convém destacar que, por meio da contratação de um único fornecedor com capacidade técnica e operacional para a prestação integrada dos serviços, torna-se possível realizar uma contratação centralizada, o que simplifica a gestão por parte do Ministério da Cultura. Essa abordagem reduz a complexidade administrativa e transfere ao contratado a responsabilidade pela coordenação e execução dos serviços de TIC, aspecto especialmente relevante diante da limitação de mão de obra especializada atualmente disponível no MinC.
Considerando a limitação da capacidade operacional interna do Ministério da Cultura para gerenciar múltiplos contratos de elevada complexidade técnica, torna-se relevante avaliar modelos de contratação que possibilitem a centralização da gestão, a racionalização administrativa e a redução do esforço operacional, sem prejuízo à competitividade, à economicidade e à observância dos princípios que regem as contratações públicas, nos termos da Lei nº 14.133/2021 e da Instrução Normativa SGD/ME nº 01/2019.

2.16. As necessidades de cada solução a ser contratada estão especificadas abaixo, de forma justificada e detalhada.

2.17. Convém destacar que a adoção de uma contratação unificada, junto a fornecedor apto a assumir a gestão integrada dos serviços de TIC, contribui para a racionalização dos processos de acompanhamento e fiscalização contratual. Tal modelo permite que a maior complexidade técnica e operacional seja absorvida pelo contratado, mitigando riscos operacionais e compatibilizando a execução contratual com a capacidade instalada de recursos humanos do Ministério da Cultura.

2.18. A partir da análise das necessidades institucionais do Ministério da Cultura, identificam-se como escopos funcionais prioritários para a presente contratação os seguintes eixos de serviços de tecnologia da informação e comunicação, cuja viabilidade técnica e econômica será analisada nas seções subsequentes deste Estudo Técnico Preliminar:

1. **CONECTIVIDADE**
2. **BACKUP COMO SERVIÇO - BAAS**
3. **EDGE COMPUTING – SEGURANÇA E PROCESSAMENTO DE BORDA**
4. **INFRAESTUTURA COMO SERVIÇO – IAAS**
5. **PLATAFORMA COMO SERVIÇO – PAAS**
6. **IMAGEAMENTO**

A descrição dos eixos de serviços e das capacidades técnicas associadas não implica, neste momento, definição de fornecedor, tecnologia proprietária, arquitetura específica ou modelo contratual, constituindo-se em requisitos

funcionais e não funcionais mínimos que subsidiarão a análise comparativa de alternativas tecnológicas e de modelos de contratação, em conformidade com a Lei nº 14.133/2021.

2.19. Inseridos no contexto de cada um dos serviços ofertados pela empresa pública, detalhamos abaixo.

2.20. CONECTIVIDADE

2.20.1 O objetivo fundamental da contratação deste serviço é garantir infraestrutura segura e redundante para os sistemas e escritórios do MinC (Sede, Anexo, CTAv e Escritórios Estaduais).

2.20.2 Principais capacidades desejadas:

- SD-WAN (Software-Defined Wide Area Network): backbone híbrido com balanceamento e QoS entre links;
- Conectividade Dedicada (IP e MPLS): interligação entre datacenters MinC e empresa pública federal provedora de conectividade e infraestrutura de TIC, com redundância;

Os elementos técnicos descritos configuram requisitos funcionais e não funcionais mínimos, destinados a assegurar o atendimento às necessidades institucionais identificadas, não representando definição antecipada de tecnologia, fornecedor ou arquitetura específica, cuja avaliação ocorrerá em etapa própria deste Estudo Técnico Preliminar.

2.20.3. Está prevista, como evolução dos serviços contratados, a integração com a Rede Privativa de Governo Federal (RPGF) e suporte à 5G Gov para futuras expansões de conectividade cultural em campo.

2.20.4 No cenário atual, onde o acesso à rede global de informações (Internet) é essencial, onde estruturas descentralizadas precisam ter acesso direto aos sistemas da estrutura central e onde existe a necessidade de que servidores e colaboradores possam desempenhar suas funções onde quer que estejam, uma estrutura de comunicação de dados robusta e segura é vital para que o Ministério possa desempenhar suas funções com eficiência.

2.20.5 Ainda no âmbito da recriação do Ministério da Cultura, restabeleceram-se os escritórios estaduais, os quais passaram a demandar equipamentos e serviços de tecnologia da informação e esses serviços, dependem de conexão dessas unidades com a sede por meio de links de comunicação. Da mesma forma, as estruturas descentralizadas do Ministério localizadas em Brasília, a Biblioteca Demonstrativa de Brasília e os órgãos que funcionam no edifício Venâncio Shopping, assim como as localizadas no Rio de Janeiro, o Centro Técnico de Áudio Visual - CTAV e o Edifício Palácio Gustavo Capanema, dependem de conexão direta com o datacenter do Ministério para desempenharem suas funções.

2.20.6 No ano de 2025, o Edifício Gustavo Capanema, situado no Rio de Janeiro, o qual abriga unidades administrativas do Ministério da Cultura, do Iphan, bem como o respectivo Centro Cultural, foi reaberto, com visitação pública.

2.20.7 A solução atual de links de comunicação e acesso à internet, oferecida pela empresa Serviço Federal de Processamento de Dados – SERPRO, por meio do Contrato nº 01/2023, não atende às atuais necessidades, seja pelo grande crescimento da estrutura do Ministério experimentada desde sua recriação, seja em razão da reativação dos escritórios estaduais. A solução atual não tem se mostrado satisfatória, registrando recorrentes episódios de instabilidade e lentidão no serviço de interconexão e de acesso à Internet, o que compromete a continuidade das atividades do Ministério, além de não possuir a necessária capacidade de expansão para as outras unidades da Federação, essencial para o atendimento aos escritórios.

2.20.8 Desta forma, há necessidade de uma nova contratação que atenda às novas necessidades de comunicação entre a sede do Ministério, os mais de 24 escritórios estaduais e às estruturas descentralizadas, integrando e modernizando a infraestrutura de conectividade do Ministério da Cultura, de modo a garantir maior disponibilidade, desempenho, segurança e eficiência na troca de informações entre a sede e as unidades descentralizadas.

2.21 BACKUP COMO SERVIÇO – BAAS

2.21.1 O objetivo fundamental da contratação deste serviço é assegurar a continuidade operacional, preservação digital e recuperação de desastres para sistemas críticos (SALIC, SNC, Mapas da Cultura, SNIIC e Data Lake).

2.21.2 Principais serviços a serem contratados:

- Backup e Recuperação de Desastres (DRaaS): ambientes ativo-passivo com replicação geográfica entre empresa pública federal provedora de conectividade e infraestrutura de TIC e MinC;
- Gestão Documental Integrada: digitalização e versionamento seguro de acervos digitais e processos administrativos;
- Armazenamento e curadoria do acervo digitalizado do CTAV, permitindo a preservação das obras para além do meio físico;
- Backup Air-Gap e Anti-Ransomware: isolamento físico e criptográfico de cópias de segurança;
- Monitoramento e Relatórios de Integridade de Backup: verificação periódica automatizada;
- Retenção de longo prazo e arquivamento de dados culturais digitais.
- Está prevista como evolução, a adoção de modelos imutáveis (Object Lock) e integração nativa com o Data Lake MinC.

Os elementos técnicos descritos configuram requisitos funcionais e não funcionais mínimos, destinados a assegurar o atendimento às necessidades institucionais identificadas, não representando definição antecipada de tecnologia, fornecedor ou arquitetura específica, cuja avaliação ocorrerá em etapa própria deste Estudo Técnico Preliminar.

2.22 EDGE COMPUTING (Serviços de Segurança e Processamento de Borda)

2.22.1 O objetivo fundamental da contratação deste serviço é fortalecer a segurança cibernética e a observabilidade da infraestrutura do MinC, com arquitetura distribuída e inteligente.

2.22.2 Principais serviços a serem contratados:

- SIEM (Monitoramento de Eventos e Logs) – integração com o SOC empresa pública federal provedora de conectividade e infraestrutura de TIC;
- SOC (Security Operations Center) – monitoramento 24×7 com resposta a incidentes;
- IAM/IDMaaS (Gestão de Identidade e Acesso) – autenticação centralizada e MFA;
- PAM (Gestão de Acessos Privilegiados) – controle de contas críticas e sessões de administração;
- Análise de Vulnerabilidades e Compliance – varredura contínua de endpoints e servidores; existe um contrato atual que atende a esta necessidade. Entretanto, consta para futuras contratações centralizadas.
- XDR/NDR/EDR (Detecção e Resposta a Incidentes) – detecção comportamental e resposta automatizada; *existe um contrato atual que atende a esta necessidade*. *Entretanto, consta para futuras contratações centralizadas*.
- Anti-Ransomware e Defesa Avançada – proteção de borda com inteligência artificial;
- Resposta a Incidentes e Forense Digital – coleta e análise de evidências pós-ataque;
- ESM – Enterprise Security Management – orquestração de segurança e governança de incidentes;
- ITSM – Information Technology Service Management (Enterprise Service Management para serviços de TIC) – gestão integrada de serviços de TI, ativos, incidentes, requisições, mudanças e problemas, com suporte a automação, inteligência artificial (AIOps) e melhoria contínua dos serviços;
- WAF/CDN – proteção de aplicações web e APIs

Os elementos técnicos descritos configuram requisitos funcionais e não funcionais mínimos, destinados a assegurar o atendimento às necessidades institucionais identificadas, não representando definição antecipada de tecnologia, fornecedor ou arquitetura específica, cuja avaliação ocorrerá em etapa própria deste Estudo Técnico Preliminar.

2.22.3 Está prevista, como evolução, a integração com plataformas de IA para correlação de ameaças (AIOps /SecOps) e com o Data Lake MinC para análises preditivas de segurança.

As capacidades descritas nesta seção constituem requisitos funcionais e não funcionais mínimos, voltados à mitigação de riscos e à continuidade dos serviços digitais do Ministério, não implicando, neste momento, definição de fornecedor, marca, tecnologia proprietária, arquitetura específica ou modelo de contratação. A seleção da alternativa mais adequada ocorrerá após análise comparativa de opções, em conformidade com a Lei nº 14.133/2021 e a Instrução Normativa SGD/ME nº 01/2019.

2.22.4 Com relação à **ANÁLISE DE VULNERABILIDADES E COMPLIANCE**, a implementação de serviço contínuo de análise e gestão de vulnerabilidades de segurança cibernética, é capaz de identificar, classificar, priorizar e apoiar o tratamento tempestivo de fragilidades existentes em ativos de TIC do MinC, incluindo servidores, dispositivos de rede, estações de trabalho, aplicações, serviços em nuvem e ambientes de missão crítica, de forma aderente às diretrizes da IN SGD/ME nº 94/2022, da Portaria SGD/MGI nº 5.950/2023 e às políticas internas de segurança da informação.

2.22.4.1 Considerando o aumento da superfície de ataque do Ministério da Cultura, aliado à elevada sofisticação das ameaças cibernéticas direcionadas à Administração Pública Federal, torna-se indispensável incorporar, como serviço complementar obrigatório da presente contratação, uma solução de gestão contínua de vulnerabilidades, capaz de identificar, classificar, priorizar e apoiar o tratamento tempestivo de fragilidades existentes em ativos de TIC.

2.22.4.2 Tal serviço permitirá a realização de varreduras automatizadas e sob demanda em servidores, dispositivos de rede, endpoints, aplicações, ambientes virtualizados e serviços críticos hospedados em infraestrutura própria ou contratada, com análise baseada em frameworks amplamente reconhecidos (CVSS, NIST, MITRE ATT&CK).

2.22.4.3 A solução deve assegurar visão integrada e em tempo quase real do risco cibernético institucional, provendo relatórios executivos e técnicos, dashboards dinâmicos e mecanismos de correlação de vulnerabilidades com ameaças ativas. Seu objetivo primário é reduzir a janela de exposição, apoiar o saneamento de fragilidades estruturais e fornecer subsídios técnicos às equipes internas da STII para priorização de correções, hardening e mitigação de riscos, em atendimento às diretrizes da Portaria SGD/MGI nº 5.950/2023, da IN SGD nº 94/2022 e das políticas de segurança vigentes no Ministério da Cultura.

2.22.4.4 O serviço de análise de vulnerabilidades não altera a métrica contratual (USC/USI/USB/USE/USN), pois se caracteriza como requisito complementar obrigatório para fortalecer a proteção dos ambientes computacionais do MinC, garantindo aderência às boas práticas de segurança e resiliência operacional exigidas para sistemas críticos, sem gerar duplicidade de escopo ou sobreposição com as soluções já previstas no presente Estudo Técnico.
O dimensionamento, a estimativa de custos e os impactos financeiros decorrentes das capacidades de gestão contínua de vulnerabilidades serão tratados em seção própria deste ETP, conforme a Instrução Normativa SEGES /ME nº 65/2021, e os riscos associados subsidiarão a Matriz de Gerenciamento de Riscos, nos termos da Instrução Normativa SEGES/MP nº 05/2017 e do art. 20 da Lei nº 14.133/2021.

2.22.5 No tocante aos serviços de **ESM – Enterprise Security Management,** a implantação de uma solução integrada, escalável e continuamente atualizável de Enterprise Security Management (ESM) mostra-se essencial para consolidar, no âmbito do Ministério da Cultura, um ecossistema de proteção cibernética que opere sob os princípios de centralização, padronização, automação e governança contínua.

2.22.5.1 Recomenda-se que a solução contemple promover a integração de todo o conjunto de ativos críticos do MinC, incluindo servidores on-premisses, ambientes de nuvem híbrida, infraestrutura SD-WAN, appliances de segurança, dispositivos de rede, sistemas de missão crítica, bases de dados sensíveis, aplicações web e mobile, ferramentas de IA, automações e fluxos operacionais específicos da Pasta.

2.22.5.2 Como requisito mínimo, espera-se que a solução de ESM deverá contemplar:

- correlação avançada de eventos de segurança, utilizando modelos comportamentais, análise de contexto e detecção de anomalias;
- orquestração automatizada de respostas a incidentes, reduzindo o tempo de detecção (MTTD) e o tempo de resposta (MTTR);
- gestão unificada de políticas de segurança, permitindo controle centralizado sobre configurações, auditorias, inventários e trilhas de auditoria; compliance contínuo, garantindo aderência permanente às normas aplicáveis, incluindo LGPD, E-Cyber, PPSI /MGI, Normas Internas de Segurança da Informação, IN GSI/PR nº 4/2020 e nº 5/2021, e demais marcos regulatórios;
- visibilidade holística do risco tecnológico, consolidando indicadores operacionais, estratégicos e de governança em dashboards executivos para a Alta Administração;
- integração nativa com soluções já existentes no MinC, como auditoria de dados, IAM, análise de vulnerabilidades, backup seguro, hiperconvergência e Service Desk baseado em IA;

- rastreabilidade completa de ações, eventos, acessos, decisões e fluxos internos, garantindo governança e responsabilização. A ausência dessa camada integrada de ESM impede a operação segura, coordenada e tempestiva dos serviços digitais culturais, especialmente considerando o aumento do volume de dados, a sensibilidade das informações tratadas e a sofisticação crescente das ameaças externas e internas.
- Com relação aos serviços de RESPOSTA A INCIDENTES E FORENSE DIGITAL, vislumbramos a implementação de capacidades avançadas de Resposta a Incidentes e Forense Digital.
- A atuação tempestiva, coordenada e tecnicamente estruturada em casos de incidentes cibernéticos é um requisito indispensável para a continuidade das atividades institucionais do Ministério da Cultura. Para tal, torna-se necessária a implantação de capacidade integrada de Resposta a Incidentes e Forense Digital, de modo a possibilitar:

    - detecção precoce, contenção imediata, mitigação e erradicação de ameaças, conforme marcos da IN GSI /PR nº 4/2020;
    - identificação, preservação, coleta, cadeia de custódia, análise e documentação forense de evidências digitais, preservando integridade, autenticidade e admissibilidade jurídica;
    - apoio direto à tomada de decisão institucional, oferecendo relatórios técnico-jurídicos com rastreabilidade, reconstrução de linha do tempo, verificação de impactos e avaliação da materialidade;
    - gestão coordenada de incidentes multidomínio, envolvendo ESM, IAM, Auditoria, Vulnerabilidades, SD-WAN e demais soluções integradas;
    - integração plena ao PPSI/MGI, garantindo que todos os fluxos e artefatos sigam os protocolos nacionais de proteção de ativos críticos.

2.22.5.3 A ausência dessa capacidade deixa o MinC exposto a riscos severos, como prolongamento de incidentes, destruição de evidências, vazamentos de dados culturais sensíveis, responsabilização legal e interrupção prolongada de serviços.

2.22.6 Quanto ao tópico **DEFESA CONTRA RANSOMWARE E AMEAÇAS AVANÇADAS**, serão realizados serviços para a implementação de mecanismos avançados de Defesa contra Ransomware e Ameaças Avançadas (APT).

2.22.6.1 No contexto de crescente sofisticação dos ataques cibernéticos direcionados à Administração Pública Federal, torna-se imprescindível ao Ministério da Cultura (MinC) a adoção de solução especializada de Defesa contra Ransomware e Ameaças Avançadas (Advanced Persistent Threats – APT), capaz de atuar de forma preventiva, detectiva e reativa, assegurando a continuidade dos serviços digitais culturais e a proteção dos dados sob sua custódia.

2.22.6.2 Como requisito mínimo, a solução deve contemplar mecanismos específicos para identificação, bloqueio, isolamento, contenção e erradicação de ataques sofisticados que utilizam, dentre outras técnicas:

- fileless malware, com execução direta em memória, dificultando sua detecção por antivírus tradicionais;
- exploração de vulnerabilidades zero-day, antes da disponibilização de atualizações pelos fabricantes;
- escalonamento indevido de privilégios, visando a obtenção de credenciais administrativas;
- movimentação lateral furtiva em redes internas, buscando servidores críticos e bases de dados sensíveis;
- criptografia de dados em ambientes híbridos (on-premisses, nuvem, edge computing), com impacto direto sobre sistemas de missão crítica;
- exfiltração automatizada de informações para servidores remotos controlados por agentes maliciosos;
- uso de inteligência artificial e técnicas de polimorfismo, tornando o código malicioso dinâmico, variável e de difícil assinatura.

2.22.6.3 A solução deverá atuar antes, durante e após o ataque, contemplando, no mínimo:

- prevenção ativa, com bloqueio automático de padrões de comportamento e assinaturas maliciosas;
- detecção comportamental (IOA/IOC), baseada em anomalias de uso de recursos, processos e tráfego de rede;
- mecanismos anti-encriptação, capazes de impedir ou interromper rapidamente a criptografia não autorizada de arquivos e volumes;
- rollback automático de arquivos e sistemas, para restauração dos dados ao estado anterior à infecção, sempre que tecnicamente possível;
- contenção imediata de hosts comprometidos, por meio de isolamento lógico e restrição de comunicação;

- bloqueio de canais de comunicação de comando e controle (C2), impedindo o controle remoto da infraestrutura comprometida;
- registro detalhado de logs e trilhas de auditoria, de forma a subsidiar ações de forense digital, responsabilização e melhoria contínua.

2.22.6.4 A inexistência dessa camada especializada de defesa contra ransomware e APT mantém os serviços digitais do MinC, muitos deles classificados como serviços de missão crítica, expostos a risco elevado de interrupção prolongada, destruição ou indisponibilidade de dados, danos à integridade de acervos culturais, impacto negativo à imagem institucional e potenciais prejuízos financeiros e regulatórios, inclusive no tocante ao cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) e da Política de Segurança da Informação e Comunicações do órgão.

2.22.6.5 Ainda em relação à segurança da informação, as soluções de SIEM/SOC - Security Information and Event Management integrada ao SOC da empresa pública federal provedora de conectividade e infraestrutura de TIC são necessárias, pois a adoção de solução de Gerenciamento de Eventos e Informações de Segurança (SIEM), integrada ao Security Operations Center (SOC) da empresa pública federal provedora de conectividade e infraestrutura de TIC, permitem viabilizar a coleta centralizada, normalização, correlação e análise em tempo quase real dos logs e eventos de segurança de todos os ambientes do Ministério da Cultura (datacenters, nuvens públicas, redes, aplicações, endpoints e dispositivos de borda).

Ainda em relação à segurança da informação, as capacidades de SIEM/SOC são necessárias, pois viabilizam a coleta centralizada, normalização, correlação e análise em tempo quase real de logs e eventos de segurança dos ambientes do Ministério da Cultura (datacenters, nuvens públicas, redes, aplicações, endpoints e dispositivos de borda), com suporte a operação 24×7, investigação e tratamento de incidentes, conforme modelo de contratação a ser definido após análise comparativa de alternativas.

2.22.6.6 A solução deverá:

- receber e tratar eventos oriundos de, no mínimo, 600 fontes simultâneas, com capacidade inicial de 60 GB/dia de logs, escalável por acréscimo de licenciamento e infraestrutura;
- suportar ambientes distribuídos, com coletores multitenant para sites remotos, sobreposição de endereços IP (overlapping) e virtualização em Hypervisor padrão (VMware, Hyper-V, KVM);
- oferecer dashboards de risco, alertas em tempo real e trilhas de auditoria para apoiar LGPD, PPSI/MGI, ECyber e normas internas de Segurança da Informação;
- operar de forma integrada ao SOC da empresa pública federal provedora de conectividade e infraestrutura de TIC, de modo que a equipe 24×7 possa investigar, classificar e tratar incidentes, emitindo relatórios técnicos e executivos periódicos.
- Sem essa solução, o MinC permanece com visão fragmentada dos eventos de segurança, com baixo grau de correlação entre camadas (rede, aplicação, identidade, endpoint) e reduzida capacidade de detecção precoce de ataques sofisticados.

Os quantitativos iniciais indicados (fontes simultâneas e volume diário de logs) representam estimativas preliminares baseadas no inventário atual de ativos e na projeção de expansão dos serviços digitais, devendo ser validados e refinados na fase de dimensionamento e estimativa de preços, conforme IN SEGES/ME nº 65/2021, de forma a evitar superdimensionamento e garantir economicidade.

2.22.7. No tocante à gestão dos usuários e acessos, as soluções d**e IAM/IDMAAS (GESTÃO DE IDENTIDADE E ACESSO) – AUTENTICAÇÃO CENTRALIZADA E MFA** são imprescindíveis ao Ministério da Cultura, porque ao adotar uma solução de Identity and Access Management (IAM) / Identity Management as a Service (IDMaaS) é possível realizar a gestão unificada, integrada, rastreável e segura de identidades e acessos, abrangendo servidores, usuários internos e externos, prestadores de serviço, bolsistas, colaboradores temporários, sistemas de missão crítica, aplicações legadas, aplicações em nuvem, serviços expostos na internet, ambientes SD-WAN e plataformas de edge computing.

2.22.7.1. Essa solução deverá atuar como camada estruturante da segurança lógica do MinC, funcionando como ponto único de verdade para identidades, perfis, credenciais, permissões e políticas de acesso, de forma alinhada às diretrizes da LGPD, da PPSI/MGI, da Estratégia Nacional de Segurança Cibernética (E-Cyber) e das normas internas de segurança da informação.

2.22.7.2. A solução deverá, no mínimo:

- centralizar identidades em um diretório mestre, com sincronização bidirecional com Active Directory, serviços de diretório em nuvem e demais repositórios de identidade, reduzindo inconsistências cadastrais e evitando múltiplas versões de uma mesma identidade em sistemas distintos;
- garantir que o acesso aos sistemas ocorra com base no princípio do menor privilégio, vinculando perfis de acesso a papéis (roles), funções e lotações, de forma que cada usuário possua apenas as permissões estritamente necessárias ao exercício de suas atividades, com mecanismos de revisão periódica (recertificação) de perfis e grupos;
- oferecer autenticação multifator (MFA) obrigatória para todos os perfis sensíveis, incluindo dirigentes, administradores de sistemas, desenvolvedores, usuários com acesso a dados pessoais e contas de serviço críticas, com suporte a múltiplos fatores (aplicativo autenticador, token, push notification, biometria, entre outros), mitigando o risco de uso indevido de credenciais;
- fornecer Single Sign-On (SSO) para aplicações internas e externas, de modo a permitir que o usuário, após uma autenticação forte, acesse de forma integrada os diferentes sistemas corporativos, reduzindo a necessidade de múltiplas senhas, o risco de anotações indevidas de credenciais e o esforço de suporte relacionado à recuperação de senha;
- prover automação de provisionamento e desprovisionamento de acessos, de forma alinhada ao ciclo de vida do usuário (ingresso, movimentação, afastamento, desligamento), eliminando contas órfãs, acessos residuais e privilégios acumulados, com definição de fluxos de aprovação e registro formal de todas as concessões e revogações;
- registrar trilhas completas de auditoria, mantendo histórico detalhado de “quem acessou o quê, quando, onde e como”, incluindo IP de origem, dispositivo, horário, sistema acessado, tipo de operação e resultado (sucesso/falha), de modo a subsidiar auditorias internas, externas, órgãos de controle, atividades de forense digital e comunicação de incidentes à ANPD, quando aplicável; Integrar-se nativamente às demais camadas de segurança já previstas ou em contratação pelo MinC (ESM, SOC, SIEM, Resposta a Incidentes e Forense Digital, Defesa contra Ransomware e Ameaças Avançadas, gestão de vulnerabilidades, backup, SD-WAN e soluções de edge computing), permitindo correlação de eventos, bloqueio automático de contas comprometidas e aplicação coordenada de medidas de contenção e remediação.
- Sem uma plataforma IAM estruturada, o MinC permanece exposto a riscos como: existência de contas órfãs e privilégios indevidos; escalonamento ilegítimo de acessos por atacantes; falhas na revogação oportuna de acessos de ex-servidores e terceirizados; aumento da superfície de ataque por credenciais frágeis; e violações de dados pessoais decorrentes de má governança de identidade, com potencial responsabilização administrativa, civil e penal da Administração.
- Fragilidades no ciclo de vida de identidades e acessos

2.22.7.3. A inexistência de solução unificada de IAM expõe o Ministério da Cultura a um conjunto de fragilidades estruturais no ciclo de vida de identidades e acessos, que impactam diretamente a segurança cibernética, a continuidade dos serviços e a conformidade legal:

2.22.7.3.1 Contas órfãs e privilégios sem governança

a) Ex-servidores, bolsistas, colaboradores temporários, terceirizados e prestadores de serviço podem manter acessos ativos mesmo após o encerramento de seus vínculos, em razão da ausência de processos automatizados de desprovisionamento. Isso resulta em contas órfãs, perfis não revistos e privilégios desnecessários, que podem ser explorados por atacantes ou utilizados indevidamente, ampliando o risco de acesso não autorizado a sistemas e dados sensíveis.

2.22.7.3.2 Falta de MFA em sistemas críticos

a) Grande parte dos acessos a sistemas críticos ainda se apoia, predominantemente, em mecanismos de autenticação baseados apenas em usuário e senha, frequentemente frágeis e reutilizados em múltiplos serviços. Essa realidade torna o ambiente vulnerável a ataques de força bruta, campanhas de phishing, credential stuffing e

reutilização de senhas vazadas, reduzindo significativamente a resiliência do Ministério frente a ameaças cibernéticas modernas.

2.22.7.3.3 Escalonamento lateral facilitado por credenciais comprometidas

a) Na ausência de uma plataforma IAM que aplique políticas de menor privilégio, segregação de funções e monitoramento rigoroso de acessos privilegiados, credenciais comprometidas podem ser utilizadas para movimentação lateral em ambientes híbridos (datacenter, nuvem, SD-WAN, edge), permitindo que atacantes ampliem seu alcance, elevem privilégios e impactem múltiplos sistemas, bases de dados e serviços de missão crítica.

2.22.7.3.4 Inexistência de SSO e automação de provisionamento/desprovisionamento

a) A criação, alteração e exclusão de acessos é realizada de forma manual e fragmentada, com múltiplos pontos de solicitação e aprovação, o que aumenta a probabilidade de erros operacionais, atrasos na concessão ou revogação de permissões, inconsistências entre sistemas e dificuldade de rastrear quem autorizou cada acesso. A ausência de SSO também induz os usuários a manterem diversas senhas, muitas vezes inseguras.

2.22.7.3.5 Inconsistência das trilhas de auditoria de acesso

a) Sem um repositório central que concentre logs de autenticação, autorização, elevação de privilégio e uso de credenciais, o MinC não dispõe de registro unificado e íntegro de todos os acessos realizados aos seus sistemas. Isso dificulta a reconstrução de cadeias de eventos em caso de incidente, prejudica a atuação de equipes de forense digital, fragiliza a prestação de informações a órgãos de controle e compromete a capacidade de demonstrar conformidade com a LGPD e com a PPSI/MGI.

2.22.7.3.6 Não aderência plena aos referenciais nacionais de segurança

a) LGPD, E-Cyber, PPSI/MGI, normas GSI/PR e as diretrizes internas de segurança da informação exigem governança de privilégios, segregação de funções, registro íntegro de acesso e mecanismos de prevenção e detecção de incidentes. A ausência de uma solução IAM/IDMaaS impede o atendimento adequado a esses referenciais, expondo o Ministério ao risco de sanções regulatórias, recomendações de órgãos de controle e fragilização de sua imagem institucional.

2.22.7.3.7 Garantia de segurança de identidades e acessos

Os requisitos e capacidades descritos nesta subseção constituem necessidades funcionais e não funcionais mínimas para mitigação de riscos e conformidade normativa, não implicando definição de fornecedor, marca, solução proprietária, arquitetura específica ou modelo contratual. A seleção da alternativa mais adequada será realizada após análise comparativa, conforme a Lei nº 14.133/2021 e a Instrução Normativa SGD/ME nº 01/2019.

a) O Ministério da Cultura necessita implementar uma solução IAM/IDMaaS que assegure a segurança, rastreabilidade e governança de identidades e acessos ao longo de todo o ciclo de vida dos usuários, contas de serviço e aplicações, com vistas a:

- Reduzir o acesso indevido, por meio da exigência de autenticação multifator (MFA) para perfis de maior risco, da aplicação consistente de políticas de menor privilégio e da centralização da autorização em mecanismos de controle baseados em papéis (RBAC/ABAC), reduzindo a probabilidade de uso malicioso de credenciais;
- Padronizar e automatizar os processos de criação, alteração e exclusão de contas, com fluxos formais de aprovação vinculados a cargos, funções, lotações e projetos, de modo a garantir que a concessão de privilégios seja sempre motivada por necessidade de negócio, com registro explícito de quem solicitou, aprovou e executou cada ação;

- Eliminar perfis órfãos e privilégios acumulados, por meio de rotinas de recertificação periódica de acessos, detecção de contas inativas, revisão de grupos de segurança e expiração automática de acessos temporários, garantindo que somente usuários em efetivo exercício e com vínculo vigente mantenham acesso aos sistemas;
- Registrar e rastrear acessos de alto privilégio, permitindo que ações sensíveis (criação de usuários, alteração de perfis, acesso a dados pessoais, mudanças de configuração crítica) sejam monitoradas, associadas a identidades específicas e passíveis de auditoria posterior, inclusive para fins de responsabilização;
- Suportar auditorias internas, externas e de órgãos de controle, com relatórios estruturados que evidenciem o atendimento a requisitos de segregação de funções, trilhas de auditoria, governança de privilégios e controles de acesso a dados pessoais e sensíveis, conforme LGPD e demais normativos aplicáveis;
- Reduzir o risco de ataques baseados em credenciais, hoje responsáveis por parcela significativa das invasões a órgãos públicos, por meio de combinação de MFA, políticas avançadas de senha, detecção de logins anômalos, bloqueios automáticos e integração com mecanismos de resposta a incidentes e defesa contra ransomware e ameaças avançadas.

2.22.7.4. As plataformas de IAM/IDMaaS – Gestão Centralizada de Identidade e MFA são solução tecnológicas de IAM /IDMaaS que deverão prover um conjunto coerente e integrado de capacidades, que contemple, no mínimo, os seguintes eixos:

2.22.7.4.1 Governança de Identidade

a) Como requisito mínimo, a solução deve contemplar oferecer um diretório central unificado de identidades, com mecanismos de sincronização confiáveis entre Active Directory, serviços de diretório em nuvem (IDaaS), bancos de dados corporativos e aplicações específicas. Deverá permitir a consolidação de atributos de identidade (nome, matrícula, CPF, vínculo, cargo, unidade, perfil de acesso, tipo de contrato, data de início e término, entre outros), evitando duplicidades e inconsistências. Também deverá suportar o cadastro automatizado de perfis temporários, com definição de datas de início e expiração, reduzindo a necessidade de intervenção manual e minimizando acessos indevidos decorrentes de vínculos encerrados.

2.22.7.4.2 Ciclo de Vida (Lifecycle Management)

a) Como requisito mínimo, a solução deve contemplar implementar fluxos completos de provisionamento e desprovisionamento de acessos, desde o ingresso do usuário (onboarding), passando por mudanças de função ou lotação (movimentações internas), até o desligamento (offboarding). Em cada etapa, os acessos deverão ser ajustados automaticamente, de acordo com perfis predefinidos, assegurando que o usuário só tenha acesso aos sistemas e dados necessários ao seu papel institucional. Deverá ser possível configurar recertificações periódicas de privilégios, preferencialmente em ciclos trimestrais, com envio de tarefas aos gestores para validação ou revogação de acessos, registrando-se todas as decisões para fins de auditoria.

2.22.7.4.3 Autenticação e Autorização

a) Como requisito mínimo, a solução deve contemplar suportar MFA (Multi-Factor Authentication) com múltiplos métodos – tais como TOTP (código temporário), notificações push em aplicativo, tokens físicos ou lógicos, biometria, entre outros – permitindo políticas diferenciadas por tipo de usuário, criticidade do sistema ou nível de sensibilidade dos dados acessados. Deverá prover Single Sign-On (SSO) com suporte a protocolos padrão de mercado (SAML 2.0, OAuth 2.0, OpenID Connect), viabilizando integração com aplicações locais e serviços em nuvem. As políticas de autorização deverão considerar condições contextuais (localização, horário, dispositivo, nível de risco, reputação do IP, entre outros), permitindo a implementação de acesso condicional e alinhamento a modelos de segurança do tipo Zero Trust.

2.22.7.4.4 Integração Completa com o Ecossistema de Segurança

a) Como requisito mínimo, a solução deve contemplar integrar-se de forma nativa e bidirecional com SIEM/ESM/SOC, soluções de PAM (gestão de acessos privilegiados), SD-WAN, plataformas SaaS utilizadas pelo MinC, bem como com as soluções de Backup, Edge Computing, Big Data e demais componentes descritos nos Termos de Referência

vigentes. Logs de autenticação, autorização, elevação de privilégio, falhas de login e bloqueios deverão ser encaminhados ao SIEM/ESM, permitindo correlação com eventos de rede, endpoint, aplicação e dados. Adicionalmente, como requisito mínimo, a solução deve contemplar receber sinais de risco dessas camadas para aplicar ações automáticas, como bloqueio de contas, exigência de MFA reforçada ou sessões de revisão de acessos.

2.22.7.4.5 Monitoramento e Auditoria Contínuos

a) Como requisito mínimo, a solução deve contemplar manter trilha completa, íntegra e inviolável de eventos de identidade e acesso, permitindo que cada tentativa de login, cada autenticação bem-sucedida ou falha, cada alteração de privilégio e cada acesso a sistema crítico seja devidamente registrado com carimbo de data/hora, origem, contexto e resultado. Deverá prover indicadores de risco e relatórios gerenciais e técnicos, adequados para atendimento a auditorias internas, externas, órgãos de controle, demandas de transparência e exigências da LGPD, com visões específicas para segurança da informação, governança de TI, corregedoria e alta administração.

2.22.8 As soluções de **PAM (GESTÃO DE ACESSOS PRIVILEGIADOS) – CONTROLE DE CONTAS CRÍTICAS E SESSÕES DE ADMINISTRAÇÃO** são imprescindíveis ao Ministério da Cultura, pois é necessário adotar uma solução de Privileged Access Management (PAM), voltada ao controle centralizado, seguro e auditável de contas críticas e sessões de administração, abrangendo:

- contas de domínio (Domain Admin / Enterprise Admin);
- contas de administração de servidores, bancos de dados, aplicações e dispositivos de rede;
- contas de serviço com privilégios elevados;
- contas técnicas utilizadas em automações, integrações e rotinas de manutenção;
- perfis administrativos em ambientes em nuvem, SD-WAN e edge computing.
- A solução PAM deverá atuar como camada de proteção específica para acessos privilegiados, reduzindo a superfície de ataque e impedindo que credenciais críticas sejam utilizadas de forma indevida, manual ou automatizada, por usuários internos ou agentes maliciosos.
- No mínimo, a solução deverá:
    - cofretar (vault) credenciais privilegiadas, impedindo armazenamento local em planilhas, arquivos, anotações físicas ou navegadores;
    - realizar check-out e check-in controlado de senhas, com liberação temporária, tempo máximo de uso, expiração automática e eventual necessidade de aprovação;
    - gravar integralmente as sessões privilegiadas, possibilitando replay para auditoria técnica e apuração de responsabilidade (“o que foi feito, por quem, quando e onde”);
    - aplicar políticas de just-in-time access, concedendo privilégios apenas pelo tempo estritamente necessário para a execução da atividade;
    - manter trilhas de auditoria completas, registrando todas as ações relacionadas a contas privilegiadas (solicitação de acesso, aprovação, início de sessão, comandos executados, encerramento, alteração de credenciais);
    - integrar-se de forma nativa com IAM/IDMaaS, SIEM, ESM, SOC 24×7, Resposta a Incidentes, Forense Digital, SD-WAN, Defesa contra Ransomware/APT e gestão de vulnerabilidades, viabilizando ações coordenadas de bloqueio, isolamento e investigação.

2.22.8.1 Sem uma solução PAM, o MinC permanece exposto a riscos como:

- uso indevido de credenciais administrativas por múltiplos técnicos;
- ausência de clareza sobre “quem executou” determinada ação crítica;
- senhas privilegiadas reutilizadas em diversos sistemas;
- impossibilidade de reconstruir ações administrativas em caso de incidente;
- elevação de impacto de ataques de ransomware e APT que consigam capturar credenciais privilegiadas

2.22.8.2 Fragilidades na gestão e uso de contas privilegiadas

2.22.8.3 A inexistência de uma solução estruturada de PAM expõe o Ministério da Cultura a fragilidades graves na gestão e no uso de contas privilegiadas, dentre as quais destacam-se:

2.22.8.3.1 Compartilhamento informal de credenciais administrativas

a) Contas de administração de domínio, servidores, bancos de dados, aplicações e dispositivos de rede tendem a ser compartilhadas entre analistas e prestadores, sem registro individualizado, o que torna impossível identificar com precisão quem executou cada ação.

2.22.8.3.2 Armazenamento inseguro de senhas críticas

a) Sem cofre central, senhas privilegiadas tendem a ser mantidas em planilhas locais, arquivos de texto, sistemas não seguros ou até anotações físicas, constituindo vetor de risco significativo para uso indevido, vazamento e exploração por agentes maliciosos.

2.22.8.3.3 Ausência de gravação e monitoramento de sessões privilegiadas

a) Atualmente, ações de administração em sistemas críticos muitas vezes não são gravadas nem monitoradas em tempo real, o que compromete a capacidade de auditoria, dificulta a perícia digital e limita a responsabilização em casos de incidente ou mau uso.

2.22.8.3.4 Rotação insuficiente de senhas privilegiadas

a) Senhas privilegiadas tendem a permanecer ativas por longos períodos, às vezes por anos, inclusive após mudanças na equipe técnica, entrada de novos prestadores ou desligamento de colaboradores, aumentando a probabilidade de uso indevido ou continuidade de acesso por pessoas não autorizadas.

2.22.8.3.5 Dificuldade de aplicar princípios de menor privilégio e just-in-time

a) Sem um mecanismo de concessão temporária e controlada de privilégios, é comum que usuários permaneçam com acesso administrativo permanente a sistemas que não exigem tal nível de privilégio na rotina, ampliando o impacto potencial de credenciais comprometidas.

2.22.8.3.6 Alto impacto de ataques de ransomware e APT com credenciais elevadas

a) Em cenários de ransomware e ameaças avançadas (APT), a captura de credenciais privilegiadas permite ao atacante ampliar rapidamente o alcance do ataque, desabilitar controles, apagar logs, criptografar múltiplos servidores e comprometer backups, gerando risco elevado à continuidade dos serviços digitais culturais e à integridade de dados pessoais e do acervo cultural.

b) Os serviços de ESM/ITSM – Enterprise Service Management e Information Technology Service Management se baseiam na necessidade de que a contratação solicitada é crucial para o cumprimento das obrigações associadas às atividades diárias e rotineiras da Área de TI, tendo em vista o suporte e atendimento aos usuários dos recursos do Ministério da Cultura.

c) O atendimento ao Cliente Interno fornece suporte técnico de TI aos colaboradores internos do MinC e seus órgãos vinculados. Este suporte técnico envolve a identificação e solução de solicitações, esclarecimentos de questões e auxílio na utilização de soluções e recursos de TI. Tais ações impactam diretamente no desempenho das Unidades Organizacionais, especialmente devido ao conhecimento especializado dessa Central em assuntos de TI e na compreensão dos sistemas e processos de negócios.

d) Com o objetivo de inovar e modernizar os serviço, o MinC incentivará a implementação de novas tecnologias em suas atividades, como: inteligência artificial (I.A.), aprendizado de máquina, principalmente relacionados aos conceitos de automação de processos em ambientes de TIC – AIOps –, assistentes de voz, análise preditiva, mapeamento e monitoramento da jornada do usuário, entre outras, visando proporcionar maior agilidade e proatividade no atendimento aos usuários, aumentando a eficiência na entrega dos serviços descritos neste Edital.

e) De acordo com a literatura técnica especializada e com referenciais amplamente adotados na gestão moderna de serviços de Tecnologia da Informação, o AIOps (Artificial Intelligence for IT Operations) consiste na aplicação de técnicas de inteligência artificial, aprendizado de máquina e análise avançada de dados para automatizar, otimizar e apoiar as operações de TI. Essa abordagem permite às equipes técnicas monitorar ambientes complexos, identificar padrões e anomalias, diagnosticar causas raiz, antecipar incidentes, automatizar respostas e aprimorar a tomada de decisões operacionais e estratégicas, aumentando a eficiência, a confiabilidade e a produtividade dos serviços de TIC.

f) Importante destacar que o AIOps auxilia significativamente na resolução de problemas de forma automática ou através de execuções de processos automatizados, reduzindo a carga de trabalho na operação de TIC como um todo.

g) Portanto, no contexto em que a modernização e a eficiência são essenciais, a implementação de novas tecnologias na operação dos serviços, aliadas às dimensões propostas no ITIL v4, bem como a aplicação de IA voltada ao AIOps se tornam uma estratégia fundamental.

h) Os benefícios vão além da redução de custos, incluindo um serviço mais ágil, transparente e que responde melhor às necessidades dos usuários de TI. Essa abordagem inovadora não apenas busca modernizar os serviços, mas também fortalecer a eficácia do atendimento de TI do MinC e promover uma gestão que esteja em sintonia com o Planejamento Estratégico da TI.

i) Os serviços e necessidades descritas neste documento têm uma natureza contínua, pois são essenciais e buscam atender de maneira duradoura e constante às necessidades públicas, por mais de um ano fiscal. Isso garante o acesso remoto às informações e, por consequência, o funcionamento das atividades principais do Ministério, de modo que qualquer interrupção poderia comprometer a missão institucional do órgão.

2.22.8.4 Dessa forma, é fundamental garantir a manutenção de uma solução de segurança que esteja constantemente atualizada e assegurada, com o objetivo de evitar falhas, aumentando assim o nível de segurança necessário para o ambiente de Tecnologia da Informação e Comunicação e para o pleno desempenho da instituição, especialmente na proteção das informações que circulam em seus sistemas principais.

2.22.9 IAAS (Infrastructure as a Service)

2.22.9.1 O objetivo fundamental da contratação deste serviço é modernizar a infraestrutura do MinC e prover capacidade elástica para os sistemas institucionais.

2.22.9.2 Principais serviços a serem contratados:

- Hiperconvergência: ambiente virtualizado integrado (compute + storage + rede), com orquestração e balanceamento automático;
- Cluster de Alta Disponibilidade e Failover: possibilidade de criação de redundância entre o datacenter do Ministério e o(s) datacenters de empresa pública federal provedora de conectividade e infraestrutura de TIC, visando construir um ambiente computacional que sobreviva em caso de desastres;
- Virtualização e Middleware Integrados: suporte a containers e microserviços (Kubernetes, Hipervisors);
- Monitoramento de Infraestrutura e Segurança Integrada.
- Disponibilização de alta capacidade de armazenamento na forma de Storages.
- Como evolução dos serviços está prevista a migração gradual para infraestrutura definida por software (SDDC) durante a vigência contratual.

2.22.9.3 Atual Arquitetura

2.22.9.3.1 Após a análise das condições do datacenter do Ministério da Cultura, restou verificado que a Pasta possui uma sala-cofre composta por: uma célula certificada com isolamento térmico acústico, à prova de fogo, sistemas de alerta e combate a incêndio, sistema de climatização de precisão, sistema de alta disponibilidade com redundância de energia elétrica, controle de umidade e monitoramento 24hx7d. O Datacenter possui ainda contrato de manutenção preventiva e corretiva. Desta forma verifica-se que o Ministério possui ambiente devidamente adequado para a utilização de soluções on-premise.

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

2.22.9.3.3 Após a recriação do Ministério da Cultura, devido a implementação de escritórios Estaduais e a fim de garantir a conectividade adequada do Edifício sede localizado no Bloco B Esplanada dos Ministérios com as demais localidades dos diversos setores da Pasta, foi necessário elaborar uma topologia que garanta a otimização da infraestrutura de tecnologia da informação das localidades além da otimização dos recursos disponíveis no Datacenter.

2.22.9.3.4 O Ministério da Cultura usa atualmente um conjunto de quatro computadores servidores em seu datacenter, operando como um único cluster lógico, e com as seguintes características:

- 4 Servidores, cada um com 4 processadores de 12 núcleos totalizando 48 núcleos físicos por servidor e 96 núcleos físicos no total, com os núcleos operando em velocidade de 1,1Ghz.
- Cada servidor possui ainda 1.534GB de memória RAM.
- Essa arquitetura hospeda hoje 301 máquinas virtuais (VMs), totalizando 1.619 núcleos de processamento “virtuais”, com uma relação entre núcleos “virtuais” (vCores) e núcleos “físicos” (pCores) de 8,4:1.
- Os servidores estão além da sua vida útil programada e sem suporte do fabricante pelo tempo em que foram descontinuados.

2.22.9.3.5 Mesmo se desconsiderarmos o fato de termos servidores sem qualquer suporte e/ou reposição de peças, o atual conjunto se mostra extremamente limitado, tanto com relação à demanda atual quanto, e principalmente, considerando a possibilidade de inclusão de novas aplicações.

2.22.9.3.7 A baixa frequência de operação dos atuais processadores, aliada ao menor desempenho dos processadores de algumas gerações passadas (o que se mede em quantidade de instruções executadas por ciclo de clock, em inglês IPC), implica em que o rendimento de cada núcleo é, para os padrões atuais, bastante limitado. Quando se alia isso a uma relação entre vCores e pCores de 8,4:1, um número que já não é recomendado sequer para aplicações não-críticas, o resultado é que o desempenho de TODAS as aplicações fica severamente limitado.

2.22.9.3.8 Junte-se às deficiências de desempenho dos servidores atuais a baixa escalabilidade da solução de Cluster atual e o resultado é um sistema defasado e engessado, e se apenas trocarmos os servidores e mantivermos o mesmo esquema de agregação, teremos o mesmo problema se repetindo daqui a alguns anos, pelo que se projeta uma solução de cluster Hiperconvergente.

2.22.9.3.9 Numa solução de Hiperconvergência, o cluster pode crescer apenas adicionando mais servidores a ele, sem restrições de marca ou configuração, e a expansão é feita de forma automática e sem interrupção nos serviços. Na prática é uma solução de nuvem privada, com escalabilidade virtualmente ilimitada, e que apresenta um custo total de propriedade absurdamente menor no médio e longo prazo.

2.22.9.3.10 Para esta demanda, projeta-se uma solução composta por 4 (quatro) servidores, cada um com dois processadores com 64 núcleos físicos, 1.536GB de memória RAM por processador e armazenamento interno “All Flash” com capacidade mínima bruta de 23TB por servidor.

2.22.9.3.11 Características da Solução de Armazenamento de Dados Atual

- Para a sustentação dos sistemas e serviços do Ministério da Cultura, foi adquirida em 2023, e implementada em 2024, uma solução de armazenamento de dados e virtualização por meio do processo SEI no. 01400.000658/2023-76. Esta solução de armazenamento é composta de 2 (dois) subsistemas de armazenamento Netapp modelo AFF C400 com 266TiB cada de armazenamento destinado ao protocolo de compartilhamento de arquivos (NAS) e réplica de proteção e a prover área virtualizada para o virtualizador Hitachi Vantara modelo VSP E 1090, também adquirido por meio da mesma contratação que dispõe ainda de área interna de armazenamento de 400TiB.
-

2.22.10 PAAS (Platform as a Service)

2.22.9.10.1 O objetivo fundamental da contratação deste serviço é implantar uma camada unificada de governança, dados e inteligência analítica sobre os sistemas culturais do MinC.

2.22.9.10.2 Principais serviços a serem contratados:

- Auditoria e Governança de Dados: trilhas de auditoria, classificação e conformidade com LGPD;
- Big Data e Data Lake do MinC: armazenamento e tratamento massivo de dados culturais (SALIC, SNC, Mapas da Cultura, SNIIC, CTAv);
- Inteligência Artificial e Analytics: algoritmos de recomendação, IA generativa e análise preditiva para políticas culturais;
- Serviços em Nuvem (USN): escalabilidade de recursos para ambientes de homologação, produção e contingência;
- APIs e Integrações com sistemas públicos (Gov.br, ConectaGov, SEI, Compras.gov).
- Existe a previsão de evolução no sentido de adoção de IA generativa de código aberto e integração com plataformas GovTech (como SERPRO Analytics e GovData) para apoiar a tomada de decisão baseada em evidências culturais.
- Com relação aos serviços de AUDITORIA E GOVERNANÇA DE DADOS, a implantação de serviço especializado de auditoria e governança de dados, capaz de monitorar, registrar, correlacionar e garantir a rastreabilidade de eventos relacionados ao uso, alteração, compartilhamento e acesso a 10 de 48 informações críticas geridas pelo Ministério da Cultura. Tal serviço reforça a conformidade com a LGPD, com as normas internas de segurança da informação e com a necessidade de visibilidade contínua sobre o ciclo de vida dos dados institucionais. Diante da dispersão dos dados culturais e da diversidade de fontes internas e externas, evidencia-se a necessidade de mecanismos permanentes de auditoria e governança de dados, para assegurar integridade, origem, rastreabilidade e uso adequado das informações que sustentam políticas culturais, análises estratégicas e prestação de contas. A ausência de mecanismos contínuos de auditoria e governança de dados aumenta o risco de manipulação indevida, acessos não autorizados, exclusões acidentais e fragilidades de integridade, comprometendo a confiabilidade institucional e a conformidade com a LGPD. A presente contratação deve mitigar esse risco mediante solução integrada de monitoramento, logging avançado, trilhas de auditoria e governança dos dados estratégicos do MinC.
- Com relação aos serviços, o DATA LAKE (BIG DATA), a pretensa aquisição visa atender o Plano Diretor de Tecnologia da Informação e Comunicação do Ministério da Cultura (PDTIC 2024-2027), que, em seu Eixo 2 (Governança de Dados), identificou a Necessidade (N3) de disponibilidade de soluções de análise e tratamento de dados (Bussiness Inteligence - BI), a qual deve ser atendida pela Ação (A3.1) de prover soluções de governança de dados (Business Inteligence, Datawarehouse, data quality, data lake etc.). Ademais, objetiva consolidar a evolução do Sistema Nacional de Informações e Indicadores Culturais (SNIIC).
- A trajetória do SNC e, posteriormente, do SNIIC, evidencia avanços significativos, mas também desafios complexos. Em 2010, com a criação do Plano Nacional de Cultura (PNC), foi introduzido um dos mais importantes instrumentos orientadores do poder público para a formulação de políticas culturais, que por sua vez buscava sintetizar o debate público e direcionar os esforços coletivos na área cultural. Contudo, mesmo com a evolução dos sistemas e a ampliação das fontes de informação, o cenário atual revela a existência de uma dispersão entre os dados gerados pelos diversos sistemas, como o Mapas Culturais, SALIC, o SNC, o CNPC e o Portal de Dados da Cultura, dentre outros. Essa fragmentação dificulta a realização de análises diagnósticas sofisticadas e impede a criação de indicadores consistentes, imprescindíveis para a formulação de políticas culturais mais eficazes e fundamentadas em dados.
- É nesse contexto que este escopo se insere, visando não apenas a consolidação dos dados e informações, mas sobretudo a criação de um processo de cocriação e aprendizado. Busca-se, portanto, estabelecer parceria

entre a expertise do próprio Ministério da Cultura e a entidade contratada. Tal parceria se mostra essencial, pois une a capacidade de análise técnica e a visão estratégica necessária para transformar o vasto repositório de dados em conhecimento aplicável à definição e implementação de políticas públicas culturais.

- A proposta enfatiza que não se trata de rediscutir a arquitetura tecnológica já estabelecida no MinC, mas de adotar uma perspectiva focada nos sistemas de informação que apoiam a área cultural. Assim, o objetivo é identificar e integrar as diversas fontes de informação, proporcionando uma visão holística que possibilite a gestão eficaz da informação. Essa integração permitirá que os indicadores e as políticas culturais se tornem cada vez mais baseados em dados reais e atualizados, contribuindo para decisões mais acertadas e para o desenvolvimento de estratégias que atendam às demandas do setor cultural de maneira dinâmica e evolutiva.
- O desenvolvimento desse trabalho precisa considerar alguns princípios reconhecidos internacionalmente, como os princípios FAIR – que orientam a criação de uma Arquitetura de Dados capaz de assegurar que os dados sejam “Encontráveis”, Acessíveis, Interoperáveis e Reutilizáveis. Essa abordagem garante a integridade e a qualidade dos dados, assim como cria condições para que as informações possam ser utilizadas de maneira inteligente e estratégica, conectando os dados às metas e objetivos do MinC e de todo o ecossistema cultural. Dessa forma, o acesso aos dados via APIs, a visualização navegável e o controle eficiente dos metadados tornam-se ferramentas essenciais para a transformação dos processos decisórios e para a construção de uma política cultural verdadeiramente integrada.
- Ademais, destaca-se a relevância de uma abordagem multidisciplinar para enfrentar os desafios decorrentes da fragmentação dos sistemas de informação. Ao integrar conhecimentos de arquitetura, engenharia e ciência de dados, tecnologia da informação e políticas culturais, a equipe contratada, em parceria com o MinC, deve identificar lacunas, propor soluções inovadoras e promover o engajamento de diferentes atores do ecossistema cultural. Essa sinergia é vital para transformar o SNIIC em um instrumento dinâmico e adaptável, que evolui continuamente em sintonia com as demandas e transformações do setor cultural.
- Outro aspecto crucial que justifica a contratação do objeto é o potencial de otimização dos processos internos do MinC. Atualmente, a gestão das informações culturais enfrenta desafios significativos, decorrentes da ausência de uma visão integrada dos dados e dos sistemas. Essa situação tem impacto direto na formulação de políticas públicas, na mensuração dos resultados e na definição de estratégias de intervenção. Ao oferecer uma abordagem que une a análise de dados à definição de metas e políticas, busca-se eliminar essas barreiras, facilitando a criação de indicadores precisos e o monitoramento contínuo dos resultados.
- Do ponto de vista estratégico, a contratação desta proposta permite ao MinC dar um salto qualitativo no processo de governança dos dados culturais. Ao conectar dados e estratégias, a iniciativa possibilita uma integração sem precedentes entre a análise de informações e a tomada de decisões, fortalecendo o papel do MinC como agente transformador da política cultural nacional. Essa conexão aprimora o controle, a gestão dos recursos públicos e amplia a capacidade do Ministério de responder de maneira ágil e precisa às mudanças e desafios impostos por um ambiente cultural em constante transformação.
- Em síntese, este escopo se justifica pela necessidade de promover uma integração sistêmica e estratégica dos dados e das informações culturais, possibilitando ao MinC uma visão única e clara do conjunto de informações que sustentam as políticas públicas culturais. Ao conectar os dados à estratégia do Ministério e de todo o ecossistema cultural, a proposta contribui para a criação de indicadores sólidos, para a formulação de políticas baseadas em evidências e para a otimização dos processos internos. Essa transformação, ancorada em disciplinas como arquitetura e ciência de dados, e sustentada pela expertise da contratada e do próprio MinC, representa um avanço decisivo rumo a uma gestão cultural mais eficiente, integrada e capaz de atender às demandas de um país que valoriza e investe na cultura.
- Portanto, a presente justificativa reforça que o objeto contratado é essencial para promover uma transformação sistêmica e estratégica dos processos de gestão e formulação de políticas culturais. A abordagem esperada deve trabalhar de forma paralela entre os dados e os objetivos estratégicos, aliada a um processo de cocriação e à expertise técnica de uma equipe multidisciplinar, para garantir a construção de um SNIIC evolutivo e adaptativo, capaz de integrar e potencializar os sistemas de informação existentes, e de fomentar a criação de políticas culturais mais eficazes e baseadas em dados.
- Tal iniciativa não apenas alinha a gestão cultural às demandas contemporâneas, mas também fortalece a capacidade do Ministério da Cultura de atuar de maneira inovadora e integrada, promovendo o desenvolvimento sustentável e a democratização do acesso à cultura em todo o território nacional.

2.22.11 IMAGEAMENTO

2.22.11.1 O objetivo principal destes serviços é garantir o acesso a imagens de satélite, radar SAR, modelagem digital e inteligência geoespacial, permitindo: Diagnóstico territorial cultural, Identificação de infraestrutura e equipamentos

culturais; Monitoramento de bens tombados e patrimônios culturais; Estudos de impacto cultural e ambiental; Apoio ao mapeamento nacional do SNC e Mapas da Cultura; Tomada de decisão baseada em dados espaciais; Transparência sobre o investimento público em cultura.

2.22.11.2 Principais serviços a serem contratados:

- Mapeamento geoespacial de pontos culturais;
- Identificação de vazios culturais em regiões remotas
- Mapas geográficos de atividades culturais;
- Dashboards públicos integrando imagem + investimentos públicos;
- Auditoria remota de equipamentos e projetos financiados;
- Priorização de investimento federal baseado em território;
- Detecção de danos e alterações indevidas;
- Apoio a políticas para povos indígenas e comunidades quilombolas;
- Acompanhamento visível de obras e gastos culturais;
- Auditoria remota de equipamentos e projetos financiados;
- Planejamento 3D de grandes eventos culturais;
- Análises de terreno para instalações temporárias;
- Apoio ao CTAv em produções e gravações aéreas.

2.22.12 Inseridos nas necessidades do projeto em tela, destacamos os SERVIÇOS COMPLEMENTARES, que são transversais a todas as camadas, como:

1. Gestão de Projetos e Transição (PMO TIC);
2. Treinamento e capacitação técnica para equipes MinC/empresa pública federal provedora de conectividade e infraestrutura de TIC;
3. Atualização tecnológica contínua (hardware e software);
4. Consultoria em interoperabilidade e padronização de dados;
5. Relatórios trimestrais de SLA e roadmap de evolução tecnológica.

3. Área requisitante

Área Requisitante	Responsável
COINF	Fernando Kleber de Araújo Souza

4. Necessidades de Negócio

4.1. Como demonstrado nas justificativas apresentadas, as políticas públicas culturais operam em janelas de oportunidade que exigem elevada capacidade de resposta institucional, nas quais convergem interesses políticos, sociais, orçamentários e técnicos.

4.2. Para que essas janelas se concretizem em ações efetivas, é essencial que o Ministério da Cultura disponha de capacidade técnica e operacional compatível com a complexidade e a escala das políticas públicas a serem implementadas. Nesse cenário, as unidades finalísticas do Ministério da Cultura, em articulação com a STII, cumprem papel estratégico como viabilizadoras das políticas públicas culturais.

4.3. Contudo, limitações orçamentárias e contratuais atualmente impostas à STII restringem sua capacidade de resposta tempestiva e escalável às demandas institucionais, especialmente em momentos críticos do ciclo das políticas culturais. Atualmente, é praticamente impossível conceber políticas públicas eficazes que prescindam do uso intensivo de tecnologia da informação, seja na implementação de programas de fomento e difusão, seja no monitoramento e avaliação das ações culturais.

4.4. Seguindo as diretrizes estabelecidas pelo Ministério da Gestão e da Inovação em Serviços Públicos, o Ministério da Cultura passou a reconhecer os contratos com empresas públicas federais como instrumentos estratégicos para a ampliação da capacidade técnica, redução de riscos operacionais e fortalecimento da inovação digital.

4.5. Essa atuação conjunta visa fortalecer o papel da tecnologia como elemento estruturante da promoção da cultura, ampliando o alcance, a efetividade e a sustentabilidade das políticas públicas no setor. Para mitigar riscos operacionais, legais, reputacionais e de continuidade dos serviços digitais, o Ministério da Cultura necessita implementar capacidades institucionais estruturadas de segurança da informação, conforme descrito a seguir.

4.6. A contratação proposta visa atender a necessidades de negócio estruturantes do Ministério da Cultura, diretamente relacionadas à execução de políticas públicas, à segurança institucional, à conformidade legal e à continuidade dos serviços digitais:

4.6.1 Modernização Tecnológica - Ampliar a capacidade da STII em realizar, de forma simultânea, atividades de sustentação dos sistemas legados e a modernização das soluções tecnológicas já existentes, além de viabilizar o desenvolvimento e a entrega de novas soluções digitais e de infraestrutura voltadas ao setor cultural.

4.6.2 Tempestividade no Atendimento às Demandas - Prover soluções que agilizem e tornem mais eficazes os processos de resposta às demandas das unidades finalísticas do MinC, sejam elas voltadas à execução de políticas públicas, ao atendimento ao público (usuários) ou à prestação de serviços internos e externos.

4.6.3 Reforço na Segurança da Informação - Implementar, de forma tempestiva, soluções de cibersegurança em todo o ambiente tecnológico sob gestão do Ministério da Cultura, reduzindo riscos, corrigindo vulnerabilidades e assegurando a proteção dos dados de agentes culturais, instituições e cidadãos. No âmbito dessa necessidade de negócio, identificam-se como capacidades essenciais os seguintes elementos:

- A presente contratação deverá contemplar, de forma explícita, serviço de análise e gestão contínua de vulnerabilidades, de modo a permitir que o MinC identifique, priorize e trate de forma sistemática as fragilidades de segurança existentes em seus ambientes tecnológicos, com monitoramento permanente, geração de alertas, painéis gerenciais e apoio às equipes técnicas na tomada de decisão quanto às ações corretivas, preventivas e de melhoria.
- A adoção de serviço de auditoria e governança de dados é indispensável para assegurar rastreabilidade e integridade das informações que suportam políticas públicas culturais, garantindo que acessos, alterações e fluxos de dados sejam monitorados e que decisões estratégicas se baseiem em informação confiável.
- Necessidade de adoção de plataforma de Enterprise Security Management (ESM): A consolidação da segurança cibernética no Ministério da Cultura exige a adoção de solução de Enterprise Security Management (ESM) capaz de unificar e correlacionar, em um repositório único e confiável, todos os eventos, logs, políticas e notificações provenientes dos mais diversos sistemas que compõem o ecossistema tecnológico institucional.

4.6.4 A plataforma servirá como núcleo central de governança de segurança, garantindo:

- padronização de políticas, regras de correlação, triagem e classificação de incidentes;
- gestão efetiva de riscos tecnológicos, com visão integrada de vulnerabilidades, acessos, auditorias e comportamentos suspeitos;
- base única de evidências para fins de auditoria interna, externa, CGU, TCU e órgãos de controle;
- suporte analítico para decisões estratégicas que envolvam continuidade digital, evolução da infraestrutura, transformação digital e gestão de riscos;
- redução significativa de exposição a ataques, interrupções de serviço e danos reputacionais.
- Implantação de capacidade institucional de Resposta a Incidentes e Forense Digital: é essencial ao MinC dispor de capacidade robusta, padronizada e automatizada de Resposta a Incidentes (IR) e Forense Digital, de modo a:
    - reduzir impactos operacionais, reputacionais e regulatórios;
    - preservar evidências conforme cadeia de custódia;
    - garantir conformidade com LGPD, PPSI/MGI, E-Cyber e normativas internas;
    - fornecer base factual para análises de causa raiz e para processos administrativos e judiciais;
    - evitar retrabalho, perda de dados e ampliação desnecessária do escopo dos danos;
    - fornecer instrumentos de governança para decisões de alto nível.
    - Fortalecimento da capacidade institucional contra ransomware e ataques avançados: o Ministério da Cultura necessita implementar solução específica que garanta proteção contínua, automatizada e

inteligente contra ransomware e ameaças avançadas, alinhada às políticas de governo digital, segurança cibernética e proteção de dados pessoais, de modo a assegurar a prestação ininterrupta dos serviços culturais. Essa solução deverá ser capaz de:

1. impedir criptografia não autorizada de dados em repouso e em uso, nos diversos ambientes (on-premisses, nuvem e edge);
2. detectar comportamentos maliciosos antes da efetiva execução do ataque, com base em padrões anômalos de acesso, execução e comunicação;
3. bloquear ameaças em memória e processos voláteis, incluindo scripts, macros, ferramentas de administração remota abusadas e técnicas fileless;
4. interromper movimentação lateral, evitando a propagação do ataque entre estações, servidores, bases de dados e serviços compartilhados;
5. impedir comunicações externas indevidas, bloqueando canais de comando e controle, túneis criptografados e conexões suspeitas;
6. garantir rollback seguro de arquivos, sistemas e configurações afetados, diminuindo o tempo de restauração e o impacto operacional;
7. proteger dados pessoais e culturais de alto valor, garantindo integridade, confidencialidade e disponibilidade, em observância à LGPD e às normas internas de segurança da informação.

4.6.5 A implantação de tal capacidade integra-se às estratégias de reforço da segurança da informação, de aumento da maturidade em gestão de riscos cibernéticos e de consolidação de uma postura proativa de defesa, reduzindo a dependência de ações reativas e emergenciais.

4.6.6 Garantia de segurança de identidades e acessos: o Ministério da Cultura necessita implementar uma solução IAM/IDMaaS que assegure a segurança, rastreabilidade e governança de identidades e acessos ao longo de todo o ciclo de vida dos usuários, contas de serviço e aplicações, com vistas a:

- Reduzir o acesso indevido, por meio da exigência de autenticação multifator (MFA) para perfis de maior risco, da aplicação consistente de políticas de menor privilégio e da centralização da autorização em mecanismos de controle baseados em papéis (RBAC/ABAC), reduzindo a probabilidade de uso malicioso de credenciais;
- Padronizar e automatizar os processos de criação, alteração e exclusão de contas, com fluxos formais de aprovação vinculados a cargos, funções, lotações e projetos, de modo a garantir que a concessão de privilégios seja sempre motivada por necessidade de negócio, com registro explícito de quem solicitou, aprovou e executou cada ação;
- Eliminar perfis órfãos e privilégios acumulados, por meio de rotinas de recertificação periódica de acessos, detecção de contas inativas, revisão de grupos de segurança e expiração automática de acessos temporários, garantindo que somente usuários em efetivo exercício e com vínculo vigente mantenham acesso aos sistemas;
- Registrar e rastrear acessos de alto privilégio, permitindo que ações sensíveis (criação de usuários, alteração de perfis, acesso a dados pessoais, mudanças de configuração crítica) sejam monitoradas, associadas a identidades específicas e passíveis de auditoria posterior, inclusive para fins de responsabilização;
- Suportar auditorias internas, externas e de órgãos de controle, com relatórios estruturados que evidenciem o atendimento a requisitos de segregação de funções, trilhas de auditoria, governança de privilégios e controles de acesso a dados pessoais e sensíveis, conforme LGPD e demais normativos aplicáveis;
- Reduzir o risco de ataques baseados em credenciais, hoje responsáveis por parcela significativa das invasões a órgãos públicos, por meio de combinação de MFA, políticas avançadas de senha, detecção de logins anômalos, bloqueios automáticos e integração com mecanismos de resposta a incidentes e defesa contra ransomware e ameaças avançadas.
- Para garantir a continuidade segura dos serviços e a conformidade com os normativos vigentes, o Ministério da Cultura necessita de solução PAM que:
    - assegure que contas privilegiadas sejam usadas apenas quando estritamente necessário, por meio de concessão just-in-time, com prazo definido e, quando aplicável, aprovação prévia;
    - cofrete e rotacione senhas privilegiadas de modo automático e periódico, evitando reutilização prolongada de credenciais e reduzindo a superfície de ataque baseada em contas administrativas;
    - registre, monitore e grave todas as sessões privilegiadas, permitindo replay técnico para auditoria, investigação de incidentes e verificação de conformidade com políticas internas e requisitos legal-regulatórios;

- forneça visibilidade gerencial sobre o uso de privilégios, com relatórios consolidados por sistema, unidade organizacional, tipo de conta, prestador e período, apoiando a tomada de decisão da alta administração;
- apoie auditorias internas, externas e órgãos de controle, oferecendo evidências objetivas de que acessos privilegiados são concedidos, utilizados e revogados dentro de critérios formalmente definidos e auditáveis;
- reduza o impacto de incidentes de segurança, permitindo revogação rápida, bloqueio temporário, redefinição massiva de senhas privilegiadas e suspensão de sessões em andamento, em articulação com o SOC e o ESM.

4.6.7 Integração de Sistemas e Bases de Dados Adoção de arquiteturas tecnológicas que promovam interoperabilidade entre os sistemas do MinC e demais entes da administração pública, permitindo maior integração entre cadastros de agentes culturais, editais, políticas de fomento e ações territoriais, o que melhora o processo decisório, a experiência do usuário e a segurança das informações.

4.6.8 Monitoramento centralizado de eventos de segurança com SIEM integrado ao SOC da empresa pública federal provedora de conectividade e infraestrutura de TIC– O Ministério da Cultura necessita garantir monitoramento contínuo, centralizado e inteligente de eventos de segurança, por meio de solução de SIEM integrada ao SOC da empresa pública federal provedora de conectividade e infraestrutura de TIC, de forma a:

- consolidar logs de sistemas, redes, aplicações, serviços em nuvem, endpoints e soluções de segurança;
- aplicar correlação avançada e mecanismos de análise comportamental sobre os eventos coletados;
- gerar alertas em tempo real e dashboards de risco voltados tanto à área técnica quanto à alta gestão;
- alimentar o SOC da empresa pública federal provedora de conectividade e infraestrutura de TIC com visão unificada do ambiente, viabilizando resposta coordenada a incidentes e emissão de relatórios periódicos;
- assegurar trilhas de auditoria abrangentes para acesso a dados pessoais e informações sensíveis, em conformidade com a LGPD e com a Política de Segurança da Informação do MinC.

4.6.9 Aumento da Eficiência Operacional Automatizar processos internos e serviços, reduzindo a burocracia, otimizando recursos e melhorando a produtividade das equipes, o que possibilita ao MinC entregar mais com menos, com maior foco na execução de políticas culturais de impacto.

4.6.10 Aprimoramento da Transparência e da Prestação de Contas Disponibilizar dados estruturados e acessíveis sobre a execução das políticas públicas culturais, editais, repasses, ações territoriais e resultados alcançados, fortalecendo a transparência, o controle social e a accountability institucional, conforme preceitos da Lei de Acesso à Informação e diretrizes do Governo Digital.

4.6.11 Para assegurar transparência plena e accountability, é necessário implementar mecanismos estruturados de auditoria e governança de dados, capazes de consolidar logs, evidências e rastros de atividades administrativas e sistêmicas, garantindo confiabilidade dos registros e aderência às normas vigentes.

4.6.12 Adequação a Requisitos Legais e Regulatórios Assegurar que as soluções digitais possam ser rapidamente adaptadas a alterações legais, normativas ou regulatórias, além de atender com celeridade demandas de órgãos de controle, tribunais ou do Congresso Nacional.

4.6.13 Suporte à Tomada de Decisão com Base em Dados Viabilizar a estrutura tecnológica necessária para que as áreas do MinC possam coletar, consolidar, analisar e utilizar dados sobre as políticas culturais, subsidiando decisões estratégicas com evidências e promovendo maior efetividade e direcionamento das ações públicas.

4.6.14 Suporte a Programas e Projetos Estratégicos do Governo Federal Apoiar a execução de programas e projetos estratégicos voltados à cultura, incluindo ações de transformação digital, difusão audiovisual, valorização de territórios criativos e implementação de sistemas integrados nacionais, em articulação com outras esferas do governo.

5. Necessidades Tecnológicas

5.1 Atualização do portfólio de soluções do Ministério da Cultura: os ativos de software do MinC estão em sua maioria defasados tecnologicamente, não sendo passíveis de:

a. Utilização em nuvem;

b. Aprimoramento de segurança para conter vulnerabilidades;

c. Integração com outras soluções;

d. Utilização de padrões de governo como design system e e-Mag.

5.2 Atualização dos ativos de TI do MinC: muitos dos ativos de TIC do MinC estão defasados, sem garantia e sem suporte pelos fabricantes, aumentando o risco de indisponibilidade dos serviços;

5.3 Saneamento das vulnerabilidades de TIC do MinC: além de ativos defasados, o MinC precisa ampliar o uso de soluções que aumentem a proteção de perímetro e monitorem ativamente os diversos ambientes, alcançando comportamento e práticas dos usuários;

5.4 Automação de processos de gestão de TIC do MinC: a STII conta com número insuficiente de servidores para monitorar todas as atividades de gestão dos serviços de TIC, sendo necessário automatizar esses serviços gerando informações para acompanhamento pela gestão;

5.5 Disponibilização de ambientes de infraestrutura adequados para as soluções de missão crítica: as soluções disponibilizadas pelo MinC têm ampliado sua utilização pela sociedade, tornando-se soluções de missão crítica, o que demanda sua operação a partir de datacenters com certificações adequadas para esse tipo de operação.

5.6 Auditoria e Governança de Dados: a crescente centralidade dos dados nas políticas públicas culturais exige mecanismos contínuos de auditoria, classificação, governança e rastreabilidade, assegurando integridade, confiabilidade e uso adequado das informações. Tais mecanismos devem operar de forma integrada às soluções de segurança já existentes e às tecnologias de armazenamento, processamento e análise de dados do MinC.

5.7 Enterprise Security Management (ESM): dada a crescente complexidade, heterogeneidade e criticidade do parque tecnológico do MinC — composto por sistemas legados, soluções modernas em nuvem, ferramentas de IA, repositórios de dados sensíveis, mecanismos de interoperabilidade e infraestrutura distribuída nacionalmente — faz-se necessária a adoção de uma solução de Enterprise Security Management (ESM) capaz de unificar, padronizar e automatizar toda a camada de gestão de segurança da informação.

5.7.1 A solução deverá:

- integrar, sem limitação, logs, eventos, trilhas de auditoria, controles de acesso, vulnerabilidades, incidentes, alarmes, acessos privilegiados, políticas e configurações;
- suportar técnicas avançadas de detecção, incluindo análise comportamental, machine learning e detecção de anomalias;
- fornecer visão operacional, tática e estratégica do risco, permitindo governança contínua;
- garantir aderência às normas internas e externas, com relatórios automáticos de conformidade;
- atuar como ponto central de decisão para ações de mitigação, resposta a incidentes e aplicação de políticas corporativas.

5.8. Resposta a Incidentes e Forense Digital: considerando a crescente sofisticação dos ataques cibernéticos, a sensibilidade dos dados culturais tratados e a criticidade dos sistemas finalísticos do MinC, torna-se necessária a adoção de solução especializada em Resposta a Incidentes e Forense Digital, capaz de:

- identificar rapidamente ações maliciosas e movimentos laterais na rede;
- aplicar técnicas forenses em tempo real ou pós-incidente;
- garantir extração segura de evidências, sem contaminação;
- analisar indicadores de comprometimento (IOCS) e táticas, técnicas e procedimentos (TTPs) do invasor;
- correlacionar eventos com ESM e IAM;
- reconstruir cadeia de eventos, linha do tempo e impacto;
- gerar relatórios com valor jurídico, aptos para subsidiar responsabilizações e auditorias.

5.9. Solução de SIEM (Monitoramento de Eventos e Logs) integrada ao SOC empresa pública federal provedora de conectividade e infraestrutura de TIC: dada a complexidade do ambiente tecnológico do MinC e a dispersão de logs entre diferentes plataformas, faz-se necessária uma solução de SIEM com as seguintes capacidades tecnológicas mínimas:

- Arquitetura distribuída e escalável, permitindo implantação centralizada ou em múltiplos servidores, com suporte a virtualização (VMware ESX, Hyper-V, KVM) e nuvens públicas (Azure, Amazon), bem como failover e disaster recovery;
- Capacidade mínima de processamento de 60 GB/dia de eventos, provenientes de até 600 fontes simultâneas, com possibilidade de expansão mediante adição de licenças e servidores;
- Coletores e agentes multitenant para obtenção de eventos em sites remotos, com suporte a sobreposição de IPs, armazenamento local temporário e envio seguro (HTTPS) em caso de falhas de conectividade;
- Suporte a amplo conjunto de protocolos e fontes de logs (syslog, NetFlow/SFlow/JFlow, SNMP trap, WMI, JDBC para múltiplos bancos de dados, APIs, firewalls, IDS/IPS, aplicações e serviços em nuvem);
- Motor de correlação e análise avançada, com suporte a queries “SQL like”, detecção de anomalias estatísticas, análise histórica e associação a técnicas do framework MITRE ATT&CK, com centenas de regras integradas;
- Integração nativa com SOC, permitindo que incidentes gerados sejam automaticamente encaminhados para tratamento pela equipe da empresa pública federal provedora de conectividade e infraestrutura de TIC, incluindo abertura de tickets, categorização, prioridade, histórico de ações e anexação de evidências.

5.10. Defesa contra Ransomware e Ameaças Avançadas (APT): considerando a sofisticação extrema dos ataques modernos e a relevância social, econômica e cultural das informações tratadas pelo Ministério da Cultura, faz-se necessária a adoção de solução tecnológica específica de Defesa contra Ransomware e Ameaças Avançadas, com arquitetura e recursos modernos, escaláveis e aderentes às melhores práticas de mercado e às normas governamentais.

5.10.1 A solução deverá possuir, no mínimo, as seguintes capacidades tecnológicas:

- monitoramento comportamental contínuo de endpoints, servidores, containers, máquinas virtuais e recursos em nuvem;
- detecção em memória (fileless), identificando código malicioso residente em processos legítimos ou em áreas de memória não mapeadas;
- resposta automatizada a incidentes, incluindo isolamento de dispositivos, bloqueio de processos e revogação de credenciais comprometidas;
- bloqueio de criptografia maliciosa, por meio de interceptação de chamadas de sistema e políticas de proteção de arquivos e volumes;
- desconexão automática de dispositivos comprometidos da rede, evitando propagação lateral e exfiltração de dados;
- proteção contra exfiltração, com inspeção de tráfego, listas de bloqueio de destinos suspeitos e limitação de canais de saída;
- análise retroativa (retrospective detection), permitindo reinterpretação de eventos passados à luz de novas assinaturas e indicadores de comprometimento;

- detecção em tempo real de IOCs (Indicators of Compromise) e IOAs (Indicators of Attack), com atualização contínua de feeds de inteligência;
- integração direta com as soluções de Enterprise Security Management (ESM), Resposta a Incidentes (IR) e Gestão de Vulnerabilidades, permitindo coordenação centralizada das ações de defesa.

5.10.2 A tecnologia adotada deverá ser compatível com o ambiente heterogêneo do MinC, suportando diferentes sistemas operacionais, plataformas de nuvem pública e privada, bem como futuras expansões de infraestrutura, sem reengenharia completa da solução.

5.11.IAM/IDMaaS – Gestão Centralizada de Identidade e MFA: a solução tecnológica de IAM/IDMaaS deverá prover um conjunto coerente e integrado de capacidades, que contemple, no mínimo, os seguintes eixos:

5.11.1 Governança de Identidade: a solução deverá oferecer um diretório central unificado de identidades, com mecanismos de sincronização confiáveis entre Active Directory, serviços de diretório em nuvem (IDaaS), bancos de dados corporativos e aplicações específicas. Deverá permitir a consolidação de atributos de identidade (nome, matrícula, CPF, vínculo, cargo, unidade, perfil de acesso, tipo de contrato, data de início e término, entre outros), evitando duplicidades e inconsistências. Também deverá suportar o cadastro automatizado de perfis temporários, com definição de datas de início e expiração, reduzindo a necessidade de intervenção manual e minimizando acessos indevidos decorrentes de vínculos encerrados.

5.11.2 Ciclo de Vida (Lifecycle Management): a solução deverá implementar fluxos completos de provisionamento e desprovisionamento de acessos, desde o ingresso do usuário (onboarding), passando por mudanças de função ou lotação (movimentações internas), até o desligamento (offboarding). Em cada etapa, os acessos deverão ser ajustados automaticamente, de acordo com perfis predefinidos, assegurando que o usuário só tenha acesso aos sistemas e dados necessários ao seu papel institucional. Deverá ser possível configurar recertificações periódicas de privilégios, preferencialmente em ciclos trimestrais, com envio de tarefas aos gestores para validação ou revogação de acessos, registrando-se todas as decisões para fins de auditoria.

5.11.3 Autenticação e Autorização: a solução deverá suportar MFA (Multi-Factor Authentication) com múltiplos métodos – tais como TOTP (código temporário), notificações push em aplicativo, tokens físicos ou lógicos, biometria, entre outros – permitindo políticas diferenciadas por tipo de usuário, criticidade do sistema ou nível de sensibilidade dos dados acessados. Deverá prover Single Sign-On (SSO) com suporte a protocolos padrão de mercado (SAML 2.0, OAuth 2.0, OpenID Connect), viabilizando integração com aplicações locais e serviços em nuvem. As políticas de autorização deverão considerar condições contextuais (localização, horário, dispositivo, nível de risco, reputação do IP, entre outros), permitindo a implementação de acesso condicional e alinhamento a modelos de segurança do tipo Zero Trust.

5.11.4 Integração Completa com o Ecossistema de Segurança: a solução deverá integrar-se de forma nativa e bidirecional com SIEM/ESM/SOC, soluções de PAM (gestão de acessos privilegiados), mecanismos de microsegmentação, SD-WAN, plataformas SaaS utilizadas pelo MinC, bem como com as soluções de Backup, Edge Computing, Big Data e demais componentes descritos nos Termos de Referência vigentes. Logs de autenticação, autorização, elevação de privilégio, falhas de login e bloqueios deverão ser encaminhados ao SIEM/ESM, permitindo correlação com eventos de rede, endpoint, aplicação e dados. Adicionalmente, a solução deverá receber sinais de risco dessas camadas para aplicar ações automáticas, como bloqueio de contas, exigência de MFA reforçada ou sessões de revisão de acessos.

5.11.5 Monitoramento e Auditoria Contínuos: a solução deverá manter trilha completa, íntegra e inviolável de eventos de identidade e acesso, permitindo que cada tentativa de login, cada autenticação bem-sucedida ou falha, cada alteração de privilégio e cada acesso a sistema crítico seja devidamente registrado com carimbo de data/hora, origem, contexto e resultado. Deverá prover indicadores de risco e relatórios gerenciais e técnicos, adequados para atendimento a auditorias internas, externas, órgãos de controle, demandas de transparência e exigências da LGPD, com visões específicas para segurança da informação, governança de TI, corregedoria e alta administração.

5.12.PAM – Gestão de Acessos Privilegiados – A solução PAM a ser contratada deverá contemplar, no mínimo, os seguintes componentes tecnológicos:

5.12.1. Cofre de credenciais privilegiadas (Password Vault): repositório seguro para armazenamento de senhas e chaves de contas privilegiadas, com criptografia forte, controle rigoroso de acesso, registro de check-out/check-in e

suporte à rotação automática de senhas, inclusive em múltiplos alvos (AD, servidores Linux/Windows, bancos de dados, dispositivos de rede, aplicações).

5.12.2. Broker de acesso privilegiado / Proxy de sessão: mecanismo de intermediação das conexões privilegiadas (RDP, SSH, SQL, consoles web administrativas etc.), permitindo que o usuário nunca visualize diretamente a senha, realizando o acesso por meio de sessão controlada, gravada e monitorada, com possibilidade de bloqueio em tempo real.

5.12.3. Gravação, monitoramento e replay de sessões: capacidade de gravar integralmente as sessões privilegiadas (tela, comandos, tempo, alvo), com armazenamento seguro e possibilidade de replay para auditoria e perícia digital. Deverá permitir a marcação automática de eventos críticos (por exemplo, execução de determinados comandos ou acesso a bases sensíveis) e geração de alertas ao SOC.

5.12.4. Gestão de ciclo de vida de contas privilegiadas: funcionalidades para criação, associação a responsáveis, definição de políticas de uso, rotação periódica, desativação e revogação de contas privilegiadas, em alinhamento com a solução IAM/IDMaaS garantindo coerência entre identidades, perfis e privilégios.

5.12.5. Fluxos de aprovação e acesso emergencial (break-glass): possibilidade de configurar fluxos de aprovação para acessos privilegiados a ativos críticos, incluindo acessos de emergência (break-glass), com registro de justificativa, tempo de validade e trilha completa das ações realizadas.

5.12.6. Integração com SIEM, ESM, SOC, IAM e demais soluções de segurança: a solução PAM deverá integrar-se ao SIEM para envio de logs detalhados, ao ESM para consolidação de risco, ao SOC para acionamento de playbooks de resposta a incidentes, à solução IAM para coerência de perfis e identidades, e a demais componentes (Defesa contra Ransomware/APT, Resposta a Incidentes, Forense Digital, Microsegmentação, SD-WAN) para suportar ações automatizadas de bloqueio e mitigação.

5.13. Hiperconvergência (Infraestrutura como Serviço): a contratação de uma plataforma Hiperconvergente como serviço, integrando computação, armazenamento e rede em um ambiente unificado, escalável e de alta disponibilidade, com administração centralizada pelo SOC e ESM.

5.13.1. Principais Funcionalidades:

- Consolidação de servidores, storage e rede em cluster Hiperconvergente.
- Alta disponibilidade nativa com failover automático.
- Escalabilidade sob demanda por adição de nós.
- Provisionamento rápido de recursos e redução de complexidade operacional.
- SLA mínimo de 99,7% de disponibilidade.
- Painéis unificados e integração com SOC/ESM.

5.13.2. Entregas Mínimas:

- Implantação completa da plataforma HCI.
- Configuração de clusters e políticas.
- Integração com SOC e ESM.
- Migração assistida de workloads.
- Documentação, treinamento e suporte.

5.14. Implantação de solução de gestão de serviços com fornecimento de serviços profissionais gerenciados: a contratação envolve serviços considerados especializados em Tecnologia da Informação e Comunicação na área de Operação, com monitoramento do ambiente 24x7 (vinte e quatro horas por dia x sete dias por semana) em serviços de Sustentação e Administração, Gerenciamento de Redes e Segurança de TIC, Serviços de Telefonia IP, Serviços de Virtualização, Servidores, Armazenamento e Backup, Serviços de Diretório, Administração de Banco de Dados, Middleware / Internet Web, Mensageria e Colaboração e Suporte a Instalações Físicas de TIC.

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

6.1. Requisitos de Continuidade do Negócio

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

6.2. Requisitos de sustentabilidade da solução de TIC

6.2.1. Não se aplica.

6.3. Requisitos da Capacitação

6.3.1. A CONTRATADA deverá repassar à CONTRATANTE todas as informações solicitadas e documentação da solução.

6.4. Requisitos Legais

6.4.1. O presente processo de contratação deve estar aderente à Constituição Federal, além dos seguintes instrumentos:

- Decreto-Lei nº 200/1967;
- Lei nº 14.133/2021 (Lei de Licitações); IN SGD/ME nº 94/2022 (Contratação de Soluções de TIC);
- Decreto nº 11.462, de 31 de março de 2023: Regulamenta os art. 82 a art. 86 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o sistema de registro de preços para a contratação de bens e serviços, inclusive obras e serviços de engenharia, no âmbito da Administração Pública federal direta, autárquica e fundacional;

- A Portaria SGD/MGI nº 5.950/2023 está explicitamente contemplada nos requisitos dispostos no ETP, bem como atendimento à estratégia de uso de software e de serviços de computação em nuvem, positivada na Portaria MinC nº 174/2024, em seu art. 4º, in verbis:

> *Art. 4º. Esta estratégia deve ser aplicada para novas contratações de software e de serviços de computação em nuvem no âmbito do Ministério da Cultura, tais como:*
>
> *I - software sob o modelo de licenciamento permanente de direitos de uso;*
>
> *II - software sob o modelo de cessão temporária de direitos de uso;*
>
> *III - software sob o modelo de subscrição ou como Serviço (SaaS);*
>
> *IV - infraestrutura como Serviço (IaaS);*
>
> *V - plataforma como Serviço (PaaS);*
>
> *VI - suporte técnico para software e serviços de computação em nuvem;*
>
> *VII - serviço de operação e gerenciamento de recursos em nuvem;*
>
> *VIII - serviço de migração de recursos para ambiente de nuvem;*
>
> *IX - integração de serviços de computação em nuvem; e*
>
> *X - consultoria especializada em software e/ou serviços de computação em nuvem.*

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

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 Gerais

6.5.1. A solução deve ser entregue em funcionamento, dessa forma, serão contemplados todos os serviços de instalação e configuração de todos os componentes adquiridos.

6.5.2. Os serviços de instalação e configuração deverão ser realizados por profissionais com capacidade técnica comprovada certificada na solução ofertada.

6.5.3. A contratação deve incluir transferência de conhecimento para a equipe técnica do Ministério, possibilitando que a mesma possa gerenciar e operar a solução tecnológica.

6.6. Requisitos Temporais

6.6.1. O prazo de vigência do contrato será de 60 (sessenta) 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.

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

6.7. Requisitos de Segurança

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

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

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

6.7.4. 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.

6.8. Requisitos de Projeto e Implementação

6.8.1. A solução de TIC deverá ser plenamente implementada pela Contratada no ambiente do MinC em no máximo 90 (noventa) dias corridos, a partir da assinatura da Ordem de Fornecimento ou Ordem de Serviço.

6.8.2. Por se tratar de expansão de solução já existente, o fornecimento em questão já deverá contemplar, em seus custos, o serviço de instalação dos módulos adicionais.

6.9. Requisitos de Garantia e Assistência Técnica

6.9.1. A Contratada deverá 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.

6.9.3. 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.

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

6.9.5. 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.

6.9.6. 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.

6.9.7. 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.

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

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

a) Telefone 0800 ou chamada com custo de ligação local em Brasília/DF;

b) E-mail;

c) Página web (ou chat) mantida pela CONTRATADA ou pelo FABRICANTE do equipamento.

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

6.9.11. 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.

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

6.9.13. 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.

6.9.14. 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.

6.10. Requisitos de Experiência Profissional

6.10.1. Capacidade Técnica do Licitante

6.10.2. Atestado(s) de Capacidade Técnica, emitido por pessoa física ou jurídica de direito público ou privado, demonstrando que a proponente prestou serviços /fornecimentos compatíveis com o objeto pretendido.

6.10.3. Declaração emitida pelo fabricante, especifica para este certame, de que a LICITANTE é uma parceira autorizada, demonstrando, desta forma, estar habilitada comercializar o objeto deste Estudo Técnico.

6.11. Requisitos Complementares

6.11.1. Deverão ser observados os regulamentos, normas e instruções de segurança da informação e comunicações adotadas, incluindo, mas não se limitando, ao definido na Política de Segurança da Informação (POSIN) e suas normas complementares, denominadas Normas Internas de Segurança da Informação, durante a execução dos serviços nas instalações do Ministério da Cultura.

6.11.2. Deverá ser garantida a disponibilidade, integridade, confidencialidade e sigilo dos documentos e informações inerentes ao contrato e seus serviços, podendo ser responsabilizado legalmente quem porventura causar perdas e danos ao Ministério da Cultura e a terceiros.

6.11.3. Devem ser utilizadas ferramentas de proteção e segurança de informações a fim de evitar qualquer acesso não autorizado aos sistemas e softwares, seja em relação ao que eventualmente estejam sob sua responsabilidade direta ou que foram disponibilizados, ainda que por meio de link.

6.11.4. Quando solicitado formalmente pela contratante, deverão ser realizadas, prioritária e concomitantemente, alterações para sanar possíveis problemas de segurança ou de vulnerabilidade nos referidos sistemas ou softwares utilizados para execução do serviço contratado.

6.11.5. Informar ao Ministério da Cultura, formal e tempestivamente, sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados.

6.11.6. Prestar os esclarecimentos necessários, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução.

6.11.7. Garantir a integridade e disponibilidade dos documentos e informações que, em função do Contrato, estiverem sob a sua guarda, sob pena de responder por eventuais perdas e/ou danos causados ao Ministério da Cultura e a terceiros.

6.11.8. Não divulgar, mesmo que em caráter estatístico, quaisquer informações originadas no Ministério da Cultura, sem prévia autorização.

6.11.9. Prover segurança através da utilização de identificação individual dos profissionais envolvidos na execução dos serviços.

6.11.10. Os profissionais deverão utilizar a conta de domínio que lhe for atribuída, de forma controlada e intransferível, mantendo secreta a sua respectiva senha, pois todas as ações efetuadas através desta, serão de responsabilidade do profissional do provedor da solução.

6.11.11. A Contratada deverá acatar e obedecer às normas de utilização e segurança das instalações do Ministério da Cultura.

6.11.12. A Contratada deverá manter os seus profissionais informados quanto às normas disciplinares, exigindo sua fiel observância, especialmente quanto à utilização e segurança das instalações.

6.11.13. Entendemos, ainda, que os requisitos necessários e suficientes à escolha da solução estão presentes ao longo deste estudo técnico. De maneira não exaustiva, seguem, abaixo, alguns deles:

- Eficiência: Atendimento pleno às necessidades de negócio da Ministério da Cultura aumentando a disponibilidade e garantindo qualidade e segurança da Infraestrutura Tecnológica;
- Eficácia: Mapear, testar e resolver as vulnerabilidades existentes nos recursos e serviços e Tecnologia da Informação do Ministério da Cultura que couberem ao projeto;
- Otimização de custos: Contratação de uma solução que atenda às necessidades pagando efetivamente pelo uso e produção;
- Visibilidade: Apoiar a gestão fornecendo completa visibilidade no acesso aos recursos da Ministério da Cultura;
- Disponibilidade Nacional: Atendimento 24x7 em todas as unidades da Ministério da Cultura distribuídas no Brasil além daqueles usuários que desempenham suas atividades de maneira remota.

7. Estimativa da demanda - quantidade de bens e serviços

7.1 A inspiração da presente contratação são os Contratos Administrativos 65/2021 e 69/2023, entre Ministério da Gestão e Inovação em Serviços Públicos - MGI e, respectivamente, o Serviço Federal de Processamento de Dados - Serpro e a Empresa de Tecnologia e Informações da Previdência – Dataprev e recentemente o Contrato n° 17/2025 celebrado entre o Ministério da Educação e a TELEBRÁS.

7.2. Com o objetivo de fomentar a inovação na gestão pública, o MGI, atualmente responsável pela coordenação do programa ColaboraGov, estruturou um modelo contratual que possibilita à sua unidade de TIC responder, de forma ágil e eficiente, a demandas originadas de diferentes ministérios. Essas demandas, em grande parte, são decorrentes de agendas de políticas públicas com características dinâmicas e, muitas vezes, imprevisíveis.

7.3. Seguindo essa diretriz estratégica, o Ministério da Cultura, embora com um número mais restrito de unidades demandantes em comparação ao MGI, enfrenta desafios semelhantes. A execução das políticas culturais requer flexibilidade e capacidade de resposta célere, considerando a diversidade de linguagens, territórios, públicos e projetos envolvidos. Assim, identificou-se nessa abordagem uma oportunidade para fortalecer a capacidade do MinC em atender prontamente a solicitações variáveis e não antecipáveis no campo da cultura.

7.4. Durante a análise preliminar das possibilidades contratuais com empresas públicas de TIC, verificou-se, ainda, a pertinência de incluir a Telebrás no escopo de avaliação, tendo em vista sua atuação voltada à oferta de serviços de conectividade e infraestrutura. Tais componentes são essenciais para garantir a continuidade e a expansão dos serviços digitais culturais promovidos pelo Ministério da Cultura.

7.5 Dimensionamento da Demanda

7.5.1 O dimensionamento da demanda foi realizado pela Equipe de Planejamento da Contratação, e os dados consolidados são apresentados a seguir. A análise também considerou as contratações em andamento no biênio 2024/2025, sob responsabilidade da Subsecretaria de Tecnologia da Informação e Inovação - STII.

7.6 Contratações em Andamento

7.6.1 As contratações em andamento refletem a amplitude das demandas de bens e serviços de tecnologia da informação e comunicação necessárias ao atendimento das atividades do Ministério. Devido à sua relevância estratégica e aderência às necessidades institucionais, essas iniciativas foram consideradas no processo de estimativa de demanda para a presente contratação.

CONTRATAÇÕES EM ANDAMENTO 2024/2025 – STII

OBJETO	PROCESSO SEI
Gestão de Identidade e Acesso	01400.013416/2023-42
Análise de Vulnerabilidades	01400.013415/2023-06
Auditoria de Dados	01400.019209/2023-00
Backup (Appliance)	01400.003738/2025-45
Storage	01400.004382/2025-67
F5	01400.013364/2023-12
Hiperconvergência	01400.024824/2025-91

Big Data (SNIIC)	–

7.6.2 **Descrição das contratações em andamento**

As contratações listadas acima irão integrar o escopo da presente contratação, conforme detalhado a seguir:

- **Auditoria de Dados**: Contratação de solução de segurança da informação para auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (Microsoft Active Directory), correio eletrônico (Microsoft Exchange Server) e servidores de arquivos. Visa garantir a governança, a rastreabilidade e a proteção de informações estratégicas, complementando soluções existentes (como DLP), com análise preditiva e resposta proativa a incidentes, em conformidade com LGPD e Estratégia Nacional de Segurança Cibernética (E-Cyber).

- **Análise de Vulnerabilidades:** Aquisição de soluções para a gestão contínua de vulnerabilidades de segurança cibernética por 12 meses. Com implantação, garantia de assistência técnica e transferência de conhecimento. Visa melhorar a segurança da rede, moderniza camadas de proteção e automatiza a identificação de ameaças, oferecendo respostas rápidas às equipes de segurança.

- **Backup (Appliance):** Contratação de solução de appliance para proteção de dados com segurança, incluindo serviços de instalação. Visa proteger dados contra exclusões e ataques maliciosos, assegura continuidade dos serviços e garante compatibilidade com softwares de backup existentes.

- **Storage:** Contratação de solução tecnológica para expansão de solução de armazenamento de dados, incluindo serviços de instalação. Trata-se da ampliação da capacidade de armazenamento, permitindo a preservação do acervo audiovisual do CTAv e consolidação de dados do Ministério da Cultura.

- **F5 – Balanceador de Cargas:** Contratação da Prestação de Serviços de direito de atualizações de versões, renovação de appliance, manutenção e suporte da para as licenças já pertencentes ao MinC. Otimiza tráfego entre servidores e usuários, aumentando disponibilidade, escalabilidade, segurança e desempenho; solução atual defasada.

- **Gestão de Identidade e Acesso:** Aquisição de soluções para a gestão contínua de segurança para Gestão de Identidade e Gestão de Acesso por 12 (doze) meses, com garantia de suporte e atualização. A solução visa identificar e corrigir vulnerabilidades continuamente, fortalecendo a infraestrutura tecnológica do MinC.

- **Big Data (SNIIC) - Data Lake:** Contratação de aplicação de Big Data no SNIIC, consolidando dados culturais em repositório único para apoio à gestão pública.

- **Hiperconvergência:** Contratação de uma Solução de Infraestrutura Computacional Hiperconvergente (HCI). Essa contratação torna-se fundamental para garantir a eficiência, escalabilidade e segurança necessárias para atender às exigências atuais e futuras deste Ministério da Cultura.

7.7 Contratações Vigentes

7.7.1 A pretensa contratação tem por objetivo substituir o Contrato nº 01/2023, firmado com o Serpro – Infovia, relativo ao fornecimento de links de conectividade e acesso à internet, por links de conectividade baseados em tecnologia SD-WAN, que interligarão as unidades do Ministério da Cultura, bem como substituir, em sua totalidade, o Contrato nº 02 /2023 – Segurança em Nuvem, referente ao processo SEI nº 72031.009972/2022-27.

7.8. Serviços a serem contratados:

7.8.1 Desta forma, considerando o cenário supracitado, de modo a definir quantitativos compatíveis com as características do Ministério da Cultura, e ainda visando a possibilidade de implementação gradativa, a equipe de planejamento da contratação considerou razoável a adoção dos quantitativos para a realização de uma pretensa contratação com os itens e quantidades estão listados no quadro a seguir:

LOTE	ITEM	DESCRIÇÃO DO ITEM	DETALHAMENTO DO ITEM	QUANTIDADE ESTIMADA	LOCALIZAÇÃO NO ETP DA QUANTIDADE ESTIMADA
Único	1	Conectividade	SD-WAN - (conectividade + internet)	2300	Item 7.10.1
	2	Imageamento	Monitoramento satelital	1000	Item 7.10.2
			Gestão de imagens e recursos		Item 7.10.2
	3	Backup-as-a-Service (BaaS)	Backup e Recuperação de Desastres (DRaaS)	1000	Item 7.10.3
	4	Edge Computing	Monitoramento de Eventos e Logs (SIEM)	2300	Item 7.10.4
			Gestão de Identidade e Acesso (IAM/IDMaaS)		Item 7.10.5
			Gestão de acessos privilegiados – (PAM)		Item 7.10.6
			Auditoria e Governança de Dados		Item 7.10.7
			Anti-Ransomware		Item 7.10.8
			ESM/ITSM com AIOPs		Item 7.10.9
			Análise Contínua de Vulnerabilidades		Item 7.10.10
			Resposta a Incidentes e Forense Digital		Item 7.10.11
			Detecção e Resposta a Incidentes		Item 7.10.12
	5	Platform-as-a-Service (PaaS)	Data Lake	1750	Item 7.10.13
			Infraestrutura-as-a-Service (Hiperconvergência)		Item 7.10.14

7.9 A seguir segue descrição dos serviços a serem contratados:

7.9.1. Item 1- Conectividade: SD-WAN (Software-Defined Wide Area Network). Esse serviço abrange:

1. Rede inteligente de interconexão entre unidades do MinC e datacenters;
2. Otimização de tráfego e priorização de aplicações críticas;
3. Gerenciamento centralizado e segmentação por políticas;
4. Redução de custos com conectividade e aumento de performance.

7.9.2. Item 2- Imageamento - Monitoramento satelital e Gestão de imagem e recursos. Esses serviços abrangem:

1. Monitoramento satelital: Abrange o monitoramento contínuo de áreas de interesse cultural por meio de imagens de satélite, incluindo a obtenção, o processamento e a análise de dados geoespaciais, com o objetivo de acompanhar a evolução temporal das áreas monitoradas, identificar alterações relevantes e subsidiar ações de planejamento, fiscalização e tomada de decisão.

2. Gestão de imagem e recursos: Abrange a gestão do acervo de imagens e dos recursos associados, contemplando a organização, o armazenamento, o tratamento, o controle de metadados, a catalogação, a recuperação e a disponibilização das informações geoespaciais, assegurando a integridade, a rastreabilidade e o acesso eficiente aos dados para uso institucional.

7.9.3. Item 3 - Backup-as-a-Service (BaaS) - Backup e Recuperação de Desastres (DRaaS) . Esse serviço abrange:

1. Cópias seguras e criptografas de todos os dados críticos do MinC;
2. Retenção mínima de 30 dias em nuvem soberana;
3. Backups imutáveis e testados periodicamente;
4. Tempo máximo de recuperação (RTO): 4 horas.

7.9.4. Item 4 - Edge Computing. Esse serviço abrange:

Monitoramento de Eventos e Logs (SIEM):

1. Plataforma unificada de coleta, correlação e análise em tempo real de eventos de segurança;
2. Integração com Active Directory, Exchange, servidores, firewall, switches, endpoints e aplicações críticas.
3. Dashboards, alertas e relatórios customizáveis com retenção mínima de 12 meses;
4. Correlação com incidentes de IAM, PAM, XDR e vulnerabilidades.

Gestão de Identidade e Acesso (IAM/IDMaaS).

1. Gerenciamento de identidades;
2. Autenticação e Autorização;
3. Gestão de Privilégios;
4. Acesso a Aplicações e Recursos;
5. Conformidade e Auditoria.

Gestão de acessos privilegiados – (PAM).

1. Cofre seguro de senhas administrativas com autenticaçõ multifator;
2. Controle Just - in- Time (JIT) de privilégios e rotação automática de senhas;
3. Gravação e auditoria de todas as sessões privilegiadas.

Auditoria e Governança de Dados.

1. Rastreamento de todas as ações em AD, Exchange, File Servers e bancos de dados;
2. Geração de relatórios automáticos de conformidade (LGPD, ISO 27001, COBIT, GDPR);
3. Correlação com IAM e SIEM para detecção de comportamentos anômalos.

Anti-Ransomware.

1. Monitoramento contínuo contra comportamentos criptográficos anômalos;
2. Isolamento automático de máquinas afetadas e bloqueio de conexões C2;
3. Integração direta entre XDR, PAM, IAM e Backup para restauração imediata;
4. Relatórios mensais de tentativas de ataque, incidentes contidos e métricas de resiliência.

ESM/ITSM com AIOPs.

1. Gestão dos processos corporativos em integração com RH, Marketing, Financeiro e Jurídico;
2. Gestão dos processos ITIL em sua versão V4, como: incidentes, problemas, mudanças, configuração e catálogo de serviços;

3. Automação de processos utilizando AIOps com Aprendizado de Máquina (ML) e Inteligência Artificial (IA);
4. Centralização das solicitações em portal único;
5. Gestão dos processos interdepartamentais.

Análise Contínua de Vulnerabilidades.

1. Varredura periódica em redes, sistemas e aplicações, com detecção de falhas críticas;
2. Classificação de riscos e relatórios priorizados;
3. Integração com o SOC para geração automática de tickets de correção;
4. Testes de intrusão controlados (pentests) trimestrais.

Resposta a Incidentes e Forense Digital.

1. Ações imediatas de conteção e mitigação de ameaças;
2. Coleta e preservação de envidências digitais;
3. Relatórios de incidentes e recomendações de remediação;
4. Apoio técnico a investigações da CGU, TCU e orgãos de controle.

Detecção e Resposta a Incidentes.

1. Detecção comportamental em endpoints e rede (Leste-Oeste);
2. Resposta automatizada a ameaças, com isolamento de dispositivos e reversão de mudanças;
3. Visibilidade completa de campanhas de ataque e ameaças persistentes (APT);
4. Tempo máximo de resposta: 30 minutos após detecção confirmada.

7.9.5. Item 5 - Platform-as-a-Service (PaaS). Data Lake e Infraestrutura-as-a-Service- Hiperconvergência. Esse serviço abrange:

1. Virtualização de Dados;
2. Governança de Dados;
3. Análises Avançadas, visualização de dados;
4. Data Self-Service para gestores, pesquisadores e sociedade civil.
5. Consolidação de servidores, armazenamento e rede em uma infraestrutura unificada;
6. Alta disponibilidade e escalabilidade sob demanda;
7. Redução de complexidade de custos de manutenção;
8. SLA mínimo de 99,7% de disponibilidade;
9. Administração centralizada pelo SOC e ESM.

7.10. DETALHAMENTO DA ESTIMATIVA

7.10.1 CONECTIVIDADE

7.10.1.1 Para melhor entendimento dos serviços atrelados à **CONECTIVIDADE** (Links de Comunicação), destacamos que o cenário atual do Ministério da Cultura é composto pela **Sede Administrativa**, localizada no Bloco B da Esplanada dos Ministérios, pelo **Anexo Administrativo**, situado no Edifício Venâncio Shopping, e pela **Biblioteca Demonstrativa de Brasília (BDB)**. Essas unidades concentram parcela significativa das atividades administrativas, técnicas e finalísticas do órgão, demandando conectividade à Internet com elevados padrões de desempenho, disponibilidade e segurança, compatíveis com a criticidade dos serviços prestados.

7.10.1.2 Em âmbito nacional, o Ministério da Cultura possui atualmente **24 Escritórios Estaduais**, distribuídos em quase todas as Unidades da Federação, além do **Centro Técnico Audiovisual –**

CTAV, localizado no Rio de Janeiro. Essas estruturas descentralizadas desempenham papel estratégico na execução das políticas públicas culturais, exigindo acesso contínuo e confiável à Internet para comunicação institucional, utilização de sistemas corporativos, serviços digitais e interação com o público externo.

7.10.1.3 Atualmente, a fornecedora dos serviços de links de comunicação e de acesso à Internet é a empresa **Serviço Federal de Processamento de Dados – SERPRO**. Com a nova contratação, pretende-se **substituir integralmente os enlaces atualmente existentes**, que incluem conexões de 10 Mbps e 1 Mbps, bem como o serviço de acesso à Internet de 400 Mbps, por links baseados em tecnologia SD-WAN. A nova solução deverá oferecer maior capacidade de banda, melhor desempenho, maior estabilidade, escalabilidade e mecanismos avançados de segurança, superando as limitações observadas na infraestrutura atualmente contratada.

7.10.1.4 A tabela abaixo resume a **quantidade estimada de serviços de acesso dedicado à Internet (IAN)** e de **links IP dedicados** a serem fornecidos no âmbito da presente contratação:

1. Serviço de acesso dedicado à INTERNET com solução de proteção Anti DDoS			
Item	**Descrição**	**Quantidade**	**Mbps**
1.1	**Serviço de acesso dedicado à Internet com solução de proteção Anti DDoS - Sede MinC – Bloco B**	**1**	**5000**
2. Serviço de LINK IP para os Escritórios do MinC			
Item	**Descrição**	**Quantidade**	**Mbps**
2.1	**Serviço de conexão IP dedicado- Sede MinC – Bloco B**	**1**	**10000**
2.2	**Serviço de conexão IP dedicado- Anexo Minc – Venâncio Shopping**	**1**	**2000**
2.3	**Serviço de conexão IP dedicado- Biblioteca Demonstrativa de Brasília - BDB**	**1**	**2000**
2.4	**Serviço de conexão IP dedicado- CTAV – Rio de Janeiro**	**1**	**1000**
2.5	**Serviço de conexão IP dedicado- Capanema - Rio de Janeiro**	**1**	**1000**

2.6	**Serviço de conexão IP dedicado para os Escritórios do MinC localizado na Região Norte do País.**	**7**	**300**
2.7	**Serviço de conexão IP dedicado para os Escritórios do MinC localizado na Região Sul do País.**	**3**	**300**
2.8	**Serviço de conexão IP dedicado para os Escritórios do MinC localizado na Região Nordeste do País.**	**8**	**300**
2.9	**Serviço de conexão IP dedicado para os Escritórios do MinC localizado na Região Sudeste do País.**	**3**	**300**
2.10	**Serviço de conexão IP dedicado para os Escritórios do MinC localizado na Região Centro Oeste do País.**	**3**	**300**

7.10.1.5 A demanda do órgão tem como base os seguintes **endereços institucionais**, os quais deverão ser atendidos pelos serviços de Internet Access Network e links dedicados previstos nesta contratação:

- **Sede MinC** – Esplanada dos Ministérios, Bloco B, Ministério da Cultura, Zona Cívico-Administrativa, Brasília/DF, CEP 70068-900;
- **Anexo MinC** – SCS, Quadra 8 (Asa Sul), Brasília/DF, CEP 70333-900;
- **Biblioteca Demonstrativa** – EQS 506/507, Brasília/DF, CEP 70350-580;
- **CTAV – Centro Técnico Audiovisual** – Av. Brasil, nº 2482, Rio de Janeiro/RJ, CEP 20930-040;
- **Edifício Capanema** – Rua da Imprensa, nº 16, Rio de Janeiro/RJ, CEP 21920-070;
- **Escritórios Regionais**, conforme endereços institucionais listados na tabela a seguir:

UF	Endereço Institucional
SÃO PAULO	Alameda Nothmann, Nº 1058, Campos Elíseos –São Paulo
CEARÁ	Rua Liberato Barroso, 525 – Centro. Fortaleza (CE)
PERNAMBUCO	R. Padre Floriano, no 160 - São José, Recife - PE, 50020-060
AMAZONAS	Rua Marechal Deodoro, nº 27, 8º andar, Centro CEP 69.005-000, Manaus (AM)
SANTA CATARINA	Rua Victor Meirelles, 198, Centro Florianópolis/SC

GOIÁS	Centro Cultural. Q. 71 - Av. Universitária, 1533 - Setor Leste Universitário, Goiânia
AMAPÁ	Av. Henrique Galucio, 1242 - Central, Macapá - AP, 68900-115
TOCANTINS	ACNE 1, Conjunto 01, Avenida Juscelino Kubitschek - JK, Rua nº 01, Lt. 41 A, Edifício Encanel, 5º andar. Palmas (TO)
RORAIMA	3512, Av. Nossa Sra. da Consolata, 3336 - São Vicente, Boa Vista - RR
MARANHÃO	R. do Giz, 235 - Centro, São Luís - MA, 65010-680
PARÁ	Tv. Antônio Baena, 1113 - Marco, Belém -PA
RIO GRANDE DO NORTE	Av. Duque de Caxias, nº 158, Ribeira CEP 59.012-200, Natal (RN) (84) 3211-3820
MINAS GERAIS	Conservatório UFMG - Av. Afonso Pena, 1534, Belo Horizonte - MG
RIO GRANDE DO SUL	R. Sete de Setembro, 1020 - Centro Histórico, Porto Alegre - RS, 90010-191
PARAÍBA	A definir
MATO GROSSO	Av. Ver. Juliano da Costa Marques, 99 - Centro Político Administrativo, Cuiabá - MT
ESPÍRITO SANTO	Rua Pietrângelo De Biase, 56. Centro. Vitória- ES
MATO GROSSO DO SUL	Rua Pimenta Bueno, 139. Amambaí. Campo Grande- MS
PIAUÍ	Praça Marechal Deodoro S/N - Centro
SERGIPE	R. Pacatuba, 171 - Centro, Aracaju - SE, 49010-150
ALAGOAS	Praça Dom Pedro II, 16 - CEP 57020-130, Centro. Maceió- (AL)
RONDÔNIA	Av. Lauro Sodré, 6500 - Aeroporto, Porto Velho - RO, 76803-260
ACRE	Rua Amazonas, 568 (esquina com Rua Benjamin Constant, 1088), bairro Cadeia Velha, Rio Branco – AC, CEP 69.900-365

PARANÁ	Rua Marechal Deodoro, 555, Centro, Curitiba - PR

7.10.1.6 Um aspecto singular desta contratação refere-se às **peculiaridades associadas aos pontos de acesso à Internet nas diversas regiões do território nacional**, os quais devem ser compreendidos como serviços essenciais e estratégicos. As demandas relacionadas à criação, ampliação ou reorganização das estruturas organizacionais do Ministério da Cultura podem ocorrer de forma intempestiva, exigindo capacidade de rápida expansão e adaptação da infraestrutura de conectividade. Nesse contexto, o acesso confiável à Internet e à rede de dados constitui elemento fundamental para o adequado desempenho das atividades institucionais.

7.10.1.7 Para estimar a necessidade de serviço de acesso à Internet da **Sede do MinC – Bloco B**, a equipe de planejamento da contratação fundamentou-se na **quantidade de usuários ativos**, no perfil de utilização da Internet, na criticidade das aplicações acessadas, bem como na intensidade do tráfego gerado pelas atividades administrativas, técnicas e de gestão. A análise considerou, ainda, padrões de uso simultâneo e picos de acesso, conforme demonstrado na tabela de dimensionamento elaborada para esse fim.

7.10.1.8 Com base nos resultados obtidos e considerando os períodos de **maior concentração de acessos e utilização intensiva da Internet**, foi aplicado um acréscimo de **20% de margem técnica**, de forma a assegurar capacidade adicional para absorção de picos de demanda e crescimento futuro. Assim, após o arredondamento técnico da capacidade necessária, concluiu-se que o valor de **5 Gbps** atende de maneira adequada e segura às necessidades atuais e projetadas do Edifício Sede do Ministério da Cultura.

7.10.1.9 Para a estimativa dos serviços de acesso à Internet do **Edifício Venâncio Shopping** e da **Biblioteca Demonstrativa de Brasília**, a equipe de planejamento da contratação considerou o histórico recente de acessos, o volume de tráfego gerado, bem como a quantidade expressiva de reclamações relacionadas à qualidade do serviço atualmente disponível, especialmente no que se refere à Biblioteca Demonstrativa. Observou-se que parcela significativa dos usuários manifesta insatisfação com a solução vigente, evidenciando a necessidade de ampliação de banda, melhoria de desempenho e maior estabilidade do acesso à Internet.

7.10.1.10 Adicionalmente, no Edifício Venâncio Shopping encontram-se instaladas diversas unidades organizacionais cujas atividades demandam uso intensivo da Internet, especialmente em processos relacionados ao audiovisual, à gestão administrativa e à atuação correcional, destacando-se:

- **SAV – Secretaria do Audiovisual**;
- **DFIA – Diretoria de Formação e Inovação Audiovisual**;
- **DPDA – Diretoria de Preservação e Difusão Audiovisual**;
- **DIGEC – Diretoria de Gestão Coletiva de Direitos Autorais**;
- **SDAI – Secretaria de Direitos Autorais e Intelectuais**;
- **DIREG – Diretoria de Regulação de Direitos Autorais**;
- **COREG – Corregedoria**.

7.10.1.11 No que se refere aos **serviços de links de comunicação**, verifica-se a necessidade de disponibilização de enlaces com **velocidade mínima de 300 Mbps** para as unidades descentralizadas, considerando que parte dessa capacidade de banda será compartilhada com os serviços de acesso à Internet, garantindo desempenho adequado, continuidade operacional e suporte às atividades institucionais desenvolvidas nas respectivas localidades.

7.10.2 Imageamento

7.10.2.1 O objetivo principal destes serviços é garantir o acesso a imagens de satélite, radar SAR, modelagem digital e inteligência geoespacial, permitindo: Diagnóstico territorial cultural, Identificação de infraestrutura e equipamentos culturais; Monitoramento de bens tombados e patrimônios culturais; Estudos de impacto cultural e ambiental; Apoio ao mapeamento nacional do SNC e Mapas da Cultura; Tomada de decisão baseada em dados espaciais; Transparência sobre o investimento público em cultura.

7.10.2.2 Principais serviços a serem contratados:

- Mapeamento geoespacial de pontos culturais;
- Identificação de vazios culturais em regiões remotas
- Mapas geográficos de atividades culturais;
- Dashboards públicos integrando imagem + investimentos públicos;
- Auditoria remota de equipamentos e projetos financiados;
- Priorização de investimento federal baseado em território;
- Detecção de danos e alterações indevidas;
- Apoio a políticas para povos indígenas e comunidades quilombolas;
- Acompanhamento visível de obras e gastos culturais;
- Auditoria remota de equipamentos e projetos financiados;
- Planejamento 3D de grandes eventos culturais;
- Análises de terreno para instalações temporárias;
- Apoio ao CTAv em produções e gravações aéreas.

7.10.3 Backup-as-a-Service (BaaS)

7.10.3.1 O objetivo fundamental da contratação deste serviço é assegurar a continuidade operacional, preservação digital e recuperação de desastres para sistemas críticos (SALIC, SNC, Mapas da Cultura, SNIIC e Data Lake).

7.10.3.2 Principais serviços a serem contratados:

- Backup e Recuperação de Desastres (DRaaS): ambientes ativo-passivo com replicação geográfica entre empresa pública federal provedora de conectividade e infraestrutura de TIC e MinC;
- Gestão Documental Integrada: digitalização e versionamento seguro de acervos digitais e processos administrativos;
- Armazenamento e curadoria do acervo digitalizado do CTAV, permitindo a preservação das obras para além do meio físico;
- Backup Air-Gap e Anti-Ransomware: isolamento físico e criptográfico de cópias de segurança;
- Monitoramento e Relatórios de Integridade de Backup: verificação periódica automatizada;
- Retenção de longo prazo e arquivamento de dados culturais digitais.
- Está prevista como evolução, a adoção de modelos imutáveis (Object Lock) e integração nativa com o Data Lake MinC.

7.10.4 MONITORAMENTO E EVENTOS E LOGS (SIEM) -Security Information and Event Management integrada ao SOC da Telebras

7.10.4.1 A solução de SIEM deverá ser dimensionada para suportar, no mínimo, o ambiente tecnológico atual do MinC, com margem de crescimento, observando-se a integração com o SOC Telebras.

7.10.4.2 Os quantitativos abaixo representam a capacidade operacional mínima para garantir: coleta e armazenamento de logs, correlação de eventos, abertura e gestão de incidentes, geração de relatórios e atendimento a requisitos de auditoria e conformidade, em linha com o Termo de Referência do SIEM e com o documento de Serviços MinC x Telebras.

Item	Componente SIEM	Unidade	Quantitativo Mínimo	Fundamentação
1	Fontes de log monitoradas	Fonte	600	Capacidade mínima prevista no TR SIEM para processamento de até 600 fontes simultâneas.
2	Volume diário de eventos processados	GB/dia	60 GB/dia	Especificação de capacidade do TR SIEM (60 GB/dia), com possibilidade de expansão por licenciamento.
3	Coletoras/agents remotos implantados	Coletor	50	Cobertura de datacenters, sede, anexo, CTAv e escritórios/unidades remotas, com margem para expansão (aprox. 1 coletor por grupo de sites críticos).
4	EPS garantidos para o MinC (equivalente)	EPS	≈ 2.500 EPS	Conversão estimada de 60 GB/dia para EPS, para dimensionamento contratual, conforme previsão de equivalência GB /dia ↔ EPS no TR.
5	Incidentes de segurança gerenciados pelo SIEM/SOC	Caso/mês	200	Volume compatível com o ambiente do MinC, ampliando o baseline de ~150 incidentes/mês já estimado para IR considerando maior visibilidade do SIEM.
6	Dashboards operacionais e executivos	Dashboard	25	Visões para segurança, redes, LGPD, sistemas críticos, conectividade, gestão e governança (técnico + tático + estratégico).
7	Relatórios automáticos agendados	Relatório /mês	40	Relatórios técnicos, mensais por domínio (rede, aplicações, IAM, PAM, vulnerabilidades, LGPD, auditoria), além de consolidados para gestão.
8	Usuários com acesso à console de SIEM	Usuário	40	Equipes do SOC Telebras, equipes técnicas do MinC (rede, sistemas, segurança) e perfis de auditoria /governança.
9	Retenção de logs on-line para investigação	Dias	365 dias	Atende boas práticas de auditoria, LGPD e necessidade de análise histórica e correlação de eventos complexos.

7.10.4.3 Memória de cálculo (estimativa)

- Fontes de log monitoradas (600) – capacidade de até 600 fontes simultâneas para 60 GB/dia de processamento. Adota-se esse valor como capacidade mínima garantida, alinhada com o modelo Telebras.
- Volume diário de eventos – 60 GB/dia, correspondente a “capacidade de processamento de até 60 GB/dia”. Corresponde a ≈ 1,8 TB/mês (60 × 30), com possibilidade de expansão com novos servidores/licenças.
- Coletoras/agents remotos (50). Serviços MinC x Telebras indicam múltiplos pontos (Sede, Anexo, CTAv, escritórios estaduais, polos regionais, ambientes de PAC Cultura, etc.). Considerando clusters de sites e margem de crescimento, adota-se 50 coletores para assegurar resiliência e segmentação (produção, testes, ambientes sensíveis).
- EPS garantidos (~2.500 EPS) – se a mensuração for por EPS, deve ser fornecido o equivalente aos 60 GB/dia. Para efeito de ETP, assume-se valor de referência de ≈2.500 EPS, compatível com ambientes federais de porte semelhante, sem exaurir a capacidade de 60 GB/dia.
- Incidentes de segurança gerenciados (200/mês). Para IR já foi adotado baseline de ~150 incidentes/mês. Com maior visibilidade e correlação do SIEM, eleva-se a expectativa para 200 incidentes/mês, incluindo: tentativas bloqueadas; correlações de baixo/alto risco; incidentes confirmados enviados ao SOC.
- Dashboards (25). Baseado em: Segurança/Operações: ~12 dashboards (rede, endpoint, IAM, PAM, vulnerabilidades, nuvem etc.); LGPD, auditoria e conformidade: ~8; visão executiva/estratégica: ~5 (indicadores consolidados para alta gestão).
- Relatórios agendados (40/mês). Relatórios mensais por domínio (rede, aplicações, bancos, IAM, PAM, vulnerabilidades, LGPD, auditoria, SOC etc.) + relatórios consolidados tático-estratégicos.
- Usuários de console (40). SOC Telebras (analistas L1/L2/L3, coordenação). Equipes internas MinC (infra, sistemas, segurança, governança).
- Retenção de logs – 365 dias – Relaciona se à necessidade de investigações históricas, análises preditivas e atendimento a obrigações de auditoria e LGPD.

7.10.5 IAM/IDMaaS- Gestão de Identidade e Acesso - AUTENTICAÇÃO CENTRALIZADA E MFA

7.10.5.1 A volumetria a seguir representa os quantitativos mínimos necessários para garantir a governança, a rastreabilidade e a segurança de identidades e acessos no Ministério da Cultura.

7.10.5.2 Os valores foram calculados com base nos ativos de TIC, nas unidades organizacionais, nos perfis de usuários (servidores efetivos, comissionados, terceirizados, bolsistas, prestadores externos), nas integrações previstas com outras soluções de segurança e na volumetria de eventos estimada para o SIEM e demais componentes.

Item	Componente IAM /IDMaaS	Unidade	Quantitativo	Fundamentação
1	Identidades gerenciadas	Identidades	3.200	Servidores (1.900), terceirizados (450), prestadores/bolsistas (150), contas de serviço e sistemas (700)
2	Autenticações mensais	Evento/mês	180.000	Média aproximada de 6.000 logins/dia × 30 dias
3	Acessos com MFA	Evento/mês	65.000	Perfis sensíveis com MFA obrigatório, estimados em 1.500 usuários × ~43 logins /mês
4		Acesso/mês	450	

	Provisionamentos automáticos			Entradas de novos usuários internos, terceirizados e perfis temporários
5	Desprovisionamento (automáticos)	Acesso/mês	380	Saídas, movimentações, expiração de contratos e encerramento de perfis temporários
6	SSO – integrações	Aplicação	95	Sistemas internos MinC + soluções SaaS + integrações com Telebras e outras empresas públicas
7	Recertificação de privilégios	Conta/trimestre	3.200	Recertificação de 100% das identidades cadastradas
8	Sessões privilegiadas monitoradas	Sessão/mês	1.500	Estimativa de sessões administrativas em sistemas críticos, IAM + PAM integrado
9	Alertas de login anômalo	Alerta/mês	1.400	Cerca de 0,8% das autenticações mensais gerando alertas de comportamento anômalo
10	Bloqueios automáticos de autenticação	Evento/mês	350	Política anti-brute force, falhas repetidas e violações de política de acesso

7.10.5.4 Memória de cálculo (estimativa)

7.10.5.4.1 Identidades gerenciadas (3.200). Sendo:

- Servidores/estatutários e comissionados: 1.900
- Terceirizados: 450
- Prestadores, bolsistas, consultores, perfis de projeto: 150
- Contas de serviço, APIs, integrações de sistema a sistema, identidades técnicas: 700
- Total: 3.200 identidades.

7.10.5.4.2 Autenticações mensais (180.000)

- Considerando a quantidade de usuários e sistemas, estima-se média de 6.000 autenticações por dia, entre acessos internos, remotos, VPN, aplicações web e serviços em nuvem. Em um horizonte de 30 dias, obtém-se: 6.000 × 30 = 180.000 eventos de autenticação/mês.

7.10.5.4.3 Acessos com MFA (65.000)

- Perfis com MFA obrigatório (dirigentes, admins, desenvolvedores, operadores de dados pessoais, contas críticas) são estimados em aproximadamente 1.500 usuários, cada um realizando, em média, 40–45 autenticações mensais em sistemas críticos. Sendo: 1.500 × ~43 ≈ 64.500, arredondando-se para 65.000 eventos/mês com MFA.

7.10.5.4.4 SSO – integrações (95)

- Consideram-se aplicações legadas internas, sistemas corporativos, soluções SaaS, sistemas de Big Data /SNIIC, plataformas colaborativas, serviços expostos e aplicações fornecidas ou integradas com a Telebras e outras empresas públicas, totalizando cerca de 95 aplicações elegíveis à integração via SSO.

7.10.5.4.5 Alertas de login anômalo (1.400)

- Tomando-se como base a estimativa de 180.000 autenticações/mês e assumindo-se que cerca de 0,8% destes eventos podem ser classificados como suspeitos ou anômalos (localização incomum, dispositivo novo, tentativas reiteradas, padrões fora da curva), obtém-se: 180.000 × 0,8% = 1.440 → arredondado para 1.400 alertas/mês.

7.10.5.4.6 Os demais quantitativos (provisionamentos, desprovisionamento, sessões privilegiadas e bloqueios automáticos) seguem a mesma lógica de dimensionamento conservador, apta a garantir a capacidade da solução IAM /IDMaaS em operar com segurança, folga operacional e possibilidade de crescimento ao longo da vigência contratual.

7.10.6 Gestão de acessos privilegiados – (PAM)

7.10.6.1 A volumetria a seguir apresenta os quantitativos mínimos necessários para que a solução PAM seja capaz de gerenciar, com segurança e folga operacional, as contas privilegiadas e sessões administrativas do Ministério da Cultura, considerando o porte da instituição, a infraestrutura descrita no ETP e os demais artefatos correlatos (IAM, ESM, SIEM, SOC, Edge, SD-WAN).

Item	Componente PAM	Unidade	Quantitativo	Fundamentação
1	Contas privilegiadas gerenciadas	Conta	650	Inventário de contas administrativas (domínio, servidores, DB, rede, aplicações, serviço)
2	Credenciais /cofre (entradas no vault)	Credencial	1.300	Média de 2 credenciais por conta (senha + chave/API/outro fator técnico)
3	Sessões privilegiadas monitoradas	Sessão /mês	1.500	Estimativa de sessões administrativas mensais em ambiente híbrido (on-prem + nuvem + SD-WAN)
4	Sessões privilegiadas gravadas	Sessão /mês	1.500	100% das sessões privilegiadas devem ser gravadas
5	Rotação automática de senhas	Evento /mês	650	Rotação ao menos mensal de todas as contas privilegiadas

6	Acessos emergenciais (break-glass)	Evento /mês	180	Média de 6 acessos emergenciais/dia em ativos críticos
7	Workflows de aprovação de acesso	Workflow	80	Combinação de perfis, unidades, tipos de recurso e níveis de aprovação
8	Integrações PAM com alvos (targets)	Integração	25	AD, servidores Windows/Linux, DBs, dispositivos de rede, aplicações críticas, nuvem, SD-WAN
9	Alertas de uso anômalo de privilégio	Alerta/mês	220	Cerca de 0,15% das sessões e operações privilegiadas gerando alertas de risco
10	Relatórios de auditoria de privilégios	Relatório /mês	60	Relatórios por sistema, unidade, tipo de conta, prestador, incidente e período

7.10.6.2 Memória de cálculo (estimativa)

7.10.6.2.1 Contas privilegiadas gerenciadas (650)

- Administradores de domínio e infraestrutura central: ~50
- Administradores de servidores (Windows e Linux): ~180
- Administradores de bancos de dados: ~60
- Administradores de dispositivos de rede / segurança (firewall, balanceadores, SD-WAN etc.): ~80
- Contas privilegiadas de aplicações críticas e serviços: ~200
- Contas técnicas de automação e integração de alto privilégio: ~80
- Total aproximado: 650 contas privilegiadas.

7.10.6.2.2 Credenciais/cofre (1.300)

- Considerando que cada conta privilegiada pode possuir, em média, duas credenciais relevantes (senha principal + chave/API ou outro segredo técnico): 650 × 2 = 1.300 credenciais a serem cofretadas.

7.10.6.2.3 Sessões privilegiadas monitoradas/gravadas (1.500/mês)

- Estimativa de volume de sessões administrativas mensais, levando em conta manutenção rotineira, atualizações, intervenções em incidentes, deploys e ajustes de configuração em ambiente híbrido, resultando em aproximadamente 1.500 sessões/mês, todas passíveis de monitoramento e gravação.

7.10.6.2.4 Rotação automática de senhas (650/mês)

- Para garantir postura de segurança adequada, assume-se rotações mensais das senhas de todas as contas privilegiadas, resultando em 650 eventos/mês. Esse valor permite, se desejado, reduzir a periodicidade para determinados tipos de conta (por exemplo, semanal para contas mais sensíveis), mantendo ainda folga operacional.

7.10.6.2.5 Acessos emergenciais (180/mês)

- Considerando o porte e a criticidade dos sistemas, assume-se média de 6 acessos emergenciais (break-glass) por dia em ativos críticos (servidores de produção, dispositivos de rede, bancos de dados sensíveis), o que resulta em: 6 × 30 ≈ 180 eventos/mês.

7.10.6.2.6 Alertas de uso anômalo de privilégio (220/mês)

- Com base no total de sessões privilegiadas (1.500/mês) e na expectativa de que uma fração reduzida apresente comportamentos atípicos (comandos fora do padrão, horários anômalos, alvos incomuns etc.), considera-se que cerca de 0,15% a 0,2% das operações privilegiadas gere alertas: 1.500 × 0,15 ≈ 225 → arredondado para 220 alertas/mês.

7.10.6.2.7 Os demais quantitativos (workflows, integrações, relatórios) foram dimensionados de modo conservador, assegurando capacidade para cobrir a complexidade da infraestrutura do MinC, a segmentação por unidades organizacionais e a necessidade de visão detalhada em auditorias.

7.10.7 AUDITORIA E GOVERNANÇA DE DADOS

7.10.7.1 No contexto da contratação presente, os serviços de auditoria e governança de dados serão integrados de maneira transversal à arquitetura tecnológica do MinC, garantindo visibilidade dos fluxos de dados, identificação precoce de anomalias, acompanhamento de acessos privilegiados e conformidade permanente com a LGPD e com normas internas de segurança da informação.

7.10.8 DEFESA CONTRA RANSOMWARE E AMEAÇAS AVANÇADAS

7.10.8.1 A solução de Defesa contra Ransomware e Ameaças Avançadas deverá operar de forma integrada ao ambiente de TIC do Ministério da Cultura, cobrindo todos os ativos classificados como críticos ou essenciais para a continuidade das políticas públicas culturais.

7.10.8.2 Os quantitativos mínimos estimados a seguir foram dimensionados com base no porte institucional do MinC, considerando sua atuação nacional; no volume de eventos de segurança projetado (EPS); na quantidade de usuários, dispositivos, servidores e serviços expostos; em referências de órgãos da APF que já sofreram ou mitigaram ataques de ransomware.

Item	Componente	Unidade	Quantitativo	Fundamentação
1	Endpoints protegidos	Dispositivo	2.800	Cobertura de estações, servidores, VMs, dispositivos remotos e ativos críticos
2	Bloqueios anti-criptografia	Evento/mês	600	Média projetada para órgão da APF de porte similar, com margem para picos de ataque
3	Deteções comportamentais	Detecção/mês	1.200	Derivado do volume de 5.200 EPS, considerando eventos relevantes e suspeitos
4	Tentativas de C2 bloqueadas	Conexões/mês	900	Combinação de métricas GovBR com perfil do setor cultural e uso intensivo de mídia
5		Evento/mês	150	

	Isolamento automático de dispositivos			Projeção de 1 isolamento para cada incidente de maior criticidade
6	Restaurações /rollback	Evento/mês	100	Ataques que chegam a alterar arquivos, considerando faixa de 70–120 casos potenciais
7	Playbooks anti-ransomware e APT	Playbook	18	Ransomware, APT, exfiltração, zero-day, lateral movement e cenários correlatos

7.10.8.3 Memória de cálculo (estimativa)

7.10.8.3.1 Endpoints protegidos – 2.800, sendo

- Servidores e VMs: 420
- Estações internas (unidades do MinC e vinculadas): 1.900
- Usuários remotos (teletrabalho, viagens, representações): 350
- Ambientes auxiliares + dispositivos críticos (equipamentos específicos, appliances, terminais especiais): 130
- Total projetado: 2.800 dispositivos a serem protegidos de forma contínua.

7.10.8.3.2 Bloqueios anti-criptografia – 600 eventos/mês

- Considera-se base de 150 incidentes mensais em diferentes níveis de gravidade (conforme item de IR/ESM);
- Estima-se que cada incidente relevante gere, em média, 4 eventos primários de tentativa de criptografia ou ações diretamente associadas;
- 150 × 4 = 600 eventos/mês.

7.10.8.3.3 Deteções comportamentais – 1.200/mês

- Volume global estimado: 5.200 EPS (events per second) para o ambiente do MinC;
- Aplicando-se recorte de 15% de eventos relevantes → ~780;
- Acrescendo-se 40% de margem para eventos anômalos adicionais (campanhas sazonais, picos, novas ameaças) → ~1.200, valor adotado como capacidade mínima.

7.10.8.3.4 Tentativas de C2 bloqueadas – 900 conexões/mês

- Referência em órgão médio da APF: ~600 tentativas de conexões C2/mês;
- Considerando o perfil do setor cultural (uso intenso de mídias, downloads, compartilhamento de arquivos, acessos distribuídos): acréscimo de ~300 tentativas/mês;
- Total projetado: 900 conexões C2 bloqueadas/mês.

7.10.8.3.5 Isolamento automático de dispositivos – 150 eventos/mês

- Considerando 150 incidentes relevantes/mês, projeta-se que, em cenários de maior criticidade, cada incidente possa demandar ao menos um isolamento automático de dispositivo;
- Adota-se, portanto, a capacidade mínima de 150 eventos/mês de isolamento automático, garantindo margem adequada para atuação tempestiva.

7.10.8.3.6 Restaurações/rollback – 100 eventos/mês

- Observando a literatura e experiências de órgãos públicos, estima-se que entre 70 e 120 eventos mensais possam demandar rollback ou restauração seletiva de arquivos/sistemas;
- Adota-se o valor intermediário de 100 eventos/mês, como capacidade mínima a ser suportada pela solução.

7.10.8.3.7 Playbooks anti-ransomware e APT – 18. Composição dos fluxos automatizados mínimos:

- Cenários de ransomware (criptografia direta, ataque em massa, ataque segmentado): 5 playbooks;
- Cenários de APT (persistência prolongada, escalonamento, espionagem): 5 playbooks;
- Cenários de exfiltração de dados: 3 playbooks;
- Cenários de vulnerabilidades zero-day: 2 playbooks;
- Cenários de movimentação lateral/comprometimento de domínio: 3 playbooks.
- Total: 18 playbooks como capacidade inicial mínima, com possibilidade de expansão.

7.10.9 ESM/ITSM - GESTÃO DE SERVIÇOS COM FERRAMENTA DE ESM/ITSM E CENTRAL DE SERVIÇOS

7.10.9.1 O Ministério da Cultura – MinC possui um ambiente de Tecnologia da Informação e Comunicação (TIC) composto por múltiplos serviços, sistemas, ativos e usuários, cuja complexidade demanda a adoção de modelo estruturado de Gestão de Serviços de TIC, suportado por ferramenta ESM/ITSM e Central de Serviços, de forma a assegurar a continuidade, a qualidade, a rastreabilidade e a padronização do atendimento aos usuários.

7.10.9.2 A ausência de gestão integrada dos serviços impacta diretamente os níveis de serviço, a capacidade de atendimento, a governança e a tomada de decisão, tornando necessária a contratação de solução que permita o gerenciamento centralizado dos serviços de TIC, conforme boas práticas consolidadas no mercado.

7.10.9.3 A tabela a seguir possui informações relevantes sobre os ambientes de TIC do MinC.

Solução	Quantidade
Balanceamento de Carga	02 (dois) - 01 ativo e 01 passivo
Web Application Firewall – WAF	01
Solução de Mail Gateway	01 – Microsoft 365
Solução de VMS – Virtual Machine Security	01 – Hyper-V
Solução de DNS (open source ou proprietário)	02
Solução de SMTP (open source ou proprietário)	01
Solução AD/DNS/DHCP	02 AD-DNS -02 DHCP
Solução de 2º Fator de Autenticação	01 SMS
Link de Internet	02
Switches Core	02
Switches SAN	02

Switches TOR/Distribuição	04
Switches de Acesso	55
Access Point	65
Dispositivos de Armazenamento (storage)	04
Versões de Sistemas Operacionais	11
VPNs	265
VOIP	1.300 ramais
Impressoras	44
CFTV	01

7.10.9.4 A tabela seguinte demonstra a quantidade de dispositivos distribuídos para os usuários do MinC.

Desktops/Computadores de Mesa	Notebooks	Total
1.101	82	1.183

7.10.9.5 A respeito dos servidores, verificou-se que atualmente o Ministério da Cultura possui sete (07) Servidores físicos. Destes, quatro (04) compõem um (01) cluster que virtualiza um total de trezentos e dez (310) servidores virtuais.

7.10.9.6 As características dos servidores estão descritas abaixo:

CARACTERÍSTICAS DOS SERVIDORES FÍSICOS				
Modelo	S.O.	Socket	Cores	Total Cores
DELL Power Edge R940	Datacenter	4	24	96
DELL Power Edge R940	Datacenter	4	24	96
DELL Power Edge R940	Datacenter	4	24	96
DELL Power Edge R940	Datacenter	4	24	96

DELL Power Edge R720	Standard	2	8	16
DELL Power Edge R710	Standard	2	4	8
DELL Power Edge R710	Standard	2	4	16
TOTAL DE CORES				416

7.10.9.7 Com relação à previsão de crescimento dos ambientes de TIC, tem-se a tabela seguinte:

EQUIPAMENTOS EM PRODUÇÃO	QUANT.	PREVISÃO DE CRESCIMENTO		QUANTIDADE DE RECURSOS
		AÇÃO	ADICIONAL	
Estação de trabalho tipo desktop	1.101	Aquisição de novas estações de trabalho do tipo desktop durante o exercício corrente e o próximo exercício (2025) para a complementação dos postos de trabalho dos escritórios estaduais e do edifício sede e anexo.	300	1.401
Estação de trabalho do tipo notebook	82	Aquisição de novas estações de trabalho do tipo notebook durante o exercício corrente e o próximo exercício (2025) para a complementação dos postos de trabalho dos escritórios estaduais e do edifício sede e anexo.	80	162
TOTAL	1.183	TOTAL PREVISTO		1.563

7.10.9.8 Ainda, para o correto dimensionamento da proposta, a tabela abaixo evidencia a previsão de crescimento dos ambientes de TIC dos usuários:

QUANTIDADE ATUAL DE USUÁRIOS	PREVISÃO DE CRESCIMENTO		TOTAL NO FINAL DO 1º SEMESTRE DE 2025
	AÇÃO	ADICIONAL	
	PROCESSO SELETIVO SIMPLIFICADO PARA CONTRATAÇÃO TEMPORÁRIA		

1.253	EDITAL PSS/MINC Nº 1, DE 13 DE MAIO DE 2024. PROCESSO SEI/MinC Nº 01400.011599/2024-42	200	1.453

7.10.9.9 A solução proposta consiste na implantação, operação e sustentação de ferramenta ESM/ITSM integrada à Central de Serviços, contemplando, no mínimo, os seguintes processos:

- Gerenciamento de Incidentes;
- Gerenciamento de Requisições de Serviço;
- Gerenciamento de Problemas;
- Gerenciamento de Mudanças;
- Gerenciamento de Ativos e Configurações (CMDB);
- Gerenciamento de Níveis de Serviço (SLAs e OLAs);
- Gerenciamento de Conhecimento;
- Monitoramento, geração de relatórios e indicadores de desempenho.

7.10.9.10 As informações detalhadas sobre o parque tecnológico e a previsão de crescimento dos ambientes de TIC são apresentadas neste ETP exclusivamente para subsidiar o dimensionamento da Gestão de Serviços, não se caracterizando como contratação direta de serviços de sustentação ou operação da infraestrutura.

7.10.10 ANÁLISE CONTÍNUA DE VULNERABILIDADES

7.10.10.1 A análise contínua permitirá identificar vulnerabilidades críticas, mensurar o nível de maturidade cibernética, revisar políticas e procedimentos internos, e propor medidas corretivas e evolutivas que fortaleçam a governança digital e reduzam a exposição institucional a riscos operacionais e reputacionais. O resultado esperado é um roadmap resiliência digital da instituição.

7.10.10.2 Diagnóstico técnico estratégico dos controles de segurança críticos do Ministério da Cultura, com vistas ao fortalecimento da governança digital e à mitigação de riscos cibernéticos.

Descrição	Unidade	Quantidade estimada
Levantamento e diagnóstico: entrevistas com áreas internas, mapeamento de ativos, análise documental e definição de escopo;	HST	200
Análise de vulnerabilidades (6 UST): contempla ciclos de varredura autenticada, análise de resultados, priorização e classificação CVSS;	HST	200
Revisão de políticas (30 HST): avaliação de aderência normativa, mapeamento de , recomendações e atualização preliminar;gaps	HST	200
Relatórios (10 PF): cada PF representa a entrega de componentes documentais (relatório técnico, executivo, painéis e matrizes);	HST	200
Workshops (10 HST): realização de capacitação técnica e		

transferência de conhecimento	HST	200
TOTAL	HST	1000

7.10.11 RESPOSTA A INCIDENTES E FORENSE DIGITAL

7.10.11 .1 Tabela de projeção de quantitativos:

Item	Componente	Unidade	QTD	Fundamentação
1	Incidentes tratáveis por mês	Caso/mês	150	Correlação ESM + histórico APF + criticidade
2	Coletas forenses de disco	Coleta	40/mês	Média de casos por porte institucional
3	Coletas forenses de memória	Coleta	65/mês	Ameaças baseadas em processos voláteis
4	Linha do tempo forense	Timeline	150/mês	Igual ao número de incidentes
5	Playbooks específicos de IR	Playbook	36	Incidentes críticos + regulares
6	Evidências preservadas	Evidência/mês	1.200	Logs, dumps, arquivos, metadados
7	Ambientes cobertos	Ambiente	12	On-prem, nuvem, edge, SD-WAN e remoto

7.10.11.2 Memória de cálculo (estimativa):

7.10.11.2.1 Incidentes tratáveis/mês (150), coerente com:

- ESM: 150 incidentes
- Vulnerabilidades: 80
- Auditoria: 70
- IAM: 20 (incidentes podem ser correlacionados → média 150)

7.10.11.2.2 Coletas forenses de disco (40/mês)

- A cada 3–4 incidentes críticos → 1 coleta de disco
- 150 incidentes/mês × 10% críticos ≈ 15
- rotinas de deep inspection = 40

7.10.11.2.3 Coletas forenses de memória (65/mês). Ataques modernos dependem de:

- fileless malware
- execução em RAM
- malware modular
- técnicas anti-forense

- Estimativa: 40–70 → fixado em 65

7.10.11.2.4 Timelines (150)

- 1 timeline por incidente → 150.

7.10.11.2.5 Playbooks (36)

- Ransomware: 6
- Phishing: 4
- Privileged escalation: 5
- Data breach: 6
- Exfiltração: 3
- Ataques à superfície externa: 4
- Anomalias internas: 8

7.10.11.2.6 Evidências/mês (1.200). Composição:

- logs: 750
- dumps: 150
- arquivos extraídos: 200
- metadados e correlatos: 100

7.10.12 DETECÇÃO E RESPOSTAS A INCIDENTES

7.10.12.1 A solução de TIC consiste em de segurança da informação. contratação de solução para realizar detecção, análise, resposta e monitoramento de incidentes;

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE
1	Solução de monitoramento de comportamento anômalo da rede, detecção, análise e resposta de incidentes de segurança da informação.	UN	1
2	Serviço de Implantação	UN	1

7.10.13 DATA LAKE - BIG DATA

7.10.13.1 Plataforma de Big Data Corporativa – 1

a) Infraestrutura para processamento distribuído de grandes volumes de dados em escala, com suporte a múltiplos casos de uso (data Warehouse, machine learning, analytics em tempo real e ingestão de dados). Deve incluir cluster gerenciado baseado em ecossistema Hadoop com HDFS, YARN, Apache Ozone, HBase, Phoenix, Solr, Hive, Tez e Kafka, garantindo segurança através de autenticação integrada (RBAC/ABAC), criptografia de dados em trânsito e repouso, trilhas de auditoria e políticas centralizadas de conformidade, além de alta disponibilidade com expansão horizontal, replicação de dados e auto recuperação de processos em caso de falhas.

7.10.13.2 Plataforma de Gestão e Governança de Dados – 1

a) Infraestrutura para integração, virtualização, controle de qualidade e governança centralizada dos dados corporativos, compatível com múltiplas fontes e permitindo acesso unificado e seguro aos dados. A solução deve atender arquitetura 64 bits com instalação local, certificações de segurança (ISO/IEC 27001:2022 e 27002:2022, Marco Civil da Internet e LGPD), interface gráfica multiplataforma (Windows, Linux, MacOS) sem dependência de Java /Flash, suporte em português ou inglês, CLI para administração e perfis de usuários não técnicos com interface responsiva. Deve possuir conectores nativos para SGBDs relacionais (Oracle, SQL Server, PostgreSQL, MySQL /MariaDB) e NoSQL (MongoDB, Cassandra, Elasticsearch), Big Data (Hive, Spark, Presto, Databricks, Trino, ClickHouse), APIs (REST, SOAP, ODATA), arquivos (XML, JSON, CSV, Excel, Parquet, Avro, ORC), middleware de mensageria (Kafka) e serviços de nuvem (AWS, Azure, GCP, Snowflake). A plataforma deve incluir controle de

acesso granular (RBAC, ABAC), integração com Active Directory/LDAP, criptografia TLS 1.3 com autenticação mútua (OAuth2 e SAML2), mascaramento dinâmico de dados com replicação ou persistência intermediária, logs detalhados de auditoria, catálogo de dados com busca avançada, exportação em formatos diversos, integração com IA Generativa para descrição automática de campos em linguagem natural (português e inglês), e perfis de dados (data profiling) com regras de qualidade para validação e enriquecimento.

7.10.13.3 Plataforma de Desenvolvimento Analítico e de ML/IA – 1

a) Infraestrutura para cobrir o ciclo de vida de desenvolvimento de projetos de dados, machine learning e IA Generativa, com abordagens no-code, low-code e full-code em ambiente unificado e governado. A solução deve ser acessível via navegador com arquitetura modular, escalável e autocontida, suportando multiprocessamento, alta disponibilidade e APIs para Design, Automação e Governança. Deve permitir conexão a dados em nuvem pública, privada e on-premises com conectores nativos para SQL, NoSQL, Big Data e SaaS, processamento de múltiplos formatos (CSV, Excel, Parquet, JSON etc.), transformações visuais e scripts Python customizados. A plataforma deve incluir AutoML com algoritmos supervisionados e não supervisionados (regressão, árvores de decisão, SVM, random forest, XGBoost, redes neurais, k-means, DBSCAN, isolation forest), técnicas de ensemble, otimização avançada e execução distribuída em Kubernetes. Deve oferecer IA Generativa com suporte a múltiplas LLMs de mercado e auto hospedadas, gateway de API para governança, criação de agentes de IA com suporte no-code e full-code, observabilidade, controles de ética e segurança (detecção de PII, toxicidade, jailbreak), integração com vector stores (FAISS, Pinecone, Qdrant, Elasticsearch) e aceleração nativa Q&A com RAG sobre bases documentais corporativas.

7.10.13.4 Serviços Técnicos Especializados (Serviços Profissionais Gerenciados) – 20.000 (HST)

a) Visa apoiar todas as fases do ciclo de vida do pipeline de dados, desde o planejamento estratégico até a sustentação operacional, assegurando a correta implementação das plataformas, transferência de conhecimento e manutenção de ambientes críticos em SLA 24x7. Os serviços devem incluir: Planejamento e Arquitetura com levantamento de requisitos técnicos e de negócio, definição de arquiteturas de referência e modelos de governança de dados, estudos de viabilidade, sizing e capacity planning; Implantação e Configuração com instalação e configuração de plataformas de Big Data, Governança de Dados e IA/ML, criação de ambientes de desenvolvimento, homologação e produção, integração entre sistemas legados, APIs, fontes de dados estruturadas e não estruturadas; Migração e Modernização com migração de dados entre ambientes on-premises, nuvem privada ou híbrida, modernização de pipelines legados incluindo reengenharia e adequação a padrões abertos, movimentação de grandes volumes de dados com garantia de integridade e continuidade operacional; Sustentação e Operação Assistida com monitoramento 24x7 com ferramentas de telemetria e alertas, suporte em múltiplos níveis (L1, L2 e L3), operação assistida com transferência gradual de conhecimento, aplicação de patches, correções de segurança e atualizações contínuas; Tuning e Otimização com ajuste de performance em clusters de Big Data, virtualização de dados e ambientes analíticos.

7.10.14 HIPERCONVERGÊNCIA

7.10.14.1 ARMAZENAMENTO - DEMANDA DE PRESERVAÇÃO DO ACERVO AUDIOVISUAL DO CTAV

7.10.14.1.1 Para o desenho da solução a ser adquirida foi realizado o levantamento da demanda de preservação de mídia do CTAv:

7.10.14.1.2 Foi levantada a demanda de preservação de mídias audiovisuais do CTAv por meio do ofício nº 245/2024 /CGCTAV/DFIA/SAV/GM/MinC, processo SEI no. 01400.023247/2024-30.

7.10.14.1.3 Nesse serviço está prevista a continuidade do processo de migração do acervo iniciada com o atendimento parcial da demanda no ambiente de armazenamento do virtualizador Hitachi Vantara existente. Conforme informado no ofício supracitado o acervo audiovisual é composto por 390 discos magnéticos externos, muitos deles com mais de 10 anos de vida e que precisam ser migrados, totalizando cerca de 780TB de mídias digitais e aproximadamente 7200 mídias magnéticas obsoletas estimadas em 722TB, totalizando 1.502 TB de arquivos históricos culturais a serem preservados.

7.10.14.1.4 Para esta demanda a solução deve prover recursos adicionais para, somada à capacidade já acumulada, atender a demanda de preservação de títulos e obras históricas.

ACERVO JÁ DIGITALIZADO		ACERVO a DIGITALIZAR	NECESSIDADE TOTAL
Acervo protegido no Ambiente Virtualizado	Armazenamento necessário para Acervos já Digitalizados	Acervo em mídias a digitalizar	Armazenamento total necessário
160 TB	620TB	722 TB	**1.342 TB**

7.10.14.2 BALANCEADOR DE CARGAS

7.10.14.2.1 A solução atual F5 do MinC, com relação as licenças estas se encontram sem suporte e atualização e o appliance físico se encontra defasado e sem atualizações

7.10.14.2.2 Esta solução F5 utiliza no ambiente do MinC o balanceamento de carga, o qual direciona e controla o tráfego da Internet entre os servidores de aplicações e seus visitantes ou clientes. Como resultado, ele melhora a disponibilidade, a escalabilidade, a segurança e a performance de uma aplicação. A solução F5 é utilizada hoje como uma importante ferramenta de sustentação no funcionamento dos sistemas do Ministério da Cultura (MinC), isto por desempenhar um papel de balanceamento de carga nas solicitações de acesso.

7.11 MODELO DE MENSURAÇÃO DE RESULTADOS (IMR) DOS SERVIÇOS

7.11.1 A execução contratual será orientada por Instrumento de Medição de Resultados (IMR), baseado em indicadores objetivos de desempenho, com vistas à aferição da qualidade dos serviços prestados.

7.11.2 Serão adotados, no mínimo, os seguintes indicadores:

7.11.2.1 Disponibilidade dos Serviços

- Meta: 99,5%
- Medição: monitoramento contínuo
- Penalidade: aplicação de glosa proporcional

7.11.2.2 Tempo de Resposta a Incidentes (MTTR)

- Meta: conforme criticidade (ex: até 2h para incidentes críticos)
- Medição: registros do sistema de chamados
- Penalidade: desconto por descumprimento

7.11.2.3 Tempo de Detecção de Incidentes (MTTD)

- Meta: redução progressiva conforme maturidade do serviço
- Medição: logs e relatórios do SOC/SIEM

7.11.2.4 Conformidade de Segurança

- Meta: 100% dos ativos monitorados e avaliados
- Medição: relatórios de vulnerabilidade

7.11.2.5 Satisfação do Usuário

- Meta: 85%
- Medição: pesquisas periódicas

7.11.3 O não atingimento das metas poderá ensejar:

- aplicação de glosas financeiras;
- abertura de plano de ação corretivo;
- eventual penalização contratual.

7.11.4 O detalhamento completo dos indicadores será consolidado no Termo de Referência.

8. Levantamento de soluções

8.1. A análise comparativa de soluções, nos termos do inc. II do art. 11 da IN-94/2022 – SGD/ME, visa 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.

8.1.1. Solução A: Contratação de empresa privada para provimentos dos serviços.

8.1.2. Solução B: Contratação de empresa pública para provimento dos serviços.

8.1.2.1 Projetos similares no âmbito da Administração Pública:

Solução	Órgão	N° Pregão /Contrato	Objeto
Solução B	Ministério do Trabalho e Emprego (MTE)	Contrato nº 20 /2024	Contratação de solução de tecnologia da informação e comunicação para execução de serviços técnicos especializados de tecnologia da informação e comunicações - TIC, buscando atendimento das necessidades do Ministério do Trabalho e Emprego (MTE).
Solução B	Ministério da Gestão e da Inovação em Serviços Públicos (MGI)	Contrato nº 69 /2023	Contratação de solução de tecnologia da informação e comunicação para atender às necessidades do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) e órgãos que compartilham serviços por meio da Portaria MGI no 43, de 31 de janeiro de 2023.
Solução B	Ministério da Economia (ME)	Contrato nº 65 /2021	Contratação de serviços para a prestação de serviços estratégicos de Tecnologia da Informação e Comunicação - TIC voltados, direta ou indiretamente, ao suporte necessário para a produção de soluções estruturantes de Governo e departamentais, que atendem as unidades do Ministério da Economia, em todo o território nacional. Tais serviços consistem na produção de soluções, desenvolvimento e manutenção de sistemas, serviços de infraestrutura, consultoria técnica, entre outros serviços técnicos, que serão prestados nas condições estabelecidas no Projeto Básico.
Solução	Ministério do Trabalho	Contrato	Contratação de serviços de conectividade de dados para prestação de serviços de telecomunicações de longa distância (WAN – Wide Area Network), com capacidade para prover tráfego de dados, voz e imagem entre as unidades do TEM, em todo

B	e Emprego (MTE)	nº 18 /2024	território nacional, via serviço de Internet com SD-WAN e INTERNET-IP, incluindo o fornecimento, configuração e gerência de roteadores, nas condições estabelecidas no Termo de Referência.
Solução B	DNIT	Contrato nº 604 /23-00	Serviço de Comunicação de dados com fornecimento de links de internet dedicada + SDWAN, incluindo o gerenciamento desta solução e gerência de nível de serviço – GNS
Solução B	Ministério da Educação - MEC	Contrato nº 17 /2025	Contratação de Serviços Técnicos Especializados em Tecnologia da Informação e Comunicação (TIC) sob demanda, para atender às necessidades do Ministério da Educação, nos termos da tabela abaixo, para o período de 60 meses, nas condições estabelecidas no Termo de Referência

9. Análise comparativa de soluções

9.1. A análise comparativa de soluções, nos termos do inc. II do art. 11 da IN SGD/ME Nº 94, de 23 de dezembro de 2022 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.

9.2. A solução para a demanda não foi encontrada nos Catálogos de Soluções de TIC com condições padrões definidos pelo Órgão Central do SISP e também não foi encontrada no Portal do Software Público.

9.3. Para a realização de análise comparativa entre as soluções, considerando aquelas foram levantadas neste estudo, foram consideradas as seguintes soluções:

9.3.1. Solução A – Contratação de empresa privada para provimento dos serviços

9.3.1.1. A possibilidade de contratação de uma empresa privada, por meio de licitação (como o Pregão Eletrônico), para a prestação de serviços especializados de Tecnologia da Informação e Comunicação (TIC) ao Ministério da Cultura apresenta limitações técnicas significativas, que inviabilizam essa alternativa. Isso se deve à natureza específica e estratégica dos serviços demandados, os quais exigem conhecimento aprofundado sobre os sistemas, as políticas públicas culturais e as peculiaridades operacionais do MinC — características que dificilmente são encontradas em soluções padronizadas do mercado.

9.3.1.2. A experiência acumulada e o domínio técnico sobre os processos e dados institucionais fazem com que a prestação desses serviços por empresas públicas seja a solução mais adequada. Esses serviços possuem caráter essencial ao funcionamento do Ministério, estando vinculados a sistemas que tratam informações sensíveis, relacionadas à formulação, execução, monitoramento e avaliação de políticas públicas culturais. A entrega à iniciativa privada de serviços dessa natureza pode comprometer a segurança, a soberania e a continuidade operacional das ações estratégicas do MinC.

9.3.1.3. Além disso, empresas públicas com atuação na área de TIC oferecem maior resiliência diante de restrições orçamentárias e maior aderência às diretrizes governamentais de governança digital. Também se destacam por sua capacidade de atuar como parceiras estratégicas do Estado, com equipes técnicas que acumulam conhecimento específico sobre o funcionamento da Administração Pública, especialmente no que se refere à gestão cultural.

9.3.1.4. Embora alguns componentes da solução estejam alinhados a padrões de mercado — como linguagens de programação, licenciamento de software e infraestrutura tecnológica — a complexidade e a sensibilidade envolvidas exigem mais do que a simples execução técnica: demandam o envolvimento de instituições que compartilhem os valores, os objetivos e o compromisso institucional com as políticas culturais do país.

9.3.1.5. Dessa forma, justifica-se a inviabilidade da contratação de empresa privada para esta finalidade, sendo recomendada a celebração de parceria com empresa pública especializada, capaz de atender, com segurança e alinhamento estratégico, às necessidades do Ministério da Cultura.

9.3.1.6 Vantagens:

- Potencial para inovação rápida e acesso a tecnologias de ponta.
- As empresas privadas possuem metodologias e ferramentas de gerenciamento de projetos que permitem acompanhar o progresso das atividades e identificar possíveis desvios.
- As empresas privadas podem otimizar o uso de recursos, como equipamentos e softwares.
- As empresas privadas estão constantemente buscando novas tecnologias e soluções inovadoras, o que pode impulsionar a transformação digital no MinC.

9.3.1.7 Desafios:

- Riscos significativos em termos de segurança de dados, continuidade dos serviços e alinhamento com objetivos governamentais.
- Garantir que a empresa contratada disponha de medidas de segurança robustas para proteger os dados sensíveis do Ministério.
- Ataques cibernéticos, como ransomware e invasões, podem comprometer a segurança da informação e a disponibilidade dos sistemas.
- Dependência do cumprimento do contrato pela empresa privada contratada, o que pode gerar vulnerabilidades caso ocorram problemas na prestação dos serviços.
- Alterações nas necessidades da instituição podem exigir negociações e adaptações contratuais, o que pode gerar atrasos e custos adicionais.
- O Ministério pode enfrentar dificuldades para acompanhar de perto as atividades da empresa contratada, especialmente se não possuir os conhecimentos técnicos necessários.
- A falta de transparência na prestação dos serviços pode dificultar a avaliação do desempenho da empresa e a identificação de problemas.
- Termos contratuais ambíguos ou incompletos podem gerar divergências entre as partes e dificultar a resolução de conflitos.
- A alta rotatividade de pessoal nas empresas prestadoras de serviços pode comprometer a qualidade do atendimento e a continuidade do conhecimento.
- A falta de qualificação dos profissionais pode dificultar a resolução de problemas complexos e a implementação de novas soluções.
- As empresas contratadas devem cumprir as normas e legislações aplicáveis, o que exige um acompanhamento constante por parte do Ministério.
- Empresas privadas visam o lucro e podem priorizar seus interesses financeiros sobre os interesses do governo. Isso pode levar a conflitos de interesse e decisões que não são necessariamente as melhores para o setor público.
- Empresas privadas podem enfrentar dificuldades financeiras ou optar por sair do mercado de TI. Isso pode resultar em interrupções nos serviços e projetos governamentais.
- Contratar empresas privadas pode limitar o controle direto do governo sobre projetos de TI e a capacidade de realizar mudanças ou ajustes conforme necessários, sem custos adicionais significativos.
- Os contratos com empresas privadas podem ser complexos e envolver disputas contratuais que podem levar a atrasos e custos adicionais.
- Empresas privadas podem não ter a mesma compreensão dos objetivos e políticas governamentais, o que pode dificultar a realização dos objetivos do governo.
- Contratar empresas privadas pode levantar questões de conflito de interesses, especialmente quando essas empresas têm relações comerciais com outros setores do governo.

9.3.2. Solução B – Contratação de empresa pública para provimento dos serviços

9.3.2.1. A contratação de empresa pública para o provimento dos serviços de Tecnologia da Informação e Comunicação (TIC) mostra-se a alternativa mais aderente às necessidades institucionais do Ministério da Cultura, considerando o caráter estratégico e finalístico das soluções envolvidas.

9.3.2.2. No âmbito das políticas públicas culturais, os sistemas e serviços de TIC processam e armazenam dados sensíveis e informações de relevância social, histórica e identitária, que demandam especial atenção quanto à segurança, à confidencialidade e à integridade. Por essa razão, é recomendável que tais serviços sejam executados por empresas públicas especializadas, cuja missão institucional contempla, entre outras atribuições, a guarda e a gestão de informações governamentais.

9.3.2.3. A contratação de empresa pública proporciona maior aderência aos princípios da Administração Pública, especialmente no que diz respeito à soberania sobre os dados, à continuidade dos serviços e à gestão do conhecimento acumulado das regras de negócio específicas do setor cultural. Tais empresas possuem equipes técnicas experientes, com domínio sobre os sistemas governamentais, e demonstram maior capacidade de adaptação às constantes mudanças regulatórias, orçamentárias e tecnológicas impostas ao setor público.

9.3.2.4. Outro fator relevante é a resiliência institucional das empresas públicas diante de eventuais contingências orçamentárias, o que garante maior estabilidade e continuidade na execução das políticas culturais, mesmo em contextos adversos. Além disso, os serviços contratados envolvem operação continuada e estratégica, com forte vínculo com a missão finalística do MinC, o que reforça a necessidade de um parceiro que compartilhe valores e objetivos institucionais.

9.3.2.5. Assim, a prestação dos serviços por empresa pública é a alternativa que melhor atende aos requisitos de segurança, continuidade, eficiência e alinhamento estratégico com as diretrizes do Ministério da Cultura.

9.3.2.6. Vantagens:

- Empresas públicas são criadas com o objetivo de atender aos interesses públicos e promover o desenvolvimento social e econômico do país. Isso garante um alinhamento natural com as políticas e diretrizes do Ministério da Cultura.
- Empresas públicas são altamente comprometidas com a segurança dos dados governamentais e têm ampla experiência em proteger informações sensíveis. Isso é crucial para garantir a integridade e a confidencialidade dos dados do governo.
- As empresas públicas têm uma longa história de atuação na área de TI, com equipes altamente qualificadas e experientes. Isso as torna capazes de lidar com os desafios complexos que surgem em projetos governamentais de grande escala.
- Empresas públicas têm a vantagem de oferecer maior estabilidade e continuidade em contratos de longo prazo, minimizando riscos de interrupções nos serviços de TI, o que pode ser crucial para o funcionamento do governo.
- As decisões e ações das empresas públicas são guiadas pelo interesse público, o que pode resultar em soluções mais adequadas às necessidades da educação brasileira.
- Empresas públicas possuem ampla experiência em projetos governamentais, compreendendo as especificidades e complexidades do setor público.
- Empresas públicas estão familiarizadas com as normas e regulamentos que regem as contratações públicas, agilizando os processos e reduzindo o risco de irregularidades.
- Ao contratar empresas públicas, o governo incentiva o desenvolvimento da indústria tecnológica nacional, gerando empregos e promovendo a inovação.
- As empresas públicas podem atuar como agentes de transferência de tecnologia, promovendo a disseminação de conhecimento e o desenvolvimento de soluções tecnológicas específicas para o setor educacional.
- Empresas públicas têm maior facilidade de integração com outros órgãos públicos, o que facilita a troca de informações e a cooperação em projetos.
- A possibilidade de compartilhar infraestrutura e recursos com outros órgãos públicos pode gerar economias de escala e otimizar os investimentos.
- Empresas públicas podem desenvolver soluções tecnológicas personalizadas para atender às necessidades específicas do Ministério da Cultura.

9.3.2.7. Desafios:

- Riscos significativos em termos de segurança de dados, continuidade dos serviços e alinhamento com objetivos governamentais.
- As empresas públicas, por estarem sujeitas a um maior controle e fiscalização, tendem a ter processos mais burocráticos e lentos, o que pode atrasar a implementação de projetos e soluções.
- As empresas públicas podem estar sujeitas a interferências políticas, o que pode comprometer a imparcialidade na tomada de decisões e a qualidade dos serviços

9.4 Comparativo Qualitativo

9.4.1. O quadro comparativo a seguir apresenta a capacidade de atendimento de cada um dos cenários examinados em relação às características das necessidades da demanda.

9.4.2. As alternativas foram avaliadas em relação à sua capacidade de atendimento aos requisitos definidos para a solução, conforme o quadro a seguir:

REQUISITOS		**CENÁRIO**	
		SOLUÇÃO A	**SOLUÇÃO B**
Negócio	Modernização Tecnológica	Parcialmente	Atende
	Tempestividade no atendimento das necessidades	Parcialmente	Atende
	Aumento da Segurança de Dados	Parcialmente	Atende
	Integração de Sistemas	Parcialmente	Atende
	Melhoria da Eficiência Operacional	Atende	Atende
	Aprimoramento da Transparência e Prestação de Contas	Parcialmente	Atende
	Cumprimento de Requisitos Legais e Regulatórios	Atende	Atende
	Suporte à Tomada de Decisão	Atende	Atende
	Melhoria da Experiência do Usuário	Atende	Atende
	Suporte a Programas e Projetos Estratégicos	Parcialmente	Atende
Tecnológico	Atualização do Portfólio de Soluções do MinC	Parcialmente	Atende
	Atualização dos Ativos de TIC do MinC	Parcialmente	Atende
	Saneamento das Vulnerabilidades de TIC do MinC	Não Atende	Atende
	Automação dos Processos de Gestão de TIC do Minc	Parcialmente	Atende
	Disponibilidade de Ambientes de Infraestrutura Adequados para as Soluções de Missão Crítica	Não Atende	Atende
Demais Requisitos	Flexibilidade	Não Atende	Atende
	Não onerosidade	Não Atende	Atende
	Plurianualidade	Atende	Atende
	Variedade	Não Atende	Atende
	Padronização	Não Atende	Atende
	Não Duplicidade de Objetos	Atende	Atende
RESULTADO DA ANÁLISE		**Inviável**	**Viável**

10. Registro de soluções consideradas inviáveis

10.1. Conforme § 1º do art. 11 da IN SGD 94/2022, após o levantamento das possíveis soluções para a prestação dos serviços de Tecnologia da Informação e Comunicação, a Equipe de Planejamento da Contratação conclui que a Solução A – Contratação de empresa privada para provimento dos serviços é tecnicamente inviável, uma vez que não é possível atender aos requisitos necessários na sua integralidade, dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

10.2. No que concerne à análise qualitativa das alternativas possíveis, observa-se que a Solução A – Contratação de empresa privada para provimento dos serviços não atende integralmente aos seguintes requisitos:

- **Saneamento da Vulnerabilidades de TIC do MinC:** as soluções de segurança de TIC são ofertadas por diversas empresas cujas ferramentas possuem recurso ora concorrentes, ora complementares. A contratação de várias soluções para alcançar as principais vulnerabilidades é complexa e demorada, tornando impossível o saneamento dessas vulnerabilidades de forma tempestiva.
- **Disponibilização de ambientes de Infraestrutura adequados para as Soluções de Missão Crítica:** os sistemas de missão crítica do MinC exigem infraestrutura em datacenters certificados, que não são ofertados de forma regular por empresas de mercado.
- **Flexibilidade**: a relação do estado com empresas privadas, em função da ampla concorrência, não permite contratos com escopo aberto;
- **Não onerosidade**: ao contratar com o estado, as empresas privadas estabelecem uma expectativa de direito sobre os valores contratuais, gerando a obrigação na execução majoritária dos serviços;
- **Variedade**: empresas privadas são em regra especialistas, não abrangendo em seu portfólio um amplo conjunto de serviços como o requerido neste processo;
- **Padronização**: empresas privadas requerem contratos com regras específicas para cada um, inviabilizando a padronização.

11. Análise comparativa de custos (TCO)

11.1. Conforme inciso III, do art. 11, da IN 94/2022/SGD, deve-se proceder a comparação de custos totais de propriedade para as soluções técnica e funcionalmente viáveis.

11.2. Para fins de obtenção de preços utilizamos como referência os valores unitários da Proposta de Preços encaminhada ao MinC.

TCO para contratação de serviços por 36 meses.

LOTE	GRUPO	DESCRIÇÃO /GRUPO	QTDE ESTIMADA (MENSAL)	VALOR UNITÁRIO	VALOR MENSAL	VALOR TOTAL 36 MESES
	1	Conectividade	2.300	R$ 500,40	R $ 1.150.920,00	R$41.433.120,00
	2	Imageamento	1.000	R$ 424,73	R $ 424.730,00	R$15.290.280,00

Único	3	Backup-as-a-Service (BaaS)	1.000	R$ 436,87	R $ 436.870,00	R$15.727.320,00
	4	Edge Computing	2.300	R$ 505,65	R $ 1.162.995,00	R$41.867.820,00
	5	Platform-as-a-Service (PaaS)	1.750	R$ 466,38	R $ 816.165,00	R$29.381.940,00
VALOR GLOBAL ESTIMADO (36 MESES)						R$ 143.700.480,00

TCO para contratação de serviços por 36 meses.

LOTE	**GRUPO**	**DESCRIÇÃO /GRUPO**	**QTDE ESTIMADA (MENSAL)**	**VALOR UNITÁRIO**	**VALOR MENSAL**	**VALOR TOTAL 60 MESES**
Único	1	Conectividade	2.300	R$ 500,40	R $ 1.150.920,00	R$ 69.055.200,00
	2	Imageamento	1.000	R$ 424,73	R$ 424.730,00	R$ 25.483.800,00
	3	Backup-as-a-Service (BaaS)	1.000	R$ 436,87	R$ 436.870,00	R$ 26.212.200,00
	4	Edge Computing	2.300	R$ 505,65	R $ 1.162.995,00	R$ 69.779.700,00
	5	Platform-as-a-Service (PaaS)	1.750	R$ 466,38	R$ 816.165,00	R$ 48.969.900,00
VALOR GLOBAL ESTIMADO (60 MESES)						R$ 239.500.800,00

Mapa Comparativo dos Cálculos Totais de Propriedade (TCO)

11.3. Aplicando o Índice de Custo da Tecnologia da Informação (ICTI) – janeiro de 2026 acumulado nos últimos doze meses que apresenta uma variação de 2,89% ao valor estimado para as prorrogações subsequentes até o período de 60 meses:

DESCRIÇÃO DA SOLUÇÃO	**ESTIMATIVA DE TCO AO LONGO DOS ANOS**				
	Ano 1	**Ano 2**	**Ano 3**	**Ano 4**	**Ano 5**
Contratação por 36 meses	**R$ 47.900.160,00**	**R$ 49.284.474,62**	**R$ 50.708.795,93**	-	-
Contratação por 60					

meses	**R$ 47.900.160,00**	**R$ 49.284.474,62**	**R$ 50.708.795,93**	**R$ 52. 174.280,13**	**R$ 53.682.116,82**

12. Descrição da solução de TIC a ser contratada

12.1. Conforme demonstrado neste Estudo Técnico, opta-se pela SOLUÇÂO B: Contratação de empresas públicas para provimento dos serviços técnicos especializados de TIC (Tecnologias da Informação e Comunicação), no âmbito do Ministério da Cultura (MinC), em seus sistemas críticos, com prazo de vigência contratual de 60 (sessenta) meses.

LOTE	GRUPO	DESCRIÇÃO DO GRUPO	QUANTIDADE MENSAL ESTIMADA
Único	1	Conectividade	2.300
	2	Imageamento	1.000
	3	Backup-as-a-Service (BaaS)	1.000
	4	Edge Computing	2.300
	5	Platform-as-a-Service (PaaS)	1.750

13. Estimativa de custo total da contratação

Valor (R$): 239.500.800,00

13.1 Conforme estabelecido no *Caderno de Logística – Pesquisa de Preços 2024*, a pesquisa de preços foi realizada diretamente no sistema Compras.gov.br. Em decorrência, foi gerada a Pesquisa de Preços de nº 85/2025.

13.2 A estimativa do custo total da contratação foi elaborada com base nas disposições da Instrução Normativa SEGES nº 65, de 7 de julho de 2021, e da Instrução Normativa SGD nº 94, de 23 de dezembro de 2022, aplicáveis às soluções de Tecnologia da Informação e Comunicação, tomando como referência o resultado da Pesquisa de Preços nº 85/2025. A tabela a seguir apresenta a estimativa do custo total da contratação.

		DESCRIÇÃO	QTDE		VALOR	

LOTE	GRUPO	/GRUPO	ESTIMADA (MENSAL)	VALOR UNITÁRIO	MENSAL	VALOR TOTAL 60 MESES
Único	1	Conectividade	2.300	R$ 500,40	R$ 1.150.920,00	R$ 69.055.200,00
	2	Imageamento	1.000	R$ 424,73	R$ 424.730,00	R$ 25.483.800,00
	3	Backup-as-a-Service (BaaS)	1.000	R$ 436,87	R$ 436.870,00	R$ 26.212.200,00
	4	Edge Computing	2.300	R$ 505,65	R$ 1.162.995,00	R$ 69.779.700,00
	5	Platform-as-a-Service (PaaS)	1.750	R$ 466,38	R$ 816.165,00	R$ 48.969.900,00
VALOR GLOBAL ESTIMADO (60 MESES)						R$ 239.500.800,00

14. Justificativa técnica da escolha da solução

14.1. A decisão do Ministério da Cultura (MinC) em contratar a empresa pública federal provedora de conectividade e infraestrutura de TIC para a prestação de serviços técnicos especializados de TIC (Tecnologias da Informação e Comunicação) em seus sistemas críticos apresenta uma série de justificativas sólidas, que vão além da mera escolha por empresas estatais.

14.2. A presente contratação será realizada por meio de dispensa de licitação, com fulcro no artigo 75, inciso IX, da Lei nº 14.133/2021, in verbis:

> IX - Para a aquisição, por pessoa jurídica de direito público interno, de bens produzidos ou serviços prestados por órgão ou entidade que integrem a Administração Pública e que tenham sido criados para esse fim específico, desde que o preço contratado seja compatível com o praticado no mercado.

14.3. Verifica-se, portanto, do disposto acima, a necessidade de atendimento a dois requisitos para a configuração de dispensa de licitação: em primeiro, o órgão ou entidade contratada deve integrar a Administração Pública e ser criada com o fim específico de produzir bens ou prestar os serviços contratados; e, em segundo, o preço contratado estar compatível com o praticado no mercado.

14.4. No que tange ao primeiro requisito, o fornecedor dos serviços será a empresa pública federal provedora de conectividade e infraestrutura de TIC:

> Art. 2º Os órgãos públicos federais da administração direta e as entidades da administração indireta federal, no exercício de suas competências, devem, preferencialmente, nos termos do inciso IX do caput do art. 75 da Lei nº 14.133, de 1º de abril de 2021 (Lei de Licitações e Contratos Administrativos), contratar diretamente:
>
> (...)
>
> II – A Telecomunicações Brasileiras S.A., para utilização de serviços de comunicação multimídia regidos pela Lei nº 9.472, de 16 de julho de 1997.
>
> Parágrafo único. Para os efeitos desta Lei, entende-se por serviço de comunicação multimídia o serviço fixo de telecomunicações de interesse coletivo, prestado em âmbito nacional, que possibilita a oferta de capacidade de transmissão, emissão e recepção de informações multimídia, inclusive o provimento de conexão à internet.

14.5. Em primeiro lugar, essas empresas possuem um profundo conhecimento do setor público e das especificidades da administração pública federal. Com anos de experiência atendendo órgãos governamentais, elas detêm um know-how único sobre as legislações, normas e processos internos, o que lhes permite oferecer soluções mais alinhadas às necessidades do MinC.

14.6. Além disso, a segurança da informação é um ponto crucial para os sistemas críticos do MinC, e as empresas públicas demonstram um compromisso maior com a proteção dos dados. Elas possuem infraestruturas robustas e equipes especializadas em segurança cibernética, garantindo que as informações sensíveis do MinC estejam protegidas.

14.7 Com relação à Defesa contra Ransomware e Ameaças Avançadas, a crescente agressividade, complexidade e frequência dos ataques de ransomware e ameaças avançadas dirigidos a órgãos públicos, aliada à relevância estratégica dos dados e sistemas do Ministério da Cultura, justificam, em termos técnicos, a necessidade de uma solução especializada de Defesa contra Ransomware e APT.

14.8 Trata-se de medida que:

- responde diretamente às diretrizes de segurança cibernética estabelecidas em normas federais (como a E-Cyber e a LGPD);
- reduz o risco de indisponibilidade de serviços de alta relevância social, relacionados a políticas públicas culturais;
- mitiga impactos de incidentes que, em cenários extremos, podem acarretar perda permanente de acervos digitais, vazamento de dados sensíveis, interrupção de editais de fomento e descrédito institucional.
- A adoção da solução proposta está alinhada aos princípios de eficiência, eficácia, efetividade e economicidade, uma vez que reduz:
    - o tempo médio de detecção (MTTD) e de resposta (MTTR) a incidentes;
    - o esforço operacional de equipes técnicas, por meio de automação e orquestração de ações;
    - a probabilidade de necessidade de reconstrução integral de ambientes, com custos muito superiores aos da prevenção.
    - Do ponto de vista técnico, a solução configura-se, portanto, como elemento estruturante da postura de segurança cibernética do MinC, não sendo substituível por soluções genéricas ou por mecanismos tradicionais de antivírus e firewall, que não oferecem cobertura adequada contra ameaças complexas e direcionadas.

14.9 Do ponto de vista administrativo, a empresa pública federal provedora de conectividade e infraestrutura de TIC é a única entidade pública federal com capacidade legal, técnica e operacional para fornecer:

1. conectividade estratégica governamental;
2. segurança cibernética integrada com SOC nacional;
3. datacenters TIER IV públicos;
4. infraestrutura crítica de comunicação protegida por arcabouço legal;
5. serviços satelitais via SGDC;
6. integração nativa com governo federal.

14.10 A oferta da empresa pública federal provedora de conectividade e infraestrutura de TIC elimina riscos de dependência de fornecedor privado, atende aos requisitos da Portaria 5.950/2023 e se integra aos objetivos do PDTIC MinC.

14.11 A adoção de solução IAM/IDMaaS pelo Ministério da Cultura justifica-se tecnicamente pelos seguintes fatores:

- Preponderância de ataques baseados em credenciais: Estudos e incidentes recentes demonstram que grande parte das invasões em órgãos públicos decorre de uso de credenciais fracas, comprometidas ou reutilizadas em múltiplos serviços. Sem uma camada robusta de IAM, com MFA, SSO e políticas de acesso dinâmicas, o MinC permanece suscetível a esse vetor de ataque;
- Exigências da LGPD e de normativos de segurança: A LGPD, a PPSI/MGI, a E-Cyber e normas GSI/PR demandam controle estrito de acessos, registro de trilhas, segregação de funções e capacidade de resposta a incidentes envolvendo dados pessoais. Uma solução IAM/IDMaaS fornece os mecanismos técnicos necessários para cumprir esses requisitos, inclusive no que se refere à prestação de contas (accountability) perante órgãos de controle e à Autoridade Nacional de Proteção de Dados (ANPD);
- Complexidade do ambiente híbrido do MinC: O Ministério opera com sistemas legados, aplicações modernas, serviços em nuvem, SD-WAN e soluções de edge computing, além de múltiplos perfis de usuários (internos, terceirizados, parceiros, beneficiários de políticas públicas). A gestão manual e fragmentada de identidades em tal contexto é inviável e insegura, impondo a necessidade de solução centralizada e automatizada;
- Redução do risco institucional de comprometimento de dados culturais e pessoais: O acervo de dados sob responsabilidade do MinC possui elevado valor cultural, social e jurídico. Sem IAM, falhas na concessão, na revisão e na revogação de acessos podem resultar em vazamentos, manipulação indevida ou destruição de informações, com impacto direto na confiança da sociedade, na continuidade dos serviços e na responsabilização do órgão;
- Pré-requisito para outras camadas de segurança: A solução IAM/IDMaaS é componente fundamental para o correto funcionamento de ESM, SOC, PAM, SIEM, Resposta a Incidentes, Defesa contra Ransomware/APT e demais controles, na medida em que fornece o contexto de identidade e privilégio necessário para decisões de bloqueio, contenção, correlação de eventos e automação de respostas.
- Dessa forma, a implementação de IAM/IDMaaS constitui medida indispensável para elevação da maturidade de segurança cibernética do Ministério da Cultura, sendo técnica e funcionalmente aderente às necessidades identificadas neste Estudo Técnico Preliminar.
- O aumento do volume de logs gerados pelos sistemas do MinC, a diversidade de plataformas (on-premise, nuvem, borda) e a sofisticação das ameaças cibernéticas tornam inviável a detecção eficaz de incidentes de segurança sem o uso de plataforma de SIEM centralizada, escalável e integrada ao SOC.

14.12 A adoção de solução de SIEM integrada ao SOC empresa pública federal provedora de conectividade e infraestrutura de TIC:

1. permite visão unificada do risco, por meio de correlação avançada de eventos entre múltiplas fontes;
2. reduz o tempo de detecção e resposta a incidentes, com alertas em tempo real e playbooks de automação;
3. fortalece a capacidade de auditoria e atendimento à LGPD, PPSI/MGI, E-Cyber e políticas internas;
4. contribui para o cumprimento das recomendações de planejamento e gestão de riscos de TIC previstas na IN SGD/ME nº 94/2022 e nos pareceres de controle.

14.12 A implantação de solução estruturada de auditoria e governança de dados reforça a segurança operacional e a integridade das informações do Ministério da Cultura, permitindo o rastreamento de acessos, a prevenção de fraudes, o atendimento célere a requisições de órgãos de controle e a garantia de decisões baseadas em dados confiáveis, conforme exigências da LGPD e melhores práticas de governança pública.

14.13 Em especial, a natureza crítica dos sistemas e dos dados sob custódia do Ministério da Cultura exige a adoção de serviço contínuo de análise e gestão de vulnerabilidades, o que reforça a pertinência da escolha por empresa pública especializada, apta a prover infraestrutura segura e mecanismos permanentes de identificação, classificação e tratamento de fragilidades de segurança cibernética, em alinhamento com a Estratégia Nacional de Segurança Cibernética, com a LGPD e com as políticas internas de segurança da informação.

14.14 A implementação de solução PAM é tecnicamente justificada pelos seguintes aspectos:

- Contas privilegiadas são o principal alvo de atacantes em campanhas de ransomware e APT, pois oferecem acesso amplo à infraestrutura, permitindo desativar controles, apagar evidências, manipular dados e ampliar rapidamente o impacto do ataque;
- A LGPD, a PPSI/MGI, a E-Cyber e normas de segurança demandam controle rigoroso das ações de administração sobre sistemas e dados, especialmente quando envolvem dados pessoais ou informações sensíveis, exigindo trilhas de auditoria detalhadas e capacidade de reconstruir eventos;
- A gestão tradicional de contas privilegiadas, baseada em senhas compartilhadas e armazenamento disperso, é incompatível com o nível de risco atual e com as melhores práticas de segurança da informação, sendo necessária adoção de cofre central, rotação automática, controle de uso e gravação de sessões;
- Ambientes híbridos e distribuídos, que combinam datacenter, nuvem, SD-WAN e edge computing, ampliam o número de pontos de administração e tornam impraticável o controle manual e fragmentado das credenciais privilegiadas, reforçando a necessidade de solução especializada;
- PAM é componente estruturante da arquitetura de segurança, integrando-se a IAM/IDMaaS, ESM, SOC, SIEM, Resposta a Incidentes, Forense Digital e mecanismos de Defesa contra Ransomware/APT, sendo fundamental para limitar o impacto de incidentes, reduzir o tempo de resposta e fornecer evidências em auditorias e investigações.
- Dessa forma, a adoção de PAM configura-se como medida indispensável para elevar a maturidade de segurança cibernética do Ministério da Cultura, mitigando riscos críticos associados ao uso de privilégios administrativos e fortalecendo a confiança institucional nos serviços digitais prestados.

14.15 A infraestrutura tecnológica do Ministério da Cultura é caracterizada por alta complexidade, diversidade de componentes, interdependência sistêmica e sensibilidade intrínseca dos dados tratados. A evolução do cenário de ameaças, associada ao aumento da dependência digital das políticas públicas culturais, exige solução que permita elevação estrutural da maturidade de segurança, portanto, a plataforma de Enterprise Security Management (ESM):

- reduz drasticamente o tempo de detecção e resposta a incidentes;
- fornece base de evidências confiável para auditorias internas e externas;
- habilita a implementação progressiva de Zero Trust;
- garante conformidade contínua por meio de automação;
- melhora a resiliência institucional;
- aumenta a eficiência operacional e reduz custos decorrentes de ataques e indisponibilidades.
- A crescente sofisticação de ataques e a criticidade dos sistemas culturais demonstram que o MinC não pode operar sem mecanismos formais, automatizados e juridicamente estruturados de Resposta a Incidentes e Forense Digital. Essa capacidade reduz danos, garante conformidade, preserva evidências, assegura continuidade institucional e protege dados sensíveis de agentes culturais.

14.16. Outro fator relevante é o desenvolvimento tecnológico nacional. Ao contratar empresas públicas, o governo incentiva a indústria nacional de tecnologia da informação, fortalecendo o mercado interno e reduzindo a dependência de soluções estrangeiras.

14.17 A transparência e o controle são características marcantes das empresas públicas, o que garante maior confiabilidade e accountability na prestação dos serviços. A gestão pública é orientada para o interesse público, buscando sempre a melhor relação custo-benefício para os serviços prestados.

14.18 Ademais, a continuidade dos serviços é um fator importante a ser considerado. As empresas públicas possuem uma longa história de parceria com o MinC, o que garante uma transição mais suave e contínua dos serviços, minimizando interrupções e perdas de dados.

14.19. Por essas razões, a escolha pela empresa pública federal provedora de conectividade e infraestrutura de TIC demonstra um compromisso do MinC com a segurança, a eficiência e o desenvolvimento tecnológico dos seus sistemas críticos. Além disso, a contratação dessas empresas contribui para fortalecer a indústria tecnológica nacional e garantir a proteção dos dados dos cidadãos.

14.20 DO NÃO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS E ECONÔMICOS

14.20.1 De acordo com as exigências contidas no art. 18, § 1º., inciso VIII, da Lei 14.133/2023 e em atendimento ao inciso I, do §2º, do art. 12, da IN 94/2022.

14.20.2 O art. 40 estabelece em seu § 3º que o parcelamento será adotado quando:

> *I - a economia de escala, a redução de custos de gestão de contratos ou a maior vantagem na contratação recomendar a compra do item do mesmo fornecedor; e, II - o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido.*

14.20.3 Desta forma, tendo em vista os requisitos de negócio e a solução integrada de tecnologia da informação pretendida, bem como os aspectos técnicos peculiares, recomendamos o Lote Único, garantindo, desta forma, a qualidade e a gestão do serviço (contrato, acordos de nível de serviço, equipes etc.), assim como sua operação, manutenção, expansão e desenvolvimento;

14.20.4 É cristalino o entendimento do Tribunal de Contas da União – TCU de que "*é lícito o agrupamento de lotes de itens por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si.*";

14.20.5 As lições do Professor Jorge Ulisses Jacoby Fernandes, no Parecer nº 2086/00, elaborado no processo nº 194 /00 do Tribunal de Contas do Distrito Federal – TDCF apontam que:

> "*Desse modo a regra do parcelamento deve ser coordenada com o requisito que a própria lei definiu: só se pode falar em parcelamento quando há viabilidade técnica para sua adoção. (...) Nesse sentido, um exame atento dos tipos de objeto licitados pela Administração Pública evidência que embora sejam divisíveis, há interesse técnico na manutenção da unicidade, da licitação ou do item da mesma. Não é, pois, a simples divisibilidade, mas a viabilidade técnica que dirige o processo decisório. Observa-se que, na aplicação dessa norma, até pela disposição dos requisitos, fisicamente dispostos no seu conteúdo, a avaliação sob o aspecto técnico precede a avaliação sob o aspecto econômico. É a visão jurídica que se harmoniza com a lógica. Se um objeto, divisível, sob o aspecto econômico for mais vantajoso, mas houver inviabilidade técnica em que seja licitado em separado, de nada valerá a avaliação econômica. Imagine-se ainda esse elementar exemplo do automóvel: se por exemplo as peças isoladamente custassem mais barato, mesmo assim, seria recomendável o não parcelamento, pois sob o aspecto técnico é a visão do conjunto que iria definir a garantia do fabricante, o ajuste das partes compondo todo único, orgânico e harmônico. Por esse motivo, deve o bom administrador, primeiramente, avaliar se o objeto é divisível. Em caso afirmativo, o próximo passo será avaliar a conveniência técnica de que seja licitado inteiro ou dividido.".*

14.20.6 Portanto, presente a possibilidade de ocorrência do risco apontado no inciso II "...possibilidade de risco ao conjunto do objeto pretendido.". Ainda, levamos em conta os requisitos de negócio e as soluções de tecnologia da informação objeto, bem como os aspectos técnicos peculiares de cada uma delas. Desta forma a equipe técnica entende como viável e justificável que a presente contratação se dê por lote único, garantindo, desta forma, a qualidade e a gestão dos serviços, assim como sua operação, manutenção e desenvolvimento.

14.20.7 Sendo assim, o Lote Único mostra-se mais viável ao atendimento das necessidades do MinC com vistas a aquisição da solução;

15. Justificativa econômica da escolha da solução

15.1 Foi realizada pesquisa de preços conforme Proposta 4910-007-26 – Modelo Contratual da empresa pública federal provedora de conectividade e infraestrutura de TIC.

15.1.1. A justificativa econômica para a escolha da empresa pública federal provedora de conectividade e infraestrutura de TIC como prestadora dos serviços especializados de Tecnologia da Informação e Comunicação (TIC) pelo Ministério da Cultura ultrapassa uma simples comparação de preços. Essa decisão considera a qualidade dos serviços prestados, a capacidade de atendimento às demandas específicas da Administração Pública e a aderência aos princípios constitucionais da economicidade, da eficiência e do interesse público.

15.1.2 Empresas públicas, como a empresa pública federal provedora de conectividade e infraestrutura de TIC, por sua estrutura consolidada e pela natureza institucional de suas operações, costumam obter condições comerciais mais vantajosas junto a fornecedores, o que se traduz em preços mais competitivos para aquisição de equipamentos, soluções tecnológicas e serviços. Além disso, a natureza pública dessas entidades favorece uma gestão mais alinhada com os objetivos do Estado, permitindo maior controle e transparência, além de menor burocracia e custos operacionais reduzidos.

15.1.3. No contexto do Ministério da Cultura, a contratação da empresa pública federal provedora de conectividade e infraestrutura de TIC representa uma oportunidade de garantir serviços qualificados, economicamente viáveis e alinhados com as políticas culturais nacionais, respeitando a especificidade das ações culturais e o papel do Estado como indutor do desenvolvimento do setor.

15.1.4 Com relação ao prazo de contratação de 60 (sessenta) meses, a princípio vale ressaltar que os serviços objeto da contratação em tela tem características de contínuos, pois são essenciais para o desenvolvimento das atividades principais do Ministério da Cultura, e sem eles não seria possível realizar com segurança os objetivos que incluem garantir a diversidade cultural, ampliar o acesso da população à cultura, fortalecer a economia criativa e preservar o patrimônio e cultural do Brasil.

15.4.5 Destaca-se, ainda, que para o cumprimento destes objetivos o Ministério se cerca de sistemas de informação, links de comunicação e toda uma infraestrutura de TIC, que, devidamente disponível, torna possível a execução das políticas públicas.

15.4.6 A vigência contratual na duração planejada no ETP e consequente TR reflete a preocupação das áreas técnicas na manutenção dos serviços disponibilizados aos cidadãos, tendo em mente que a movimentação deste aparato de serviços requer um planejamento de médio a longo prazo, pois, em um simples exemplo de uma atividade de “preservação de bases de dados – backup”, seriam movidos centenas de milhares de dados de um datacenter para outro, tarefa que não é simples e pode acarretar riscos de perda de informações.

15.4.7 De forma estratégica, o Ministério entende que a contratação por um período mais extenso permite que o fornecedor faça investimentos, se organize e, consequentemente ofereça preços mais competitivos e vantajosos para a Administração no momento da contratação.

15.4.8 Sob o ponto de vista da eficiência na redução da burocracia, entendemos que esta duração de sessenta meses evita a necessidade de licitações anuais ou frequentes para o mesmo objeto, **evitando, também, migrações e diminuindo a curva de aprendizado das equipes técnicas.**

15.4.9 Vislumbramos como outro benefício da contratação com este intervalo como sendo a segurança jurídica, no ponto em que o Ministério sabe que o serviço será prestado pelo tempo definido e a empresa pública federal provedora de conectividade e infraestrutura de TIC(fornecedor) pode planejar seus recursos humanos e materiais, facilitando o planejamento plurianual da gestão pública.

16. Benefícios a serem alcançados com a contratação

16.1. A contratação de empresas públicas como a empresa pública federal provedora de conectividade e infraestrutura de TIC pode trazer diversos benefícios para o Ministério da Cultura, como a garantia de segurança da informação, a agilidade na implementação de soluções, a otimização de processos e o desenvolvimento de soluções personalizadas.

16.2. Os principais benefícios potencialmente alcançáveis com o provimento da solução são:

- Maximizar a usabilidade dos serviços de TIC;
- Priorização de políticas públicas, como a inclusão digital no âmbito da Cultura.
- Alinhamento com as políticas públicas do governo, contribuindo para a realização dos objetivos estratégicos do país.
- Adquirir soluções necessárias ao suporte dos serviços prestados pela TI;
- Garantir a continuidade de serviços estratégicos de interesse público;
- Aumentar a eficiência do Órgão mediante o uso integrado da tecnologia da informação e o aprimoramento da gestão, contribuindo para a segurança da informação e comunicações e a segurança cibernética;
- Aprimoramento dos processos de negócios, administrativos e técnicos no que tange aos serviços de Empresas Públicas;
- Padrões elevados de segurança da informação;
- Conformidade com as normas legais;
- Modernização tecnológica das plataformas.

16.3. Redução contínua da superfície de ataque e da janela de exposição a riscos cibernéticos, por meio da implementação de serviço estruturado de análise e gestão de vulnerabilidades, com monitoramento permanente, priorização de correções e apoio à tomada de decisão das equipes técnicas.

16.4. Melhoria da confiabilidade, rastreabilidade e integridade das informações institucionais, por meio de solução de auditoria e governança de dados que assegura plena visibilidade sobre o ciclo de vida dos dados, fortalecendo a tomada de decisão e a conformidade regulatória.

16.5. A implantação de plataforma de Enterprise Security Management permitirá ao MinC alcançar um grau de maturidade significativamente superior, com:

- visão unificada e contínua de todos os riscos, eventos, vulnerabilidades e incidentes;
- capacidade de resposta automatizada e coordenada;
- monitoramento permanente de conformidade;
- redução do risco reputacional, operacional e regulatório;
- fortalecimento da governança e da tomada de decisão.

16.6. Alguns benefícios adicionais podem ser obtidos através da implantação de processos de Resposta a Incidentes e Forense Digital:

- redução dos impactos materiais e reputacionais;
- recuperação mais rápida dos serviços afetados;
- preservação de evidências conforme cadeia de custódia (valor jurídico);
- apoio às análises de causa raiz e auditorias internas/externas;
- reforço da resiliência institucional contra ameaças avançadas;
- adequação plena ao PPSI/MGI, LGPD e E-Cyber.

16.7. A implantação de solução de Defesa contra Ransomware e Ameaças Avançadas proporcionará, entre outros, os seguintes benefícios ao Ministério da Cultura:

- proteção prévia e ativa contra criptografia maliciosa de dados, reduzindo drasticamente a probabilidade de sequestro de informações;
- redução do impacto e do tempo de indisponibilidade de sistemas e serviços digitais, contribuindo para a continuidade das políticas públicas culturais;
- preservação de dados culturais e pessoais, em conformidade com a LGPD e com as normas de proteção de acervo e patrimônio digital;
- capacidade de resposta imediata e coordenada, com isolamento automático de dispositivos e bloqueio de canais de ataque;
- fortalecimento da integração com ESM, Resposta a Incidentes (IR) e Forense Digital, viabilizando visão unificada do risco e tratamento estruturado de incidentes;
- contribuição direta para o cumprimento da PPSI/MGI, da E-Cyber e das normas de segurança do GSI/PR, posicionando o MinC em patamar mais elevado de maturidade em segurança cibernética;
- redução de custos indiretos relacionados à gestão de crises, reconstrução de ambientes, perda de produtividade e eventual responsabilização jurídica;
- aumento da confiança de cidadãos, agentes culturais, parceiros institucionais e órgãos de controle quanto à capacidade do Ministério de proteger informações sob sua guarda.

16.8. Em relação às soluções de SOC – Security Operations Center, podemos destacar:

- monitoramento centralizado e contínuo de eventos de segurança, com integração plena ao SOC empresa pública federal provedora de conectividade e infraestrutura de TIC;
- aumento significativo da capacidade de detecção precoce de incidentes e ataques complexos, por meio de correlação avançada de eventos e uso de inteligência de ameaças;
- fortalecimento das trilhas de auditoria e da governança de acessos, em aderência à LGPD e PPSI/MGI;
- suporte técnico e operacional contínuo do SOC empresa pública federal provedora de conectividade e infraestrutura de TIC, com relatórios mensais e trimestrais para a gestão do MinC;
- base estruturada para evolução da arquitetura de segurança (integração com ESM, Forense, PAM, IAM, XDR, Anti-Ransomware e Vulnerabilidades).
- Entre os principais benefícios a serem alcançados com a implementação da solução IAM/IDMaaS, destacam-se:
    - Eliminação de contas órfãs e privilégios acumulados, por meio de automação do ciclo de vida de acessos e recertificações periódicas, reduzindo significativamente o risco de utilização indevida de credenciais e perfis herdados;
    - Controle rigoroso de identidades temporárias, como terceirizados, prestadores, bolsistas e colaboradores de projetos, com definição clara de datas de início e término de acesso, bem como de perfis estritamente necessários ao desempenho de suas atividades;
    - Redução expressiva da probabilidade de invasões baseadas em credenciais, em virtude da adoção de MFA, políticas avançadas de senha, SSO controlado, acesso condicional e integração com mecanismos de detecção de login anômalo, aumentando a resiliência frente a ataques de phishing, brute force e credential stuffing;
    - Melhoria da produtividade dos usuários e da eficiência da STII, ao simplificar a experiência de autenticação com SSO, reduzir chamados de suporte relacionados a senha, padronizar fluxos de solicitação e aprovação de acessos e automatizar tarefas repetitivas de criação, alteração e exclusão de contas;
    - Conformidade reforçada com LGPD, PPSI/MGI, E-Cyber e normas internas, mediante geração de relatórios estruturados de acessos, trilhas de auditoria completas, evidências de segregação de funções, recertificações e medidas de mitigação de risco, facilitando o atendimento a auditorias e a demandas de órgãos de controle;
    - Integração plena com o ecossistema de segurança do MinC, permitindo que decisões de bloqueio, contenção e resposta a incidentes considerem, em tempo real, o contexto de identidade e privilégios, aumentando a eficácia do SOC, do ESM, da Resposta a Incidentes, do PAM, das soluções de Defesa contra Ransomware/APT e dos mecanismos de microsegmentação e SD-WAN.

16.9. Entre os principais benefícios decorrentes da implementação da solução PAM, destacam-se:

- Redução drástica do risco associado a contas privilegiadas, com eliminação de senhas compartilhadas, armazenamento inseguro e uso não rastreado de credenciais administrativas;
- Aumento da capacidade de auditoria e responsabilização, por meio de gravação integral de sessões privilegiadas, trilhas detalhadas de uso e relatórios estruturados por ativo, usuário, período e tipo de operação;
- Mitigação do impacto de ataques de ransomware e APT, graças à possibilidade de bloqueio rápido, rotação imediata de senhas privilegiadas, suspensão de sessões ativas e integração com SOC, ESM, Resposta a Incidentes e Defesa contra Ransomware/APT;
- Melhoria da conformidade com LGPD, PPSI/MGI, E-Cyber e normas internas, fornecendo evidências objetivas de controle sobre atividades de administração de sistemas e acesso a dados pessoais e sensíveis;
- Profissionalização da gestão de acessos privilegiados, reduzindo dependência de procedimentos informais e aumentando a robustez dos processos de administração de infraestrutura;
- Visão gerencial consolidada do uso de privilégios, apoiando a tomada de decisão da alta administração, o planejamento de capacidade e a priorização de ações de reforço de segurança nos ativos mais críticos para as políticas públicas culturais.

16.10. Para a solução de Hiperconvergência destacamos os seguintes benefícios:

- Redução de custos e simplificação da infraestrutura.
- Maior resiliência e continuidade dos serviços.
- Escalabilidade rápida e segura conforme a demanda.
- Governança centralizada e alinhamento com boas práticas de TI.
- Com relação às soluções de ESM/ITSM com AIOps para a gestão dos serviços de TIC, podemos destacar benefícios como:
    - Continuidade dos serviços de suporte e sustentação de infraestrutura de TIC;
    - Maior conformidade com as boas práticas, considerando as diretrizes dos órgãos de controle;
    - Maior eficiência nas entregas, gerando melhor custo-benefício;
    - Maior abrangência na prestação dos serviços, considerando os avanços tecnológicos;
    - Assegurar a qualidade e disponibilidade na prestação de serviços de Sustentação aos recursos de TIC;
    - Suportar o crescimento dos serviços de TIC a níveis de desempenho satisfatório a fim de fortalecer as ações institucionais do Ministério da Cultura
    - Melhoria do nível de atendimento às demandas dos usuários finais, relacionadas ao apoio técnico no uso dos recursos computacionais e serviços disponibilizados na rede;
    - Melhoria no processo de gestão de recursos tecnológicos (Hardware e Software) do MinC.
    - Aplicação das melhores práticas de gestão de serviços de TI com base nas dimensões propostas na ITIL v4.

17. Providências a serem Adotadas

17.1. 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.

17.2. Todos os eventos da execução contratual deverão ser apontados em registro histórico adequado.

17.3. Os RISCOS mapeados estão listados no MAPA DE GERENCIAMENTO DE RISCOS.

17.4. Designar equipe para fiscalização e gestão do contrato nos moldes do Art. 29 da IN SGD/ME nº 94/2022.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

O presente Estudo, elaborado pelos integrantes Técnico e Requisitante em harmonia com o disposto no art. 11 da Instrução Normativa n° 94/2022/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.

O art. 12 do Decreto nº 9.612/2018 que foi alterado pelo Decreto nº 10.799/2021, e posteriormente, revogado pelo Decreto nº 11.299/2022, em seu texto original tratava de deveres das prestadoras de serviços de telecomunicações, conforme art. 7º do Marco Civil da Internet, dentre elas a empresa pública federal provedora de conectividade e infraestrutura de TIC, que, de acordo com o Decreto nº 11.299/2022 detém a gestão exclusiva da Rede Privativa de Comunicação da Administração Pública Federal, estabelecendo a preferência da empresa pública federal provedora de conectividade e infraestrutura de TIC para os serviços de telecomunicações, exigindo uma consulta à empresa antes da abertura de licitações, que, atendendo aos requisitos, a contratação pode ser feita por dispensa de licitação (inciso IX do art. 75 da Lei 14.133/2021).

Neste diapasão, a empresa pública federal provedora de conectividade e infraestrutura de TIC através de instrumentos denominados Solicitação de Proposta (Request For Proposal – RFP) capta potenciais fornecedores para a prestação de serviços (Concetividade, Imageamento, Edge Computing, Backup-as-a-Service – BaaS, Infraestructure-as-a-Service – IaaS e Platform-as-a-Service - PaaS), consoante o Ato nº 1.027/2011 e Termo PVST/SPV nº 118/2011 – Anatel. Trata-se, portanto, de potenciais contratos que têm por objeto o fornecimento, pela(as) contratada(s), de bens especificamente vinculados à execução das atividades que compõem o objeto social da empresa pública federal provedora de conectividade e infraestrutura de TIC, razão pela qual as contratações advindas das RFPs se amoldam ao permissivo legal do § 3º, inciso II do art. 28 da Lei nº 13.303/2016, que possibilita a aquisição dos insumos pertinentes para a execução direta das atividades relacionadas ao objeto social da empresa pública federal provedora de conectividade e infraestrutura de TIC.

Vale ressaltar que a oferta de serviços de telecomunicações disponibilizados pela empresa pública federal provedora de conectividade e infraestrutura de TIC ao Governo Federal apresenta-se como sinérgica à disponibilização de serviços de Datacenter uma vez que otimiza a comunicação dos clientes, no caso o Ministério da Cultura, dentro da própria rede da empresa pública federal provedora de conectividade e infraestrutura de TIC, reduzindo a necessidade de saída para a internet.

Por fim, as equipes de planejamento do Ministério entendem como pertinente e amplamente legal a contratação da empresa pública federal provedora de conectividade e infraestrutura de TIC para o objeto em questão.

Em complemento, os requisitos listados atendem adequadamente às demandas formuladas, os custos previstos são compatíveis e os riscos identificados são administráveis, pelo que RECOMENDAMOS o prosseguimento da pretensa contratação.

19. Responsáveis

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

FERNANDO KLEBER DE ARAUJO SOUZA

Integrante Requisitante

Assinou eletronicamente em 20/03/2026 às 15:34:49.

DIEGO LISBOA RIOS

Integrante Técnico

Assinou eletronicamente em 20/03/2026 às 15:36:10.

FRANCISCO SAMUEL PINHEIRO SALES

Integrante Administrativo

Assinou eletronicamente em 20/03/2026 às 15:32:14.

MUNIQUE REIS BRAZ COUTINHO

Autoridade Máxima de TIC

Assinou eletronicamente em 20/03/2026 às 15:38:28.