

Estudo Técnico Preliminar 53/2024

1. Informações Básicas

Número do processo: 01400.013416/2023-42

2. Descrição da necessidade

Contratação de subscrição de solução de Segurança da Informação para Gestão de Identidade e Gestão de Acesso por doze (12) meses, incluindo garantia de suporte e atualização.

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

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

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

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

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

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

providos pelo Ministério do Turismo com a implementação e a modernização do próprio parque de tecnologia da informação do Ministério da Cultura.

2.2. Sobre as Contas de Usuários e os Sistemas de Autenticação do MinC

2.2.1. O Ministério da Cultura (MinC) utiliza uma infraestrutura de TI diversificada para suportar suas operações e fornecer serviços aos cidadãos. A infraestrutura inclui vários sistemas e portais, cada um com seus próprios mecanismos de autenticação e gestão de identidade. A rede do MinC é projetada para ser robusta e segura, garantindo a conectividade e proteção dos dados.

2.2.2. O MinC possui instalações em várias regiões do Brasil, com a sede localizada em Brasília. A distribuição geográfica exige uma infraestrutura de TI que possa suportar a colaboração e comunicação entre diferentes locais, garantindo que todos os escritórios e departamentos estejam integrados e operem de maneira coesa.

2.2.3. Com a crescente adoção do trabalho híbrido e remoto, o MinC precisa garantir que seus funcionários tenham acesso seguro e eficiente aos sistemas e dados necessários para realizar suas tarefas. Isso inclui a implementação de políticas e tecnologias que suportem o trabalho a partir de qualquer localização, sem comprometer a segurança da informação.

2.2.4. O MinC utiliza contas Microsoft para uma grande parte de seus funcionários, aproveitando a integração com a suíte de produtividade do Microsoft Office 365 e outros serviços associados. Essas contas são gerenciadas centralmente para garantir a segurança e o controle de acesso adequado.

2.2.5. O Microsoft Active Directory (MS AD) é utilizado pelo MinC para a gestão centralizada de identidades e acessos. O MS AD facilita o provisionamento e desprovisionamento de contas de usuários, a definição de políticas de acesso baseadas em funções e a integração com diversos sistemas e aplicações utilizadas pelo Ministério.

2.2.5. O MinC opera diversos sistemas e portais, cada um com seus próprios requisitos de autenticação. Essa diversidade requer uma estratégia integrada de gestão de identidade e acesso que possa unificar e simplificar o processo de login para os usuários, garantindo ao mesmo tempo a segurança e a conformidade.

2.2.6. Para suportar o trabalho remoto, o MinC precisa garantir que seus funcionários possam se conectar de maneira segura aos recursos internos. Isso inclui o uso de VPNs (Redes Privadas Virtuais) para proteger as comunicações e a implementação de autenticação multifator (MFA) para adicionar uma camada extra de segurança. Além disso, é fundamental monitorar continuamente essas conexões para detectar e responder rapidamente a qualquer atividade suspeita.

2.2.8. O MinC adota a Política de Segurança da Informação (POSIN), que estabelece diretrizes e princípios para garantir a proteção das informações e sistemas sob sua responsabilidade. A POSIN aborda aspectos como controle de acesso, gestão de riscos, resposta a incidentes, e conscientização dos usuários. Mais detalhes podem ser obtidos no site oficial do MinC.

2.2.9. A Norma Interna de Segurança da Informação de Controle de Acesso (NISI 01/2024) detalha os procedimentos e controles específicos para a gestão de acesso às informações e sistemas do MinC. Essa norma complementa a POSIN, especificando as medidas de segurança necessárias para garantir que apenas usuários autorizados possam acessar recursos sensíveis. Para mais informações sobre a NISI 01/2024 e outras normas de segurança do MinC, acesse <https://www.gov.br/cultura/pt-br/acesso-a-informacao/acoes-e-programas/governanca/politica-de-seguranca-da-informacao>.

2.2.10. A infraestrutura de TI do Ministério da Cultura é projetada para suportar uma operação segura, eficiente e distribuída geograficamente. Com a adoção de tecnologias modernas e práticas

robustas de gestão de identidade e acesso, o MinC está bem posicionado para enfrentar os desafios do trabalho híbrido e remoto, garantindo ao mesmo tempo a segurança e a conformidade com as regulamentações aplicáveis.

2.3. Quanto a necessidade de implementação de solução *Gestão de Identidade*

2.3.1. A Gestão de Identidades, ou ainda Gestão de Identidade e Acesso (Identity and access management - IAM), pode ser definida como um conjunto de processos, políticas e tecnologias capazes de garantir a identidade de uma entidade, a qualidade das informações de uma identidade, além da autenticação, autorização, responsabilização e auditoria em ambientes online, incluindo a gestão de permissões e privilégios.

2.3.2. Em relação a classificação das identidades quando consideramos a natureza em relação ao uso dos Serviços e Infraestrutura de Tecnologia da Informação, é possível identificar quatro (04) tipos de usuários no contexto das organizações:

2.3.2.1. Cliente ou Usuário Final (End-User): São indivíduos que utilizam as soluções de TI da organização. Usuários Normais ou Padrões com Uso Individual, com pouco acesso e com informações restritas, e privilégios restritos. Geralmente estão em maior número na empresa. Ainda podem ser classificados com Internos ou Externos.

2.3.2.2. Administradores (Admin): Administradores ou Super Usuários, do inglês SuperUsers, com uso compartilhado, existente para realizar mudanças de configuração (planejadas ou não) e que possui acesso elevado a informações, e privilégios elevados. São exemplos deste tipo de conta: Administrator, Local Admin, Root, db2admin e sysadmin

2.3.2.3. Desenvolvedores (Devs): São especialistas que tem acesso a recursos específicos que subsidiam o desenvolvimento de software e projetos no contexto da organização. Precisam de privilégios específicos a depender da sua especialidade. A exemplo de programadores, administradores de Banco de Dados, entre outros.

2.3.2.4. Aplicações e Serviços (Application): Contas de Serviço são contas para execução, manutenção ou permissão de acesso referentes a aplicações e serviços específicos. Geralmente de uso compartilhado, e dependente de uma aplicação específica, que necessidade de privilégio elevado para desempenhar sua tarefa (Aplicações – A2A, Banco de Dados – A2DB, Monitoração de Desempenho, Backup, entre outros).

2.3.3. Para contas dos Tipos Administradores, Desenvolvedores e de Serviço há recursos de Gestão de Acessos Privilegiados (Privilege Account Management – PAM). São soluções que realizam a Gestão de Credenciais, Monitoramento de Sessão, Autorização de Comandos, entre outros.

2.3.4. A gestão de privilégios possibilita armazenar informações detalhadas sobre cada permissão concedida, gerar diagnósticos precisos para a conformidade de todos os aplicativos utilizados, documentos e registros acessados, conferindo para a Organização, o controle necessário para regular o uso dos dados.

2.3.5. Visto isso, vale destacar que uma solução de Gestão de Acesso serve tanto para o gerenciamento de acesso para os clientes/usuários não institucionais, aqueles que de alguma forma utilizam sistemas da instituição, como clientes. Quanto para gerenciamento de acesso dos servidores, colaboradores e parceiros institucionais.

2.3.6. O controle de usuários pode trazer benefícios a serem detalhados na seção Necessidade de Negócio, tais como: Redução da complexidade dos acessos; Hierarquização das permissões; Automação e centralização da administração.

2.3.7. Dentre as possibilidades de serviços associadas à Gestão de Identidade está o Sigle Sign-ON (SSO), soluções de Múltiplos Fatores de Autenticação (Multiple Fator Authentication - MFA) e o Gateway de Aplicações.

2.3.8. O Single Sign-On (SSO) é um método de autenticação que permite que um usuário faça login uma vez em um sistema e seja automaticamente autenticado em vários outros sistemas, sem a necessidade de inserir suas credenciais novamente. Em vez de ter que lembrar e inserir várias combinações de nome de usuário e senha para acessar diferentes aplicativos ou serviços, o SSO permite que o usuário acesse todos eles com apenas um conjunto de credenciais de login. Isso simplifica o processo de autenticação e aumenta a segurança, pois reduz a necessidade de múltiplas senhas e minimiza o risco de exposição de credenciais.

2.3.9. O Gateway de Aplicativos (App -gateway) permite o acesso seguro a aplicativos locais sem usar VPNs, fazer alterações de código ou implantar infraestrutura adicional.

2.4. Quanto a necessidade de implementação de solução Gestão de Acesso

2.4.1. No contexto da segurança da informação, a Gestão de Acesso refere-se ao conjunto de práticas, políticas e tecnologias utilizadas para gerenciar e regular o acesso a recursos, sistemas e dados dentro de uma organização. O objetivo principal do controle de acesso é garantir que apenas usuários autorizados tenham permissão para acessar informações específicas, sistemas ou áreas físicas, enquanto usuários não autorizados são impedidos de fazê-lo.

2.4.2. Dentre tantas soluções existe o *Secure Access Service Edge (SASE)*, em tradução livre para o português seria Borda de Serviço de Acesso Seguro. É uma abordagem de arquitetura de rede e segurança da informação que combina conectividade de rede e serviços de segurança em plataforma unificada, proporcionando acesso seguro à nuvem, aplicações e recursos de rede, independentemente da localização do usuário. A ideia é integrar funções como SD-WAN (Rede Definida por Software), segurança de perímetro, CASB (Cloud Access Security Broker), FWaaS (Firewall as a Service), ZTNA (Zero Trust Network Access) e outros serviços de segurança em uma arquitetura unificada baseada na nuvem.

2.4.3. Essa abordagem permite que as organizações simplifiquem e fortaleçam sua postura de segurança, ao mesmo tempo em que oferecem uma experiência de usuário consistente e segura, independentemente de onde os usuários estejam e de quais dispositivos eles estejam usando. SASE é especialmente relevante em um ambiente de trabalho moderno, onde os funcionários podem estar distribuídos geograficamente e acessar recursos de TI de diferentes locais e dispositivos.

2.4.4. A relação entre Controle de Acesso e SASE está na integração desses conceitos dentro da arquitetura unificada proposta pelo SASE. O controle de acesso é uma parte essencial da abordagem SASE para garantir que o acesso aos recursos de rede e aplicativos seja seguro e controlado, independentemente da localização do usuário ou do dispositivo que ele está usando.

2.4.5. Dentro do contexto do SASE, o controle de acesso desempenha um papel importante em várias áreas:

2.4.5.1. Acesso Seguro à Nuvem e Aplicações: O controle de acesso garante que apenas usuários autorizados tenham permissão para acessar aplicativos e dados hospedados na nuvem, aplicando políticas de autenticação e autorização.

2.4.5.2. Zero Trust Network Access (ZTNA): O SASE incorpora princípios de ZTNA, que enfatiza a necessidade de verificar continuamente a identidade e a postura de segurança de todos os usuários e dispositivos antes de conceder acesso aos recursos de rede.

2.4.5.3. Políticas de Segurança Adaptativa: A integração de políticas de segurança adaptativas no SASE permite ajustar dinamicamente os controles de acesso com base em fatores como a localização do usuário, o dispositivo usado e o contexto da solicitação de acesso.

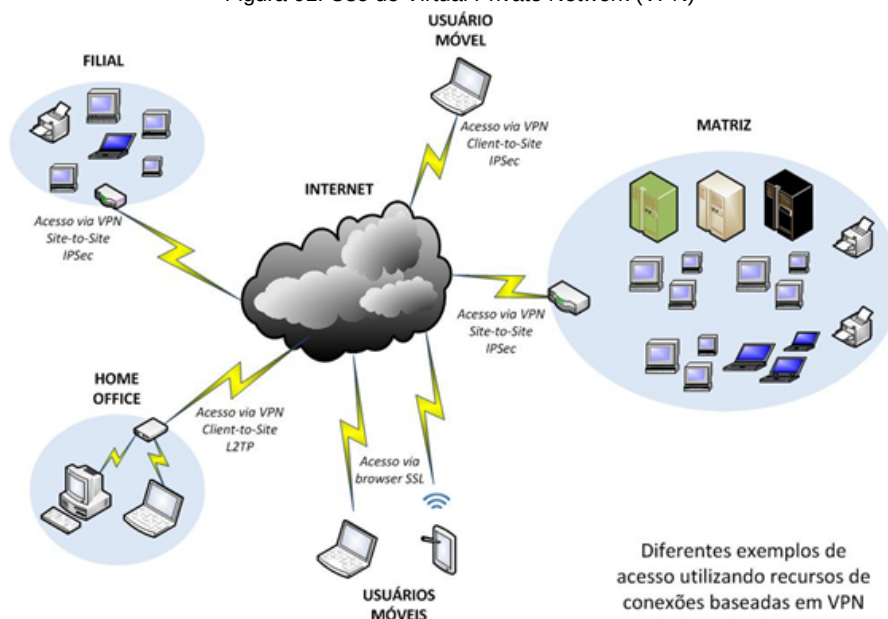
2.4.5.4. Controle de Acesso a Dados: O SASE pode fornecer controle granular sobre o acesso a dados sensíveis, garantindo que apenas usuários autorizados tenham permissão para visualizar, modificar ou transferir informações confidenciais.

2.4.6. Para destacar a vantagem do ZTNA é preciso entender o Virtual Private Network (VPN). Esta é uma tecnologia que permite estabelecer uma conexão segura e criptografada entre dispositivos ou redes através de uma rede pública, como a Internet.

2.4.7. Quando você se conecta a uma VPN, seu dispositivo cria um túnel criptografado para um servidor VPN remoto. Todo o tráfego de dados enviado e recebido entre o seu dispositivo e o servidor VPN é criptografado, o que significa que é difícil para terceiros interceptarem ou monitorarem suas comunicações.

2.4.8. As VPNs são comumente usadas por razões como: Privacidade e Segurança; Acesso Remoto e Acesso a Conteúdo Restrito Geograficamente. Esses acessos, via de regra, ocorrem conforme demonstrado na Figura 01 a seguir:

Figura 01. Uso de Virtual Private Network (VPN)



2.4.9. A seguir apresentamos os problemas mais comuns associados ao uso de VPNs:

- I. Vulnerabilidades de segurança: As VPNs podem ter vulnerabilidades de segurança que podem ser exploradas por atacantes. Isso inclui falhas de criptografia, protocolos desatualizados ou mal configurados, bugs de software e fraquezas no gerenciamento de chaves.
- II. Ameaças de segurança internas: Embora as VPNs sejam projetadas para proteger a comunicação entre pontos remotos, elas também podem ser alvo de ameaças internas. Isso inclui funcionários mal-intencionados que podem acessar informações confidenciais ou comprometer a integridade da rede por meio de uma conexão VPN.

- III. Conexões não confiáveis: Em algumas situações, a segurança de uma VPN pode ser comprometida devido a conexões não confiáveis ou públicas. Por exemplo, ao usar uma rede Wi-Fi pública, a comunicação por meio da VPN pode estar sujeita a interceptação de dados ou ataques de homens no meio.
- IV. Configuração inadequada: Uma configuração incorreta ou inadequada da VPN pode levar a problemas de segurança. Isso inclui a utilização de criptografia fraca, escolha inadequada de protocolos, autenticação fraca ou configurações de firewall mal implementadas.
- V. Riscos de gerenciamento de chaves: A segurança de uma VPN depende do gerenciamento adequado das chaves criptográficas. Se as chaves forem comprometidas ou mal gerenciadas, a integridade da conexão VPN e a confidencialidade dos dados podem estar em risco.
- VI. Dependência de fornecedores de VPN: A segurança de uma VPN também está sujeita à confiabilidade e às práticas de segurança do provedor de VPN. Se o provedor não seguir as melhores práticas de segurança ou tiver vulnerabilidades em seus sistemas, isso pode afetar a segurança das conexões VPN.

2.4.10. Para se contrapor ao acesso VPN surge o ZTNA, que visa aprimorar a proteção de redes corporativas e recursos de Tecnologia da Informação (TI), adotando um modelo de segurança baseado no princípio de confiança zero, já citado anteriormente.

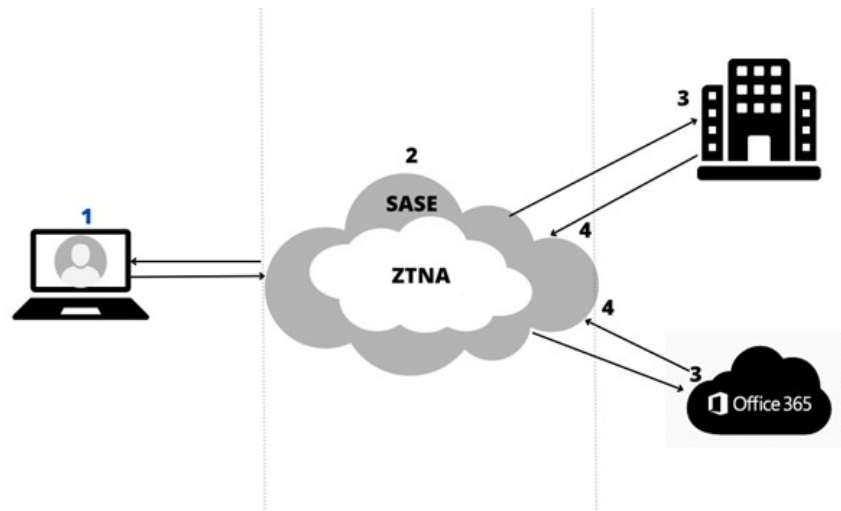
2.4.11. Ao contrário do modelo tradicional de segurança de rede, que assume que tudo dentro da rede é confiável e seguro, o ZTNA parte do pressuposto de que nada é confiável por padrão, nem mesmo os dispositivos dentro da rede corporativa. Portanto, em vez de confiar na localização física da rede ou em uma rede privada tradicional, o ZTNA autentica e autoriza cada usuário e dispositivo individualmente, independentemente de sua localização ou da rede de onde estão acessando.

2.4.12. Os principais princípios do ZTNA incluem:

- I. Autenticação Contextual: Em vez de depender apenas de credenciais de usuário, o ZTNA considera vários fatores de contexto, como identidade do usuário, tipo de dispositivo, localização, hora do dia e status de segurança do dispositivo, para tomar decisões de acesso.
- II. Acesso Baseado em Política: As políticas de acesso são aplicadas de forma granular, determinando quem tem acesso a quais recursos com base em critérios específicos, como função do usuário, necessidade de acesso e sensibilidade dos dados.
- III. Segmentação de Aplicativos: Os recursos e aplicativos são segmentados e protegidos individualmente, reduzindo a superfície de ataque e minimizando o impacto de violações de segurança.
- IV. Túneis de Acesso Direto: Em vez de rotear todo o tráfego de rede através de uma VPN tradicional, o ZTNA estabelece túneis de acesso direto entre o usuário e o recurso ou aplicativo específico que estão acessando, minimizando a exposição a ataques.

2.4.13. O ZTNA é considerado uma abordagem mais eficaz e adaptável à medida que as organizações enfrentam desafios crescentes de segurança em ambientes de trabalho distribuídos e na nuvem. Ele ajuda a garantir a segurança dos dados e recursos de TI, mantendo a flexibilidade e a acessibilidade necessárias para apoiar as operações de negócios modernas. Como exemplifica a Figura 02 a seguir.

Figura 02. Arquitetura ZTNA/SASE



2.4.14. Nesse acesso demonstrado na Figura 02, temos a disponibilização do acesso por meio do ZTNA, que ocorre da seguinte forma:

- I. Na etapa 1 temos o usuário externo, no caso um desenvolvedor da fábrica de software atuando de maneira remota necessita acessar um ambiente (servidor de aplicação) de desenvolvimento específico. O usuário se conecta por meio de credencial e senha à rede ZTNA onde o serviço está publicado
- II. Aqui o pedido de conexão é recebido pela rede ZTNA que, por sua vez, se encarrega de se conectar no recurso solicitado e previamente liberado.
- III. O datacenter do MinC e/ou a nuvem O365 recebe o pedido de conexão, validando o usuário solicitante e após isso libera apenas o recurso à rede ZTNA.
- IV. Recurso liberado para a rede ZTNA. A rede ZTNA então libera o acesso ao recurso solicitado pelo usuário. Dessa maneira a infraestrutura do MinC fica invisível reduzindo a superfície de ataque e favorecendo o controle e visibilidade de acesso aos recursos disponibilizados.

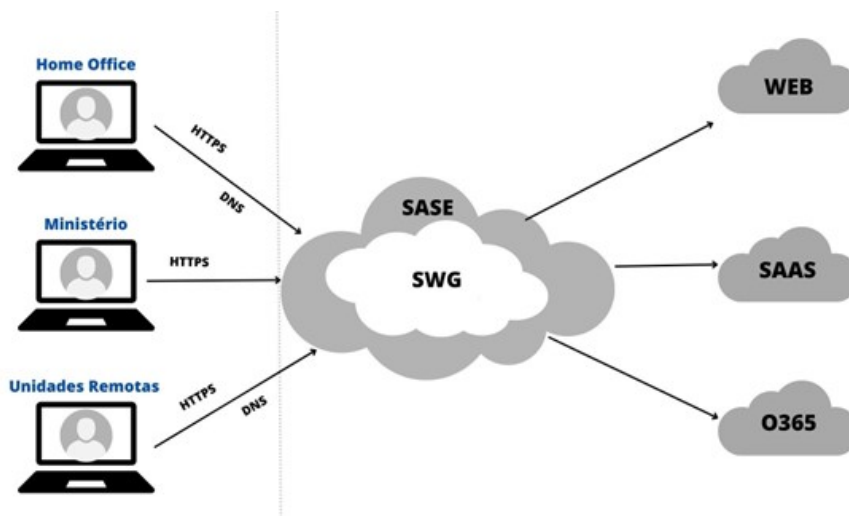
2.4.15. Para completar o Controle de Acesso e possibilitar que aconteça de forma segura há o Secure Web Gateway (SWG). Que por sua vez é uma solução de segurança da informação projetada para proteger usuários finais e redes corporativas contra ameaças online ao filtrar e monitorar o tráfego da web que entra e sai da rede corporativa.

2.4.16. As principais funcionalidades de um SWG incluem:

- I. **Filtragem de Conteúdo:** O SWG examina o tráfego da web em busca de conteúdo malicioso, como malware, phishing, sites de phishing, conteúdo inadequado ou não autorizado, e bloqueia ou alerta os usuários sobre conteúdo suspeito.
- II. **Controle de Acesso à Web:** O SWG impõe políticas de acesso à web, permitindo que os administradores de TI definam quais sites e aplicativos os usuários podem acessar, com base em categorias de conteúdo, URLs específicos, horários de acesso e outros critérios.
- III. **Inspeção SSL/TLS:** O SWG pode realizar inspeção profunda de tráfego criptografado usando SSL/TLS, descriptografando e inspecionando o tráfego para identificar ameaças ocultas dentro de conexões criptografadas.

2.4.17. Em resumo, o SWG é uma peça fundamental da infraestrutura de segurança cibernética de uma organização, ajudando a proteger contra uma variedade de ameaças online e garantindo o uso seguro e produtivo da web por parte dos usuários finais. Funciona como exemplificado na Figura 03 a seguir.

Figura 03. Arquitetura SWG/SASE



2.4.18. Portanto, o conjunto de ferramentas SASE se torna um componente fundamental do Controle de Acesso. Trabalhando em conjunto com outras funcionalidades de rede e segurança para fornecer uma abordagem unificada e integrada para proteger o acesso aos recursos de TI de uma organização em um ambiente distribuído e em constante mudança.

2.5. Motivação/Justificativa

2.5.1. Diante do cenário em que os sistemas e serviços de tecnologia da informação se tornaram cruciais para as organizações e frente a constante proliferação e evolução das ameaças cibernéticas, incluindo incidentes já ocorridos em órgãos públicos, como os ataques ao Ministério da Gestão e Inovação em Serviços Públicos (MGI), fica evidente a necessidade imperativa de evoluir constantemente, aprimorar os mecanismos de segurança e desenvolver equipes e métodos de proteção cada vez mais sofisticados.

2.5.2. Desta forma verifica-se que a pretendida contratação faz-se indispensável pois visa prover a segurança necessária aos dados e informações trafegadas em toda a rede do Ministério, minimizando, e até coibindo, a tentativas de acesso indevido aos serviços e sistemas informatizados. Considerando, ainda, que o impacto gerado pela perda ou compartilhamento de credenciais de acesso pode ocasionar indisponibilidades, acessos não autorizados, evasões e/ou danos de integridade dos dados e informações.

2.5.3. Como já foi dito anteriormente, o MinC conta com vários sistemas que implementa acesso por através de usuário e senha, bem como os sistemas de autenticação que validam estes acessos são variados, a depender do sistema que se busca o acesso.

2.5.4. O Microsoft Active Directory é utilizado para gerenciar acesso a alguns recursos para usuários internos. Já o Sistema ID Cultura (<https://id.cultura.gov.br/>) se propõe a unificar o acesso à aplicações e serviços do MinC, em especial dos usuários externos. Contudo, ambos não se consolidaram como com fonte única de autenticação.

2.5.5. Para Controle de Acesso, o MinC conta com duas (02) soluções que fazem parte do escopo do SASE: a Ferramenta de Prevenção e Perda de Dados (Data Loss Prevention - DLP) e o Cloud Access Security Broker (CASB) do Fabricante Forcepoint.

2.5.6. Dispomos, também, de Web Application Firewall que implemente alguma segurança no acesso às aplicações. Contudo, por limitações presente nos sistemas legados, esta ferramenta não é aplicada à todos os sistemas disponibilizados ao público.

2.5.7. Os acessos providos para usuários que precisam de uma conexão segura, acontece por meio de Virtual Private Network (VPN). São disponibilizados acessos VPNs para servidores /colaboradores no MinC, nos seguintes casos: (1) o acesso ao servidor de arquivos nas unidades; (2) acesso à aplicações disponíveis apenas na rede interna; (3) acesso ao SEI por colaboradores que estão fora do Brasil; (4) acesso ao ambiente de desenvolvimento, homologação e produção (fábrica de software – desenvolvedor externo); (5) acesso privilegiado para as equipes de N3 sustentar a infraestrutura.

2.5.8. Cumpre destacar que as VPNs possuem, reconhecidamente, problemas que afetam os aspectos de Segurança da Informação, conforme ALERTA 08/2022 do CTIR GOV - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo:

"...O acesso via VPN provê autenticação, integridade e confidencialidade dos dados em tráfego. Entretanto, ao mesmo tempo em que o acesso via VPN permite e flexibiliza o trabalho organizacional, o abuso deste recurso pode também ser usado como vetor para ações maliciosas ou mesmo ataques direcionados as Redes Internas das Instituições.

2.5.9. Assim, pensando aplicar mais camadas de segurança ao acesso e, conseqüentemente, aos serviços providos, bem como aumentar a utilização de soluções inerentes ao escopo do SASE buscamos, aqui, estabelecer um estudo para provável contratação do Zero Trust Network Access (ZTNA) e do Secure Web Gateway (SWG).

2.5.10. Verifica-se extremamente necessário, no âmbito desta Subsecretaria de Tecnologia da Informação e Inovação que esta Pasta envie esforços para a aquisição de solução de segurança da informação que possibilite a implantação de solução em questão, para todos os servidores e estações de trabalho do Ministério, uma vez que tais equipamentos encontram-se distribuídos em várias localidades e não possuem solução de segurança similar que contemple o gerenciamento centralizado e atualização contínua, tornado tais equipamentos vulneráveis.

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

2.5.12. A Subsecretaria de Tecnologia da Informação tem em sua missão de acordo seu Plano Diretor de Tecnologia da Informação e Comunicações - PDTIC 2024 a 2027: "Prover soluções de TI necessárias ao cumprimento da missão institucional da Ministério da Cultura por meio da adoção das melhores práticas de Governança e Gestão". Motiva-se nesse cenário, os diversos objetivos e iniciativas estratégicas da Governança e Gestão de TI para atender o Plano Diretor de Tecnologia da Informação e Comunicações - PDTIC 2024 a 2027.

2.5.13. Em seu planejamento sobre a perspectiva de Governança de TI a Subsecretaria de Tecnologia da Informação e Inovação (STII) busca alinhamento com os objetivos da Estratégia Nacional de Governo Digital 2024-2027, a exemplo do "Objetivo 4: Privacidade e Segurança", que busca:

"Ampliar a resiliência e a maturidade das estruturas tecnológicas governamentais com atenção à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética".

2.5.14. Já em seu planejamento, no intuito de alcançar seus objetivos estratégicos de Governança e Gestão de TI, o PDTIC possui um eixo específico para Segurança da Informação, "Eixo 6 – Segurança e Privacidade", onde enumera 4 macro necessidades, dentre as quais se destaca:

- N16 - Provimento de segurança de TIC adequada ao órgão
- N15 - Garantia da salvaguarda dos dados e informações do MinC
- N16 - Prevenção, tratamento e respostas a incidentes de segurança

2.5.15. Considerando ainda a necessidade de se prover os devidos recursos tecnológicos para o ambiente de forma adequada, eficiente e segura, em consonância com a Política de Segurança da Informação (POSIN)/MinC, Portaria MINC Nº 48, de 1º de Agosto de 2023, para posicionar o MinC como órgão em conformidade com os padrões estabelecidos para integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), este instituído pelo Decreto nº 7.579, de 11 de outubro de 2011.

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

2.5.17. O Programa de Privacidade e Segurança da Informação (PPSI), definido através da Portaria SGD/MGI Nº 852, de 28 de março de 2023, define em seu framework controles/salvaguardas de segurança da informação a serem atendidos pelos órgãos.

2.5.18. Entende-se que as soluções alvo deste estudo devem atender medidas presentes nos seguintes controles:

- Controle 05 – Gestão de Contas;
- Controle 06 – Gestão do Controle de Acesso;
- Controle 12 – Gestão da Infraestrutura de Rede;
- Controle 13 – Monitoramento e Defesa da Rede.

2.5.19. Diante disso, a aquisição de uma solução de segurança para o MinC, que contemple: a Gestão de Identidades e o Controle de Acesso na Infraestrutura Tecnológica do Ministério, além de contribuir significativamente com o aumento do nível de disponibilidade dos serviços de TI, possibilitará a adequação a proposição de órgãos de controle externo.

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

2.5.21. Ameaças como: malwares e ransomwares, esta em franca expansão, não se limitam apenas as estações de trabalho dos usuários, mas também ao ambiente de datacenter (virtualizado ou físico) e infraestrutura de rede de computadores.

2.5.22. Considerando a velocidade de surgimento de novas e complexas ameaças, bem como o aumento de ataques direcionados a órgãos importantes do governo é essencial possuir uma de solução de segurança atualizada e em garantia. Isso com o intuito de evitar falhas, elevando-se assim o grau de segurança necessário para o ambiente de TIC e para o funcionamento do órgão como um todo, em especial para a proteção das informações que são transitadas em seus principais sistemas.

2.5.23. Outro ponto de extrema relevância diz respeito à proteção de dados pessoais, em consonância com a Lei Geral de Proteção de Dados Pessoais – LGPD, Lei nº 13.709/2018 onde é determinado: "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

2.5.24. Neste sentido, em que pese o fato de que já foram realizados esforços para a contratação de soluções do tipo *Data Loss Prevention (DLP)* e *Cloud Access Security Broker (CASB)*, para a proteção dos dados gerenciados no âmbito desta Pasta, serviços fundamentais para proteger os dados contra vazamentos e garantir o controle de acesso com base no conteúdo, tais ferramentas se concentram principalmente na camada de aplicação e na proteção dos dados em trânsito, desta forma a implantação de uma solução de segurança para storage é essencial para proteger os dados armazenados nos sistemas de armazenamento, abordando ameaças que podem surgir internamente ou através de acesso não autorizado aos dados em repouso.

2.5.25. Desta forma busca-se uma maior abrangência da proteção, ao integrar uma solução de software de segurança para storage ao ambiente existente com DLP e CASB, assim o Ministério da Cultura pode garantir uma proteção abrangente dos dados em todas as fases do ciclo de vida, desde o armazenamento até o acesso e a transferência. Isso ajuda a mitigar os riscos de exposição de dados e reforça as medidas de segurança em toda a infraestrutura de TI.

2.6. Conclusão

2.6.1. Objetivando aumentar a maturidade de segurança da informação, reduzir a superfície de ataque, prevenir, remediar e tratar os incidentes de segurança da informação, esta equipe de planejamento da contratação tem como definição do objeto do presente Estudo Técnico, a aquisição de solução de segurança da informação que garanta no mínimo:

- a) Disponibilização de licenças de Software de segurança para a Gestão de Identidades em seus diversos níveis de permissão;
- b) Disponibilização de Software de segurança para a gestão de conexões externas à infraestrutura do MinC;
- c) Gestão dos acessos de usuários remotos à sites e sistemas;
- d) Centralização da gestão de usuários e de acessos;
- e) Treinamento/transferência de conhecimento para implantação operação e gestão das soluções fornecidas nos itens dos grupos.

2.6.2. Os serviços mencionados neste documento possuem natureza continuada, uma vez que, pela sua essencialidade, visam atender à finalidade pública de forma permanente e contínua, por mais de um exercício financeiro, com vistas a assegurar o acesso remoto da informação e, consequentemente, o funcionamento das atividades finalísticas do Ministério, de modo que, sua interrupção comprometeria o cumprimento da missão institucional do órgão.

2.6.3. Nesse sentido, é essencial que se mantenha uma solução de segurança atualizada e em garantia com o intuito de evitar falhas, elevando-se assim o grau de segurança necessário para o ambiente de TIC e para o funcionamento do órgão como um todo, em especial para a proteção das informações que são transitadas em seus principais sistemas.

2.6.4. Outro ponto de extrema relevância está nas questões de proteção de dados pessoais, o que nos remete à Lei Geral de Proteção de Dados Pessoais – LGPD, Lei nº 13.709/2018. Com a solução objeto deste estudo, o MinC realiza uma atualização tecnológica, necessária para a adequação do novo cenário de cibersegurança, quanto para a LGPD.

3. Área requisitante

Área Requisitante	Responsável
COINF	Fernando Kleber

4. Necessidades de Negócio

4.1. As necessidades de negócio, também chamadas de requisitos do negócio, são metas de mais alto nível, objetivos ou necessidades deste ministério.

4.2. Neste tópico, estão descritas as principais razões pelas quais um projeto foi iniciado, os objetivos que o projeto vai atingir e as métricas que serão utilizadas para medir o seu sucesso. Nesse sentido, a presente seção visa descrever as necessidades de negócios que conduzirão as análises de soluções e definição da solução mais adequada a tais objetivos organizacionais. A contratação da solução de segurança para identidades e acessos é motivada por diversas necessidades de negócio que visam proteger e fortalecer a infraestrutura tecnológica do órgão.

4.3. De maneira inicial e não exaustiva podemos listar as seguintes necessidades de negócio a serem atendidas:

4.3.1. Redução da complexidade dos acessos: É possível eliminar a necessidade de que os colaboradores mantenham uma grande quantidade de senhas diferentes, que normalmente são esquecidas. Por meio de uma solução de gestão de acessos, é possível realizar a integração de sistemas, simplificando o processo e, ao mesmo tempo, ampliando o controle da TI.

4.3.2. Hierarquização das permissões: O trabalho da TI em controlar os privilégios de cada tipo de funcionário aos ambientes é reduzido. Por meio de um sistema de gestão centralizado, você pode construir uma hierarquização de permissões de forma que cada colaborador tenha acesso apenas ao necessário.

4.3.3. Automação e centralização da administração: A TI perde muito tempo revendo o privilégio de acesso dos funcionários para garantir que cada um visualize apenas o permitido. Portanto, é possível automatizar todo o processo, eliminando a conta de colaboradores que deixam a organização, por exemplo. Ademais, todo o controle passa a ser feito em um único painel, simplificando a gestão para a TI.

4.3.4. Acesso remoto seguro: Garante que os colaboradores possam acessar os recursos de forma segura, independentemente da localização.

4.3.5. Prevenção contra malware e ataques cibernéticos: Como órgão do governo, o Ministério da Cultura pode ser alvo de ataques cibernéticos por diferentes motivos, incluindo espionagem, roubo de informações ou interrupção de serviços, desta forma espera-se que a solução ajude a prevenir infecções por malware e ataques de ransomware, protegendo os dispositivos e a rede contra ameaças cibernéticas. Mitigando dentre outros riscos, os associados a ameaças internas, limitando o acesso dos usuários apenas ao necessário para suas funções.

4.3.6. Conformidade regulatória: Considerando que o Ministério da Cultura está sujeito a regulamentações específicas relacionadas à proteção de dados e segurança da informação, espera-se que a Gestão de Contas e Acessos possa ajudar a garantir a conformidade com essas regulamentações, fornecendo recursos de segurança necessários para limitar o acesso indevido aos dados e sistemas contra violações.

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

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

4.3.6. Escalabilidade: A implantação de uma solução eficiente de Gestão de Identidades e Gestão de Acessos torna-se ainda mais crucial com o crescimento do Órgão. A necessidade de acompanhar o aumento do número de usuários, dispositivos e aplicativos, bem como a manutenção e possível ampliação do trabalho remoto por meio do Programa de Gestão do Desempenho (PGD). Assim, solução escolhida deve ser capaz de acompanhar a expansão do Órgão e se adaptar às novas demandas de segurança, garantindo que todos os acessos sejam devidamente controlados e protegidos.

4.4. Em suma, a contratação da solução de segurança para identidades e acessos é justificada por atender às demandas dos Plano Anual de Contratação e Plano Diretor de TI (PDTI), assegurar a segurança e controle de acessos, proteger dados governamentais, minimizar riscos de segurança, garantir conexões remotas seguras, seguir melhores práticas e possibilitar a expansão da empresa com segurança e eficiência.

5. Necessidades Tecnológicas

5.1. As necessidades tecnológicas, também chamadas de requisitos da solução de tecnologia, descrevem as características de uma solução que atendam aos requisitos do negócio.

5.2. Considerando as necessidades técnicas envolvidas na contratação da solução de segurança para identidades e acessos, destacamos os seguintes requisitos que justificam a escolha da solução.

5.3. Necessidades Tecnológicas para Soluções de Gestão de Identidade

5.3.1. Proteção das Informações:

- Proteção das informações sensíveis e confidenciais contra acessos não autorizados.
- Implementação de medidas de segurança contra ataques cibernéticos.
- Criptografia de dados em repouso e em trânsito.

5.3.2. Conformidade e Governança:

- Atender às exigências das legislações e normas aplicáveis, como LGPD, Lei de Acesso à Informação, e outras.
- Ferramentas de verificação de conformidade com regulamentos e normas.
- Implementação de políticas de conformidade e governança de identidade.

- Capacidade de gerar relatórios de conformidade para auditorias e revisões regulatórias.

5.3.3. Gestão de Identidades e Acessos:

- Gestão completa do ciclo de vida da identidade, desde a criação até a desativação.
- Controles específicos para a gestão de acessos privilegiados.
- Implementação e gestão de políticas de acesso baseadas em funções e riscos.
- Automação do provisionamento e desprovisionamento de usuários e recursos.
- Abranger todos os tipos de acessos e identidades
- Gestão de permissões e perfis de acesso, inclusive os privilegiados.
- Controle de acesso baseado em função (RBAC) e em atributos (ABAC).
- Capacidade de proteção de identidades não humanas em plataformas de containerização

5.3.4. Eficiência Operacional:

- Melhorar a eficiência operacional através da automação de processos de gestão de identidade e acesso.
- Integração com LDAP, Active Directory, e outros diretórios.
- Suporte para integração com sistemas legados e aplicações modernas (via APIs, conectores, etc.).
- Integração com serviços de nuvem e ambientes híbridos.
- Capacidade de suportar um grande número de usuários e transações.
- Suporte técnico contínuo e atualizações regulares.

5.3.5. Monitoramento e Auditoria:

- Possibilitar o controle e auditoria dos acessos aos sistemas e dados da instituição.
- Relatórios detalhados de acessos e atividades dos usuários.
- Prover registros de uso de privilégios e trilhas de auditoria
- Capacidade de auditoria completa e geração de logs.

5.3.6. Segurança Avançada:

- Suporte para autenticação multifator (Multiple Factor Authentication - MFA).
- Autenticação baseada em riscos e contexto.

5.3.7. Usabilidade e Experiência do Usuário:

- Interface intuitiva e amigável.
- Portais de autosserviço para usuários e administradores.
- Autosserviço para redefinição de senhas.
- Políticas de complexidade e expiração de senhas.
- Portal de Login Único Seguro para aplicações (SSO, Single Sign-On Seguro)
- Gestão de senhas de aplicações de negócio que não suportam Single Sign-On (login único)

5.3.8. Flexibilidade e Customização:

- Capacidade de personalização para atender às necessidades específicas da instituição.
- Suporte para workflows personalizados de aprovação de acesso.

5.3.9. Infraestrutura de Identidade:

- Repositório centralizado de identidades.
- Alta disponibilidade e resiliência.

5.3.10. Essas necessidades tecnológicas garantem que a solução de Gestão de Identidade seja eficaz na proteção de dados, conforme com regulamentos, eficiente em operações, segura contra ameaças, e amigável para usuários e administradores.

5.4. Necessidades Tecnológicas para Soluções de Gestão de Acesso (ZTNA e SWG)

5.4.1. Segurança de Acesso Remoto:

- Proteção das informações sensíveis e confidenciais contra acessos não autorizados.
- Autenticação contínua e baseada em contexto, verificando a identidade do usuário e a integridade do dispositivo.
- Implementação de autenticação multifator (MFA) para acesso seguro a aplicativos e dados internos.

5.4.2. Proteção contra Ameaças da Web:

- Bloqueio de sites maliciosos e prevenção de downloads perigosos.
- Filtragem de conteúdo e políticas de acesso para proteger os usuários durante a navegação na internet.
- Proteção contra ameaças da web, como malware, phishing e ataques de dia zero.

5.4.3. Visibilidade e Monitoramento:

- Monitoramento contínuo das atividades na web, fornecendo visibilidade completa do tráfego.
- Relatórios detalhados das atividades de navegação dos usuários.
- Capacidade de auditoria completa e geração de logs.

5.4.4. Conformidade e Governança:

- Atender às exigências das legislações e normas aplicáveis, como LGPD, Lei de Acesso à Informação, e outras.
- Ferramentas de verificação de conformidade com regulamentos e normas.
- Capacidade de gerar relatórios de conformidade para auditorias e revisões regulatórias.

5.4.5. Gestão de Acessos:

- Implementação e gestão de políticas de acesso baseadas em funções e riscos.
- Controle de acesso granular que garante que os usuários acessem apenas os recursos necessários para suas funções.
- Automação do provisionamento e desprovisionamento de acessos.

5.4.6. Monitoramento e Auditoria:

- Possibilitar o controle e auditoria dos acessos aos sistemas e dados da instituição.
- Monitoramento contínuo das atividades dos usuários e dispositivos.
- Capacidade de auditoria completa e geração de logs detalhados.

5.4.7. Eficiência Operacional:

- Melhoria da eficiência operacional através da automação de processos de acesso.
- Integração com sistemas de gestão de identidade (IDM) e outras infraestruturas existentes.
- Suporte técnico contínuo e atualizações regulares.
- Centralização da gestão das políticas de segurança web.
- Integração com outros sistemas de segurança e infraestrutura existente.
- Interface intuitiva e amigável para administração.

5.4.8. Segurança Avançada:

- Implementação de medidas de segurança contra-ataques cibernéticos, como detecção de anomalias, resposta a incidentes e inspeção SSL/TLS.
- Criptografia de dados em trânsito para proteger as comunicações durante a navegação na web, bem como entre dispositivos e aplicativos.
- Suporte para padrões de segurança como SAML, OAuth, OpenID Connect.

5.4.9. Escalabilidade e Desempenho:

- Capacidade de suportar muitos usuários e transações.
- Alta disponibilidade e resiliência.
- Desempenho otimizado para minimizar latências e garantir uma experiência de usuário positiva.

5.4.10. Flexibilidade e Customização:

- Capacidade de personalização para atender às necessidades específicas da instituição.
- Suporte para workflows personalizados de acesso e políticas de segurança.

5.5. As soluções de ZTNA e SWG são essenciais para proteger o ambiente de TI de um órgão governamental como o Ministério da Cultura, garantindo a segurança dos dados e sistemas contra ameaças cibernéticas, conformidade com regulamentos, eficiência operacional e uma experiência de usuário otimizada.

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 Sociais, Ambientais e Culturais da solução de TIC

6.2.1. Os relatórios de atividades executadas deverão ser apresentados em formato digital.

6.2.2. A CONTRATADA deverá apresentar comprovação de adoção de prática sustentável em suas operações.

6.2.3. A CONTRATADA deverá ainda observar as observações contidas no Decreto nº 7.746/2012 que estabelece critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável e a Lei nº 12.305/2010 que institui a política de resíduos sólidos, no que couber.

6.2.4. É dever da CONTRATADA observar entre outras: o menor impacto sobre recursos naturais como flora, fauna, ar, solo e água; preferência para materiais, tecnologias e matérias-primas de origem local; maior eficiência na utilização de recursos naturais como água e energia; maior geração de empregos, preferencialmente com mão de obra local; maior vida útil e menor custo de manutenção do bem e da obra; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens, serviços e obras.

6.3. Requisitos da Capacitação

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

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

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

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

6.3.5. O treinamento deverá capacitar as equipes técnicas do CONTRATANTE a operar, configurar, administrar e resolver problemas usuais na solução adquirida.

6.3.6. Quando o treinamento for ofertado remotamente (modalidade Educação à Distância), deverá ser ministrado de forma síncrona. Não computando na carga horária cursos assíncronos, matérias multimídia, voucher e similares

6.3.7. Deverá ser ofertada para uma (01) turma com no mínimo cinco (05) alunos/participantes e com carga horária mínima de vinte (12) horas por item contratado, para os itens de 1 a 9, e 12.

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

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

6.3.10. Deverá ser fornecido material didático completo e com conteúdo oficial do fabricante, podendo ser fornecido por meio de manuais/documentos em PDF.

6.3.11. É de responsabilidade da CONTRATADA registrar em ata todas as etapas do treinamento. De forma a apresentar ao final desta fase registros de data de realização da(s) sessão(ões), o conteúdo abordado e a assinatura dos participantes.

6.4. Requisitos Legais

6.4.1. Cabe destacar alguns preceitos legais e direcionamentos do Governo Federal quanto à contratação e prestação de serviços de TIC, a saber:

- I. Lei 14.133, de 01 abril de 2021 – Lei de Licitações e Contratos Administrativos;
- II. Instrução Normativa SGD/ME Nº 94, de 23 de dezembro de 2022 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISF do Poder Executivo Federal.
- III. Decreto nº 10.024, de 20 de setembro de 2019 – Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal;
- IV. Decreto Nº 7.174, de 12 de maio de 2010 – regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;
- V. Instrução Normativa nº 05/2017, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional;

- VI. Portaria MP/SGD nº 778, de 04 de abril de 2019, que dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - SISP.
- VII. Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 e seus anexos, que estabelece modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.
- VIII. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados).

6.5. Requisitos Temporais

6.5.1. Os serviços devem ser prestados no prazo máximo previstos no “Catálogo de Serviços (Apêndice B)” deste documento, a contar do recebimento da abertura da Ordem de Serviço (OS), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

6.5.2. Para os serviços de instalação e configuração das soluções, treinamento e o serviço de suporte para as soluções disponibilizadas será considerada como hora útil, aquela compreendida entre 07:30h e 18:30h em dias úteis, podendo também ser denominado como horário útil.

6.5.3. Para o serviço de monitoramento deverá ser considerada a janela de atendimento 24 x 7, ou seja, todos os dias (segunda a domingo) 24 horas diárias, sendo realizado de forma contínua.

6.5.4. Para fins de contagem de tempo estipulados nos níveis mínimos de serviço para Solicitações, a prestadora de serviço deverá observar as horas úteis, as quais são definidas pelo horário de funcionamento do órgão, devendo os serviços serem atendidos conforme previsto no “APÊNDICE B - Composição do Catálogo de Serviços”. Em caso de insucesso no atendimento a prestadora deverá designar técnico capacitado para comparecimento presencial, sempre respeitando os níveis mínimos de serviços estabelecidos para o atendimento.

6.5.5. Não existirá redefinição de tempo caso a contratada ultrapasse os tempos de atendimento entre o recebimento do chamado e o efetivo atendimento durante sua locomoção.

6.5.6. A relação de “Atividades” apresentadas “APÊNDICE B - Composição do Catálogo de Serviços” poderão ter sua execução alterada ao longo da vigência contratual, sendo passível de alterações a critério do órgão em comum acordo junto à CONTRATADA.

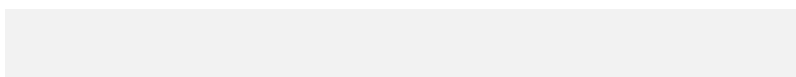
6.5.7. Todas as atividades descritas neste documento deverão ser executadas preferencialmente nas localidades e/ou modalidades estabelecidas pelo Ministério, durante o horário estabelecido.

6.5.8. Os serviços de monitoramento serão entregues para a CONTRATANTE, de forma remota com possibilidade de interação por meio de encontros e reuniões virtuais e acesso, troca e interação segura com a necessidade e encontros, reuniões, salas de crises e planejamento presencial no Distrito Federal, de forma a garantir a supervisão e fiscalização da contratação.

6.5.9. Na contagem dos prazos estabelecidos neste estudo, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

6.5.10. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.

6.5.11. Na execução dos serviços, deverão ser observados os seguintes prazos:



Atividade, Tarefa ou Serviço	Prazo máximo de início de atendimento	Prazo máximo de solução de problema
Serviços de Instalação e Configuração das Soluções (por item / módulo)	dez (10) dias	trinta (30) dias
Serviço de treinamento / capacitação por item / módulo (12 horas) ** não ocorrerão de forma concomitante	De acordo com a OS	De acordo com a OS
Monitoramento	De acordo com o catálogo de serviço	

6.6. Requisitos de Privacidade e Segurança da Informação

6.6.1. 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. Sendo:

- I. **Disponibilidade:** propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;
- II. **Integridade:** propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- III. **Confidencialidade:** propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidades não autorizados nem credenciados;
- IV. **Autenticidade:** propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

6.6.2. A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, códigos-fonte e artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venham a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de aplicação de sanção e outras reprimendas prevista em lei, independente da classificação de sigilo conferida pelo Ministério de Cultura tais documentos.

6.6.3. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em

decorrência da execução do objeto, sem autorização, por escrito, do Ministério da Cultura sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

6.6.4. Os representantes, empregados e colaboradores da CONTRATADA deverão zelar pela manutenção do sigilo absoluto de dados, informações, documentos e especificações técnicas, que tenham conhecimento em razão dos serviços executados.

6.6.5. Todas as informações, imagens e documentos a serem manuseados e utilizados são de propriedade do Ministério da Cultura e não poderão ser repassados, copiados, alterados ou absorvidos pela CONTRATADA sem expressa autorização do Ministério da Cultura, de acordo com o Termo de Compromisso de Manutenção do Sigilo a ser disponibilizado e firmado entre o Ministério da Cultura e a CONTRATADA.

6.6.6. Cada profissional a serviço da CONTRATADA deverá estar ciente de que a estrutura computacional do órgão não poderá ser utilizada para fins particulares, sendo que quaisquer ações que tramitem em sua rede poderão ser auditadas.

6.6.7. São requisitos exigidos para CONTRATADA com relação a sigilo e segurança da informação:

- I. 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.
- II. Obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pelo órgão;
- III. Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse do órgão ou de terceiros de que tomar conhecimento em razão da execução do objeto desta contratação, devendo orientar seus empregados nesse sentido.

6.6.8. 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.

6.6.9. 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.

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

6.6.11. Os profissionais, se necessário, 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.

6.6.12. Deverá acatar e obedecer às normas de utilização e segurança das instalações do Ministério da Cultura.

6.6.13. Promover o afastamento, no prazo máximo de vinte e quatro (24) horas após o recebimento da notificação, de qualquer dos seus funcionários que não correspondam aos critérios de confiança ou que perturbe a ação da equipe de fiscalização do órgão.

6.6.24. Responsabilizar pelos materiais, produtos, ferramentas, instrumentos e equipamentos disponibilizados para a execução dos serviços, não cabendo ao órgão qualquer responsabilidade por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer.

6.6.25. Não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, do órgão.

6.6.26. Manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas à política de segurança adotada pelo órgão e as configurações de hardware e de softwares decorrentes.

6.6.27. Não efetuar, sob nenhum pretexto, a transferência de qualquer responsabilidade da CONTRATADA para outras entidades, seja fabricantes, técnicos, subempreiteiros, etc.

6.6.28. Executar todos os testes de segurança necessários e definidos na legislação pertinente;

6.6.29. Garantir o cumprimento:

- I. Dos normativos vigentes editados pelo Gabinete de Segurança Institucional (GSI/PR) sobre Segurança da Informação, bem como, suas atualizações e demais normativos complementares, encontrados em: <https://www.gov.br/gsi/pt-br/assuntos/dsi>.
- II. Dos normativos internacionais de boas práticas da família ISO/IEC 27000, em especial, quanto às normas ABNT NBR ISO/IEC 27001:2013; 27002:2013; e, 27005:2019;
- III. De boas práticas do Center for Internet Security (CIS) e do *National Institute of Standards and Technology* (NIST), a critério do Ministério de Cultura
- IV. Das diretrizes da Lei Geral de Proteção de Dados – LGPD (Lei Federal nº 13.709/18).

6.6.30. Promover a implementação de controles de segurança da informação conforme as práticas dispostas nos normativos citados.

6.6.31. A execução dos serviços de forma remota, fora das dependências do órgão, é permitida, desde que cumpridas as diretrizes de segurança estabelecidas pelo MinC.

6.6.32. Na hipótese dos colaboradores da CONTRATADA trabalharem remotamente, os seguintes requisitos devem ser cumpridos:

- I. Todo acesso ao ambiente do Ministério da Cultura deve ser realizado por meio do ambiente corporativo da CONTRATADA, considerando os mecanismos de segurança obrigatórios pontuados neste item;
- II. Os colaboradores devem ser capacitados quanto às boas práticas de segurança da informação, não excluindo as certificações exigidas neste Termo de Referência;
- III. A CONTRATADA deve prover recursos suficientes e com a adequada segurança para seus colaboradores.

6.6.33. Prospectar e implementar soluções de segurança da informação aplicando, sempre que possível, um modelo de segurança *Zero Trust*.

6.6.34. Definir, apresentar e executar processo de gestão de riscos de segurança da informação nos ambientes gerenciados sob sua responsabilidade técnica.

6.6.35. Garantir a rastreabilidade das ações realizadas nos ambientes gerenciados sob sua responsabilidade técnica, mantendo trilhas de auditoria de segurança da informação.

6.7. Requisitos de Arquitetura Tecnológica

6.7.1. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da Contratante.

6.7.2. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela Contratante. Caso não seja autorizada, é vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela Contratante.

6.7.3. A arquitetura tecnológica, especificações e peculiaridades da solução consta assentada no “Anexo I – Caderno de Especificações Técnicas”.

6.8. Requisitos de Projeto e de Implementação

6.8.1. A CONTRATADA deverá alimentar e manter atualizada toda a documentação gerada em decorrência da execução do contrato, inclusive rotinas e relatórios técnicos e gerenciais.

6.8.2. Para execuções de tarefas, mesmo quando não especificadas nas atividades, a CONTRATADA deverá contemplar todos os processos necessários para garantir a execução das atividades relacionadas à manutenção da operacionalidade de ambientes computacionais, como a análise de viabilidade, aplicação das boas práticas, implementação e migração dos recursos, criação de documentação técnica, operacional e de análise e controle, execução de rotinas proativas e reativas, análise de desempenho, monitoramento e operação dos serviços.

6.8.3. Com vista a mitigar riscos de descontinuidade de serviços e de dependência técnica pelo órgão, a CONTRATADA se compromete a habilitar equipe de técnicos do órgão ou outra por ele indicada no uso das soluções implantadas no escopo deste contrato, repassando todo o conhecimento necessário para tal.

6.8.4. Todo processo, serviço, base de dados, aprendizado e afins produzidos em decorrência da prestação dos serviços deverá gerar documentação técnica por parte da contratada e que será de propriedade do Ministério da Cultura.

6.9. Requisitos de Implantação

6.9.1. Observar o estabelecido no “Anexo I – Caderno de Especificações Técnicas”.

6.9.2. Antes do início da prestação dos serviços deverá ser estabelecido o conjunto de procedimentos e scripts de atendimento que serão adotados, contendo o detalhamento das atividades na operação dos equipamentos e execução dos serviços do Ministério da Cultura. Este documento deverá apresentar os procedimentos para cada equipamento ou serviço.

6.9.3. A CONTRATADA deverá apresentar processo de disponibilização da solução para os ambientes de produção (e outros) para aprovação prévia do Ministério da Cultura.

6.9.4. O Ministério da Cultura poderá propor alterações nos procedimentos estabelecidos a qualquer tempo, com o objetivo de melhorar o desempenho dos equipamentos e dos sistemas.

6.9.5. A frequência de aferição da Medição de Resultados do Monitoramento será mensal e as metas deverão ser apuradas para os períodos compreendidos entre o primeiro e o último dia de cada mês.

6.10. Requisitos de Garantia e Manutenção

6.10.1. Garantia de Execução

6.10.1.1. O adjudicatário, no prazo de 5 (cinco) dias após a assinatura do Termo de Contrato, prestará garantia no valor correspondente a 5% (cinco por cento) do valor do Contrato, que será liberada de acordo com as condições previstas neste Edital, conforme disposto no art. 18, inciso III, da Lei nº 14.133/21, desde que cumpridas as obrigações contratuais.

6.10.2. Garantia dos serviços

6.10.2.1. O prazo de garantia contratual dos serviços, complementar à garantia legal, será de, no mínimo, seis (6) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto. O término do contrato não cessará a garantia do serviço.

6.10.2.2. Durante o prazo de garantia do serviço, a CONTRATADA deverá manter canal de comunicação por telefone, e-mail ou sistema.

6.10.2.3. As demandas de serviços em garantia serão realizadas por meio de reabertura de ordem de serviço na qual houve serviço prestado que implica em reexecução em garantia. Os prazos de execução a serem considerados são os constantes da respectiva ordem de serviço.

6.10.2.4. A não observância do prazo para atendimento do serviço sob garantia implica na execução das penalidades cabíveis estabelecidas em contrato.

6.10.2.5. Os serviços executados em garantia deverão ser documentados e encaminhados ao órgão.

6.10.2.6. Dentro do período de garantia, a correção de erros identificados nas soluções entregues pela CONTRATADA deverá ser efetuada sem qualquer ônus para o órgão, seja financeiro ou de atraso na prestação de outros serviços, salvo, se comprovadamente, os erros tenham se dado em razão das especificações feitas pelo Ministério da Cultura.

6.10.2.7. Durante todo o período de execução dos serviços, a CONTRATADA é obrigada a manter, em base histórica, os dados sobre a execução de serviços em garantia.

6.10.2.8. A Contratada deve assegurar e responsabilizar-se pela continuidade do fornecimento dos serviços contratados, e o seu monitoramento conforme os Níveis Mínimos de Serviço exigidos – o que inclui a necessidade de cumprir tempos de resposta a incidentes e de soluções de problemas nos ambientes gerenciados.

6.10.2.9. A Contratada também responderá pela reparação dos danos causados ao Ministério da Cultura e/ou a terceiros devido aos defeitos nos serviços ocasionados em razão de sua ação ou omissão. Os serviços executados como garantia não serão remunerados.

6.10.2.10. A CONTRATADA deverá fornecer garantia e suporte para os itens contemplados nesta contratação

6.11. Requisitos de Experiência Profissional e Formação da Equipe

6.11.1. Para a execução do objeto da pretensa contratação, considera-se necessário que a equipe técnica da CONTRATADA satisfaça alguns requisitos de experiência profissional. Dadas a complexidade do serviço a ser prestado e o nível de conhecimento exigido para as atividades afetas a tecnologia da informação, é intuitivo afirmar que maior grau de experiência irá resultar em melhores níveis de serviços prestados. É possível ainda que se observe ganhos de produtividade, com consequente redução de custos, e não incorrer no consagrado "paradoxo lucro-incompetência" (Acórdão 1.558/2003-TCU-Plenário).

6.11.2. A responsabilidade pelo dimensionamento do quantitativos, qualitativo e dos perfis técnicos, administrativos, operacionais de profissionais para o planejamento e execução antes e durante a execução dos serviços eventuais é integralmente da CONTRATADA, considerando a especificação de atividades a serem realizadas na manutenção preditiva, preventiva, construtiva, evolutiva.

6.11.3. A definição da composição e dos perfis dos profissionais de referência das equipes da Contratada que manterão relacionamento direto com o Ministério da Cultura serão estabelecidos nos requisitos específicos de cada item da pretensão contratual no Termo de Referência.

6.11.4. No levantamento do “Catálogo de Serviço” foi identificado o perfil profissional responsável para cada uma das atividades, sendo possível uma estimativa da quantidade de profissionais para sua execução, que servirá de referência para as licitantes.

6.11.5. Os serviços contratados deverão ser prestados por técnicos devidamente capacitados nas tecnologias e serviços em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

6.11.6. O modelo de serviço prevê a necessidade de perfis profissionais em 2 (dois) diferentes níveis de especialização, a saber:

CBO de Referência	Perfis Profissionais	Descrição e Experiência Profissional
1425-25	Gerente de Projetos em Segurança da Informação	Nível Superior em Tecnologia da Informação, experiência em gestão de projetos de segurança da informação - mínimo de 5 anos.
2123-20	Especialista em Cibersegurança	Experiência em implementação e operação de projetos de Segurança da Informação. Certificações obrigatórias – equipe (*): - 02 certificados em Segurança da Informação. Como exemplo: EXIN, ISO, ISC2, dentre outros. (*) todas essas certificações deverão ser comprovadas pela CONTRATADA, deverão existir profissionais em seu quadro de colaboradores como condição de assinatura do CONTRATO.
<p>- O Gerente de Projetos em Segurança da Informação será responsável por liderar a implementação das soluções em cada grupo de itens contratados.</p> <p>- O Especialista em Cibersegurança será responsável pela Implementação, configuração e operação da solução de gerenciamento dos itens contratados, as atividades a serem executadas.</p>		

6.12. Requisitos de Metodologia de Trabalho

6.12.1. A metodologia de trabalho será baseada no conceito de delegação de responsabilidade, onde o Ministério da Cultura é responsável pela gestão e fiscalização do contrato e pela atestação da aderência aos padrões de qualidade exigidos, e a CONTRATADA como responsável pela execução dos serviços e gestão dos seus recursos humanos.

6.12.2. A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante.

6.12.3. A OS indicará o serviço, a quantidade e a localidade na qual os serviços deverão ser prestados.

6.12.4. A execução do serviço deve ser acompanhada pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

6.12.5. A CONTRATADA deverá executar os serviços seguindo os processos, padrões e procedimentos indicados pelo órgão.

6.12.6. Todas as atividades devem estar de acordo com as especificações e melhores práticas dos fabricantes dos equipamentos/software e com as recomendações de organizações padronizadoras do segmento, desde que não entrem em conflito com os padrões, procedimentos e documentação definidos pelo órgão.

6.12.7. Também, no que couber, na execução dos serviços a CONTRATADA deve manter observância às políticas, regulamentações, especificações técnicas e orientações definidos pelos padrões de GOVERNO.

6.13. Requisitos complementares

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

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

6.13.3. Quando aplicável, o provedor da solução deverá realizar transferência de conhecimentos tecnológicos para usuários internos e/ou equipe técnica do requisitante nas soluções entregues, conforme definição, sem custo adicional, a fim de garantir a necessária independência do requisitante em relação ao provedor. Essa transferência se dará ao longo dos projetos, através do repasse de toda documentação e código-fonte da solução produzida, pelo menos quando entregue em ambiente de produção, ou quando for mais conveniente para o requisitante, principalmente quando o repasse de conhecimento for necessário para a homologação da entrega.

6.13.4. 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:

- I. Eficiência: Atendimento pleno às necessidades de negócio da Ministério da Cultura aumentando a disponibilidade e garantindo qualidade e segurança da Infraestrutura Tecnológica;
- II. Eficácia: Subsidiar a gestão de identidades e o controle de acesso aos recursos e serviços e Tecnologia da Informação do Ministério da Cultura que couberem ao projeto;
- III. Otimização de custos: Contratação de uma solução que atenda às necessidades pagando efetivamente pelo uso e produção;
- IV. Visibilidade: Apoiar a gestão fornecendo completa visibilidade no acesso aos recursos da Ministério da Cultura;
- V. 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.

6.14. Caderno de Especificações Técnicas

6.14.1. O detalhamento de cada item que faz parte da solução a ser adquirida deverá constar em documento "Anexo I – Caderno de Especificações Técnicas".

7. Estimativa da demanda - quantidade de bens e serviços

7.1. A presente seção contém o registro do quantitativo estimado de bens e serviços necessários para a composição da solução a ser contratada, de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo.

7.1.1. Busca-se descrever também os métodos, metodologias e técnicas de estimativas que foram utilizados, nos termos do:

- I. inciso I do art. 11 da Instrução Normativa SGD/ME Nº 94, DE 23 de dezembro de 2022;
- II. "Modelo de Contratação de Software e de Serviços de Computação em Nuvem" em sua seção "7.3.3. Dimensionamento", definido pela Portaria Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

7.1.2. Para o dimensionamento da demanda, foi efetuado o estudo de informações de forma a contemplar os seguintes levantamentos de dados.

7.2. Inventário de hardware e software: levantamento de todos os servidores e estações de trabalho em uso no ambiente do Ministério da Cultura.

7.2.1. A tabela seguir mostra o quantitativo de computadores a ser utilizado por nossos colaboradores:

Descrição	Quantidade
Desktop	966
Notebook	73
Total	1039

7.2.2. Sendo um total de mil e trinta e nove dispositivos distribuídos nas sedes do MinC.

7.2.3. A respeito dos servidores, verificou-se que atualmente o Ministério da Cultura possui sete (07) Servidores físicos virtualizando um total de duzentos e noventa e dois (292) servidores virtuais, distribuídos da seguinte forma:

Unix	Windows	Total de Servidores
230	62	292

7.2.4. Ressalta-se que os quantitativos supracitados são estimados com base nas informações coletadas do sistema de inventário, porém o parque computacional encontra-se em processo de adaptação para a recriação do Ministério da Cultura o que envolve procedimentos de revisão de ambientes e criação de novos ambientes de forma rotineira, desta forma os números foram levantados para proporcionar uma análise do percentual dos Sistemas operacionais em uso no âmbito do Ministério da Cultura.

7.2.5. Para o levantamento do volume de licenças necessárias para os servidores virtuais é necessário identificar as características dos servidores físicos existentes no Datacenter do Ministério da Cultura, conforme ilustrado no quadro a seguir.

CARACTERÍSTICAS DOS SERVIDORES FÍSICOS					
Tipo	Modelo	SO	Socket	Cores	Total Cores
Servidor Físico	DELL Power Edge R940	Datacenter	4	24	96
Servidor Físico	DELL Power Edge R940	Datacenter	4	24	96
Servidor Físico	DELL Power Edge R940	Datacenter	4	24	96
Servidor Físico	DELL Power Edge R940	Datacenter	4	24	96
Servidor Físico	DELL Power Edge R720	Standard	2	8	16
Servidor Físico	DELL Power Edge R710	Standard	2	4	16
Servidor Físico	DELL Power Edge R710	Standard	2	4	16
TOTAL DE SOCKETS			22		
TOTAL DE CORES					432

7.2.6. Projeção de crescimento: Considerando o crescimento futuro do Ministério da Cultura e a expansão do ambiente de TI, foi realizado o estudo do aumento esperado no número de servidores e estações de trabalho ao longo deste e dos dois próximos exercícios, uma vez que é possível adotar uma Ata de Registro de preços com vigência de 1 (um) ano renovável por igual período.

7.2.7. Desta forma, além das quantidades de estações de trabalho e servidores em produção, foram considerados outras informações conforme ilustradas no quadro a seguir:

EQUIPAMENTOS EM PRODUÇÃO	QUANT.	PREVISÃO DE CRESCIMENTO		QUANTIDADE DE RECURSOS A SEREM LICENCIADOS PARA COMPOSIÇÃO DO REGISTRO DE PREÇOS
		AÇÃO	ADICIONAL	
Estação de trabalho tipo desktop	966	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	1266
Estação de trabalho do tipo notebook	73	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	153
Smartphones institucionais	30	Aquisição de smartphones para uso de autoridades do Ministério da Cultura e para os escritórios estaduais durante o exercício corrente e o próximo exercício (2025).	250	280
Servidores de rede (Físicos)	8	Aquisição de servidores de rede para a ampliação/renovação do parque de servidores do Ministério da Cultura para o próximo exercício (2025). * a atualização será por meio de substituição e equipamentos obsoletos não havendo portanto, a ampliação da quantidade atualmente em produção	4	7
		previsão de ampliação da quantidade de servidores virtuais para a implantação de		

Servidores de rede (virtuais)	292	clusters e ambientes de alta disponibilidade para a ampliação /renovação do parque de servidores do Ministério da Cultura até o próximo exercício (2025).	28	320
Servidores de Armazenamento de Dados	03	Considerando que forma instalados recentemente 02 equipamentos novos e que estes possuem capacidade de expansão de discos, não há necessidade de aquisições de outros equipamentos do tipo para os próximos 03 (três) anos	0	03

7.2.8. Após os levantamentos ilustrados no quadro supracitado, de modo a prever margem de segurança para os quantitativos levantados e ainda, considerando a possibilidade da implementação de salas de treinamento no CTA_v e o uso de outras estações de trabalho em outras unidades, verifica-se oportuno e razoável que seja realizado um acréscimo de 10% aos totais calculados.

7.3. Inventário de Sistemas, Banco de Dados e Contas de Usuários

7.3.1. O Ministério da Cultura Desenvolve, Mantém e Suporta Sistemas para uso interno, de outros Órgão e da Sociedade Civil.

7.3.2. Em números gerais, são apresentados um panorama acerca dos sistemas na Tabela a seguir.

Tipo	Quantidade
Aplicações WEB	99
Solução de BI	01
Banco de Dados (SGBD)	44

7.3.3. Neste quantitativo estão sistemas críticos e não críticos. Das mais diversas finalidades de uso no cotidiano do MinC.

7.3.4. Não há um sistema único de autenticação que contemple todos os sistemas. Alguns destes funcionam com login realizado por um (01) servidor de controlador de domínio *Microsoft Active Directory*.

7.3.5. Com dados coletados a partir da ferramenta de gestão do *Microsoft Active Directory* foram constatadas, na data de 10 de setembro de 2024, as informações no quadro a seguir.

Tabela. Previsão de Crescimento

QUANTIDADE ATUAL DE USUÁRIOS	Ação	Adicional	TOTAL NO FINAL DO 1º SEMESTRE 2025
	PROCESSO SELETIVO SIMPLIFICADO PARA		

1695	CONTRATAÇÃO TEMPORÁRIA - EDITAL PSS /MINC Nº 1, DE 13 DE MAIO DE 2024 - PROCESSO SEI/MinC Nº 01400.011599/2024-42	99	1794
------	---	----	------

7.3.6. Estes são os usuários aptos utilizar estações de trabalho, rede de computadores e sistemas institucionais, a exemplo do Sistema Eletrônico de Informações (SEI)/MinC.

7.3.7. No MinC é utilizada a suíte de produtividade e correio eletrônico Microsoft Office 365. Da qual existem mil quatrocentos e noventa e uma (1491) licenças em uso.

7.3.8. Vale ressaltar que a quantidade de computadores e contas no diretório de usuários não necessariamente coincide com a quantidade de licenças MS Office a medida que estas não estão disponíveis para todos os servidores /colaboradores.

7.3.9. No que diz respeito a contas com acesso privilegiado, estima-se que existam aproximadamente oitenta (80) contas no Ministério da Cultura.

7.3.10. 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.

7.3.11. De forma que a equipe de planejamento da contratação considerou razoável a adoção dos quantitativos estimados conforme ilustrados na Tabela a seguir.

7.3.12. Utilizando o levantamento realizado, a equipe de planejamento apresenta o quantitativo necessário para cada um dos itens previstos.

Grupo	Item	Descrição	Unidade	Qtde.
01	1	Subscrição para solução de segurança para identidades e acessos - Logon único adaptativo para identidades dos usuários.	Usuários	1800
	2	Subscrição para solução de segurança para identidades e acessos - Autenticação multifator adaptativa para identidades dos usuários.	Usuários	1800
	3	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	Usuários	100
	4	Subscrição para solução de Segurança para Armazenamento de Credenciais.	Usuários	1900
	5	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Servidores Windows.	Servidor	70
	6	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Servidores Linux/Unix.	Servidor	250

	7	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Estações de Trabalho.	Estação de Trabalho	1800
	8	Subscrição para solução de segurança para identidades e acessos - Proteção para Aplicações Containerizadas.	Cluster	01
	9	Subscrição para solução de segurança para identidades e acessos - Proteção para Aplicações.	Aplicação	100
	10	Serviços de Instalação e Configuração das Soluções (por item / módulo)	Serviço	09
	11	Serviço de treinamento / capacitação (por item / módulo)	Turma	09
02	12	Serviço de acesso remoto confiança zero (ZTNA)	Usuários	400
	13	Serviço de acesso seguro interno /externo (SWG)	Usuários	1800
	14	Serviços de Instalação e Configuração das Soluções (por item / módulo)	Serviço	02
	15	Serviço de treinamento / capacitação (por item / módulo)	Turma	02

8. Levantamento de soluções

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 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.

8.1.1. Existem várias opções de soluções as quais são possíveis se considerar para atender às necessidades de um órgão da administração pública federal. Assim, se faz importante observar Critérios para Seleção, a exemplo de:

- Conformidade e Segurança
- Funcionalidades e Integração
- Escalabilidade e Desempenho
- Usabilidade e Experiência do Usuário

- Suporte e Manutenção

8.2. Gestão de Identidade

8.2.1. Quanto a análise de disponibilidade de solução similar no portal do software público.

8.2.1.1. Por meio da pesquisa realizada não foram identificadas soluções de softwares públicos que atenda a essa necessidade.

8.2.1.2. Palavras-chave utilizadas na pesquisa Gestão de Identidade, SSO, IAM, PAM, MFA, autenticação. (Fonte: https://softwarepublico.gov.br/social/search/software_infos)

8.2.2. Quanto a disponibilidade de solução no Catálogo de Soluções de TI da SGD.

8.2.2.1. Por meio de consulta junto ao portal, não foi identificada a existência de Catálogo de Soluções de TIC contendo acordo de plataforma ou solução similar para o objeto em estudo.

8.2.2.2. Também não foi encontrado projeto similar no Cronograma de Projetos.

8.2.2.3. Fonte: <https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic>

8.2.3 Quanto a uso em outros órgãos públicos similares.

8.2.3.1. A equipe de planejamento da contratação buscou junto ao mercado, contratações, com as seguintes características: Escopo similar ao objeto, similaridades de requisitos negociais e tecnológicos, publicados recentemente e que foram atendidos com as soluções de mercado identificadas neste estudo técnico.

8.2.3.2. Necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas/ Contratações Similares.

ÓRGÃO	PREGÃO	DESCRIÇÃO
Superintendência Estadual de Licitações - SUPEL/RO	820/2021	Solução de Gerenciamento de Acessos Privilegiados (<i>Privileged Access Management - PAM</i>)
Agência Nacional de Telecomunicações - ANATEL	25/2021	Solução de PAM (Gerenciamento de Acesso Privilegiado) e Solução de auditoria de serviços Microsoft
Conselho da Justiça Federal - CJF	37/2021	Solução, serviços e transferência de conhecimento
Ministério Público do Distrito Federal e Territórios - MPDFT	72/2021	Solução, serviços e transferência de conhecimento
UNIFAP	15/2020	Solução de Segurança da informação para Sistemas Críticos com Monitoramento Comportamental, Repositório Seguro, Proteção de Aplicações dentro ou fora de containers, Proteção para Servidores e Estações de Trabalho, entre outros

CADE	08/2018	Contratação de soluções de gerenciamento de identidade, gerenciamento de acessos privilegiados e correlacionamento de eventos, provendo ao Conselho Administrativo de Defesa Econômica - CADE
Tribunal Superior do Trabalho	58/2021	Registro de preços para aquisição de soluções de segurança, auditoria e prevenção de ameaças.
Tribunal Superior Eleitoral	02/2022	Registro de preços para eventual aquisição de Solução de Gerenciamento de Acessos Privilegiados para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos), com capacidade para armazenar, proteger, controlar, gerenciar, auditar e monitorar o acesso privilegiado incluindo serviço de instalação e transferência de conhecimento, consoante especificações, condições, quantidades e prazos constantes do Termo de Referência - Anexo I do Edital.

8.2.4. Disponibilidade de solução disponível no mercado

8.2.4.1. Nesta seção, pretende-se apresentar os aspectos relacionados ao mercado fornecedor, apontando suas principais características e especificidades relacionadas às compras de governo nesse segmento.

8.2.4.2. O Segmento de soluções de gerenciamento de identidades e acessos compreende um tipo de objeto de extrema relevância para proteção do ambiente tecnológico. Esse segmento de mercado é amplo e possui diversos fabricantes de soluções que podem ser capazes de atender à demanda identificada pela área requisitante, com funcionalidades e modelos distintos.

8.2.4.3. Foram identificadas algumas ferramentas gratuitas e/ou open-source (software livre) para o contexto das soluções, mas, durante análise técnica, elas se mostraram insuficientes para atender a demanda. Seja pela falta de funcionalidades, compatibilidade com requisitos técnicos necessários para o atendimento das demandas ou por requererem demasiado esforço técnico-operacional para customização, dessa forma, foi concluído que há vantagem para a Administração se as soluções descritas sejam adquiridas nos moldes deste estudo, que para este fim não foram identificadas ferramentas gratuitas/públicas que atendessem a necessidade deste Ministério.

8.2.4.4. Um ponto crítico para o sucesso deste projeto é que as revendas das soluções tenham capacidade de entregar os serviços solicitados para o perfeito funcionamento do software.

8.2.4.5. Dessa forma, foi identificada uma grande quantidade de revendas com capacidade e aptidão de fornecer o objeto e prestar os serviços técnicos especializados exigidos e necessários, foram consideradas as seguintes premissas para esta análise:

- I. Os bens e serviços que compõem a solução pretendida são do segmento de segurança da informação.
- II. Desta forma, apenas soluções que sejam capazes de monitorar e controlar identidades são capazes de atender plenamente as necessidades identificadas.
- III. Com objetivo de viabilizar a maior participação de fabricantes e garantir a ampla concorrência concluímos que o processo deve considerar a possibilidade das revendas ofertarem soluções tecnologias compostas por múltiplos fabricantes.

8.2.4.6. A equipe de planejamento seguiu uma ordem lógica, que permitiu registrar todo o esforço empreendido até a escolha da solução que atende a demanda de forma mais eficiente.

8.2.4.7. Em primeiro lugar, a equipe de planejamento buscou entender o objeto junto ao segmento de mercado. Posteriormente, buscou avaliar as alternativas que se encontram disponíveis e por fim buscou avaliar qual o melhor modelo de fornecimento do objeto, que atende às necessidades de forma mais eficiente.

8.2.4.8. Diante dos argumentos apresentados, esta equipe de planejamento da contratação entende que a plataforma tecnológica objeto do presente estudo deve ser baseada nos pilares tecnológicos elencados a seguir.

8.2.4.9. Essa orientação tem como objetivo o direcionamento correto das características fundamentais da solução de modo a permitir a contratação de solução de segurança para gerenciamento de identidades e acesso, dos integrantes do SISP.

- **Segurança para identidades**: Administração de identidades de tipos internos e externos, incluindo serviços de sincronização de diretórios e identidades, autoatendimento de usuários, incluindo interfaces administrativas e de usuário final para registro de usuários, gerenciamento de senhas, gerenciamento de perfis e administração delegada, métodos de autenticação de usuário, incluindo autenticação multifator (MFA) e SSO e recursos de análise, incluindo relatórios históricos, logs e informações de análise de identidade sobre eventos de acesso de administração e tempo de execução
- **Gerenciamento e proteção para contas privilegiadas com gerenciamento de sessões (PASM)**: As contas privilegiadas devem ser protegidas com o cofre de suas credenciais e o acesso a essas contas é então intermediado para usuários humanos, serviços e aplicativos por meio da ferramenta PAM. As funções de gerenciamento de sessão privilegiada (PSM) estabelecem sessões, geralmente com injeção de credenciais e gravação de sessão completa. As senhas e outras credenciais, como certificados e tokens para contas privilegiadas, são gerenciadas ativamente (por exemplo, sendo alternadas em intervalos definíveis ou na ocorrência de eventos específicos). Opcionalmente, as soluções PASM também podem fornecer gerenciamento de senha de aplicativo para aplicativo (AAPM) e/ou recursos de acesso remoto privilegiado sem instalação para equipe de TI externa e terceiros que não exigem uma VPN.
- **Gerenciamento e proteção de elevação e delegação de privilégios (PEDM)**: Os agentes baseados em host no sistema gerenciado concedem privilégios específicos a usuários conectados. As ferramentas PEDM fornecem controle de comando baseado em host (filtragem), controles de permissão/negação/isolamento de aplicativos e/ou elevação de privilégios, o que permite que processos específicos sejam executados com um nível mais alto de privilégios. As ferramentas PEDM devem ser executadas no sistema operacional real (no nível do kernel ou do processo). O controle de comando por meio de filtragem de protocolo é explicitamente excluído dessa definição porque o ponto de controle é menos confiável. As ferramentas PEDM também podem opcionalmente fornecer controles de aplicativos e recursos de monitoramento de integridade de arquivos. As ferramentas PEDM são frequentemente um requisito obrigatório para indústrias regulamentadas e onde a conformidade com PCI-DSS, SOX e outros controles regulatórios e financeiros são estipulados. Ambientes de defesa e governo também exigem a remoção de privilégios de administrador local.
- **Gerenciamento e proteção de segredos**: Credenciais (como senhas, tokens OAuth e chaves SSH) e segredos para software e máquinas são gerenciados, armazenados e recuperados programaticamente por meio de APIs e SDKs. A confiança é estabelecida e intermediada com a finalidade de trocar segredos e gerenciar autorizações e funções relacionadas entre diferentes entidades não humanas, como máquinas, contêineres, aplicativos, serviços, scripts, processos e pipelines de DevSecOps. O gerenciamento de segredos é frequentemente usado em ambientes dinâmicos e ágeis, como IaaS, PaaS e plataformas de gerenciamento de contêineres. Os produtos de gerenciamento de segredos também podem fornecer AAPM.

- **Identificação das soluções:**

8.2.4.10. Foram identificadas algumas soluções open-source (softwares livres) para o objeto proposto, tais como: Kleycloak e OpenIAM, contudo em função de não contemplar todas as funcionalidades almejadas, incompatibilidade com alguns requisitos técnicos necessários para o atendimento das demandas e principalmente pela ausência de suporte técnico, essas soluções não foram incluídas no comparativo de soluções viáveis, por considerar que o suporte técnico de um fabricante nos assuntos relacionados a segurança da informação é de suma importância para a administração.

8.2.4.11. Observando-se as necessidades e os requisitos tecnológicos elencados nesse estudo técnico, bem como a análise do mercado, realizamos o levantamento das soluções relacionadas ao gerenciamento de identidades e acesso e apresentamos uma descrição sucinta de cada uma delas.

ID SOLUÇÃO	NOME DA SOLUÇÃO
01	Delinea
02	Microsoft
03	Cyberark
04	Google
05	OpenText
06	Beyond Trust
07	Senha Segura

- **Solução de Mercado 01 - Delinea:** O "Account Lifecycle Manager" ajuda a gerenciar a proliferação de contas de serviço e permite que você gerencie e controle essas contas com fluxos de trabalho e provisionamento automatizado, governança, conformidade e capacidades de descomissionamento. Ainda possui às soluções Delinea Privileged Behavior Analytics, Connection Manager, Server Suite, Cloud Suite, Privilege Manager, Cloud Access Controller. (Fonte: <https://delinea.com/products/account-lifecycle-manager>)
- **Solução de Mercado 02 - Microsoft:** Protege o acesso de qualquer identidade, em qualquer lugar, à IA, aos aplicativos e aos recursos no local e nas nuvens com uma solução unificada de identidade e acesso à rede. O fabricante Microsoft possui a solução na sua suite de Identity and Access Management o Azure AD Premium P2 e o Azure AD Privileged Identity Management. (Fonte: <https://www.microsoft.com/pt-br/security/business/solutions/identity-access>)
- **Solução de Mercado 03 - Cyberark:** A plataforma de segurança de identidade da CyberArk permite acesso seguro para qualquer identidade — humana ou máquina — a qualquer recurso ou ambiente de qualquer lugar, utilizando qualquer dispositivo. Possui a solução Cyberark Workforce Identity - Single Sign-On, Adaptive Multi-Factor Authentication, Directory Services, Endpoint Authentication, App Gateway, User Behavior Analytics e Secure Web Sessions, Privileged Access Manager, DevSecOps e Endpoint Privilege Manager. (Fonte: <https://www.cyberark.com/products/>)

- Solução de Mercado 04 - Google: Uma plataforma unificada de gerenciamento de identidades, acessos, apps e endpoints (IAM/EMM). O fabricante possui a solução Google Cloud Identity Premium - Multi-Factor Authentication, Endpoint management, Single Sign-On. (Fonte: <https://cloud.google.com/identity?hl=pt-BR>)
- Solução de Mercado 05 - Opentext: O "Identity Manager" é uma suíte abrangente de gestão de identidade. Ele fornece uma estrutura de identidade inteligente que aproveita seus ativos de TI existentes e novos modelos de computação, como Software como Serviço (SaaS), reduzindo custos e garantindo conformidade em ambientes físicos, virtuais e em nuvem. O fabricante possui as soluções NetIQ Access Manager e Privileged Access Manager, Risk Service e Self-service Password Reset. (Fonte: <https://www.netiq.com/documentation/identity-manager-48/>)
- Solução de Mercado 06 – Beyond Trust: O fabricante Beyond Trust possui as soluções Password Safe e Privilege Management. Afirma que a plataforma oferece visão completa de todas as identidades, privilégios e acessos para revelar pontos cegos e bloquear ataques em todo o seu ambiente de identidades. (Fonte: <https://www.beyondtrust.com/pt>)
- Solução de Mercado 07 - Senha Segura: O Senha Segura possui as soluções Account and Session PAM Core, Domum acesso remoto, Endpoint PAM Senha Segura Go. Oferece um conjunto abrangente de recursos de PAM. A plataforma PAM se integra perfeitamente a várias tecnologias e sistemas, garantindo acesso. (Fonte: <https://senhasegura.com/pt-br>)

8.2.4.12. Todo o “estudo dos requisitos tecnológicos” foi considerado para a definição dos "ANEXO I - Caderno de Especificações Técnicas) para atender as necessidades deste Ministério.

8.2.4.13. Diante dos levantamentos realizados na pesquisa apresentada acima, pode-se observar que existem diversas soluções presentes no mercado para atender a demanda do Ministério da Cultura.

8.3. Controle de Acesso (ZTNA e SWG)

Selecionar a solução adequada dependerá das necessidades específicas do Ministério da Cultura, incluindo requisitos de segurança, orçamento e infraestrutura existente.

8.3.1 Quanto a análise de disponibilidade de solução similar no portal do software público.

8.3.1.1 Por meio da pesquisa realizada não foram identificadas soluções de softwares públicos que atenda a essa necessidade.

8.3.1.2. Palavras-chave utilizadas na pesquisa Gestão de Acesso, Controle de Acesso, ZTNA, SWG, Acesso remoto. (Fonte: https://softwarepublico.gov.br/social/search/software_infos)

8.3.2. Quanto a disponibilidade de solução no Catálogo de Soluções de TI da SGD.

8.3.2.1. Por meio de consulta junto ao portal, não foi identificada a existência de Catálogo de Soluções de TIC contendo acordo de plataforma ou solução similar para o objeto em estudo.

8.3.2.2. Também não foi encontrado projeto similar no Cronograma de Projetos.

8.3.2.3. Fonte: <https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic>

8.3.3. Quanto a uso em outros órgãos públicos similares.

8.3.3.1. A equipe de planejamento da contratação, mais uma vez, buscou junto ao mercado, contratações, com as seguintes características: Escopo similar ao objeto, similaridades de requisitos negociais e tecnológicos, publicados recentemente e que foram atendidos com as soluções de mercado identificadas neste estudo técnico.

8.3.3.2. Verifica-se que há a prática de contratação destes serviços de subscrição de licenças por outros órgãos conforme exemplos listados a seguir.

ÓRGÃO	PREGÃO	DESCRIÇÃO
Agência Nacional de Transportes Terrestres - ANTT	24/2023	Registro de Preços para eventual contratação de plataforma integrada para proteção de usuários e visibilidade da superfície estendida de ataques, com resolução contínua de vulnerabilidades e priorização e correlação dos eventos de segurança, conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.
MINISTÉRIO DAS COMUNICAÇÕES - MCOM	10/2023	Contratação de Solução integrada de Segurança Cibernética, contando com gestão de vulnerabilidade, defesa cibernética, resposta incidentes de segurança, incluindo os serviços de segurança da informação especializados em sustentação e implementação de soluções de cibersegurança,
Postal Saúde	09/2023	Contratação de plataforma única para segurança e controle de acesso à internet, aplicações SaaS e privadas, contemplando monitoramento constante da experiência do usuário

8.3.4. Disponibilidade de solução disponível no mercado

8.3.4.1. Por meio de consulta aos portais dos fabricantes de soluções de gestão de identidade, foram encontradas as seguintes informações de fabricantes de soluções disponíveis no mercado.

ID SOLUÇÃO	NOME DA SOLUÇÃO
01	ZScaler
02	CloudFlare
03	Fortinet
04	Palo Alto Network
05	NetSkope
06	Forcepoint

- Solução de Mercado 01: Zscaler: Zscaler Private Access (ZPA) é uma solução ZTNA baseada em nuvem que oferece acesso seguro a aplicativos internos sem expor a rede à internet. Utiliza a abordagem de confiança zero para fornecer conexões seguras entre usuários e aplicativos. Zscaler Internet Access (ZIA) é uma plataforma SWG de segurança em nuvem que oferece proteção abrangente contra ameaças web, inspeção SSL e filtragem

de conteúdo para garantir uma navegação segura. Baseado em nuvem, segurança web abrangente, inspeção SSL, proteção contra ameaças avançadas. (Fonte: <https://www.zscaler.com.br/products-and-solutions>)

- **Solução de Mercado 02: Cloudflare:** A solução ZTNA verifica e protege o acesso de funcionários e terceiros em todos os seus aplicativos auto-hospedados, SaaS e não web, ajudando a mitigar riscos e garantir uma experiência do usuário tranquila. Ele verifica o contexto granular, como a identidade e a postura do dispositivo, para cada solicitação, fornecendo acesso rápido e confiável em toda a sua empresa. Já a solução SWG visibilidade de aproximadamente 20% da web, a escala de rede incomparável da Cloudflare protege a navegação dos funcionários na internet e bloqueia ameaças que causam violações. Simplifique a criação e auditoria de políticas com categorias predefinidas. (Fonte: <https://www.cloudflare.com/pt-br/zero-trust/products/>)
- **Solução de Mercado 03: Fortinet:** A Solução ZTNA proporciona acesso seguro e controlado a aplicativos internos e em nuvem, aplicando os princípios de segurança de Zero Trust. A solução é projetada para substituir VPNs tradicionais, oferecendo uma abordagem mais segura e eficiente para o acesso remoto. O SWG oferece proteção abrangente contra ameaças da web, controle de conteúdo e políticas de acesso para proteger os usuários durante a navegação na internet. A solução é projetada para garantir uma navegação segura, prevenindo acessos a sites maliciosos e protegendo contra malware e outras ameaças online. (Fonte: <https://www.fortinet.com/br/solutions/enterprise-midsize-business/unified-sase>)
- **Solução de Mercado 04: Palo Alto Networks:** Uma plataforma de segurança em nuvem que fornece acesso seguro e escalável a aplicativos e dados corporativos. Integra-se com outras soluções de segurança da Palo Alto Networks para uma proteção abrangente. Abordagem unificada de segurança, integração com outros produtos Palo Alto, proteção abrangente. (Fonte: <https://www.paloaltonetworks.com.br/sase>)
- **Solução de Mercado 05: Netskope:** Projetada para fornecer acesso seguro e contínuo a aplicativos internos, sem a necessidade de VPNs tradicionais. Utiliza a abordagem de confiança zero para garantir que apenas usuários e dispositivos autorizados possam acessar recursos específicos. Solução baseada em nuvem que oferece segurança abrangente para navegação na web e uso de aplicativos na nuvem. Proporciona visibilidade e controle sobre o tráfego web, protegendo contra ameaças cibernéticas e garantindo conformidade com as políticas de segurança. Facilita implementação e escalabilidade sem necessidade de hardware adicional. Minimiza o impacto na produtividade dos usuários. (Fonte: <https://www.netskope.com/pt/products/ztna-next> <https://www.netskope.com/pt/products/next-gen-swg>)
- **Solução de Mercado 06: Forcepoint:** Oferece acesso seguro a aplicativos internos e na nuvem, eliminando a necessidade de VPNs tradicionais. Baseada nos princípios do modelo de segurança de Zero Trust, a solução garante que o acesso seja concedido apenas a usuários e dispositivos autenticados e autorizados. Fornece proteção contra ameaças avançadas e análise de comportamento para identificar e mitigar riscos. Oferece políticas granulares de controle de acesso e filtragem de conteúdo. Análise de comportamento, proteção contra ameaças avançadas, políticas granulares de controle de acesso. (Fonte: <https://www.forcepoint.com/product/ztna-zero-trust-network-access> e <https://www.forcepoint.com/product/forcepoint-one-web-security>)

8.3.4.2. Diante dos levantamentos realizados na pesquisa apresentada acima, pode-se observar que existem diversas soluções presentes no mercado para atender a demanda do Ministério da Cultura.

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. Em relação às possibilidades em alinhamento ao inciso II do art. 11 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, tem-se que:

- a. O Software Público brasileiro não atende o objeto desta contratação.
- b. As políticas, os modelos e os padrões da arquitetura e-PING de Interoperabilidade de Governo Eletrônico não se aplicam nessa contratação, visto que o objeto não abrange serviços disponibilizados pelo governo eletrônico que trabalham conjuntamente com interação e troca de informações.
- c. Não há necessidade de adequação do ambiente do Ministério da Cultura para viabilizar a execução contratual

9.3. Viabilidade de adesão a uma ata de registro de preços: Considerando que há vários produtos disponíveis no mercado e ainda considerando que as contratações de soluções similares são frequentemente realizadas por Órgãos Federais, cabe a realização de pesquisa quanto a disponibilidade de uma Ata de Registro de Preços vigente para adesão, desde que atenda aos requisitos demandados por este estudo.

9.4. Entende-se que uma análise comparativa se torna viável e necessária visto que há possibilidades de atendimento à necessidade, dessa forma deve-se considerar que a solução para os serviços listados não dispõe de outra solução de maneira que estamos partindo como primeira contratação para atender às necessidades já elencadas.

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

- A. Contratação de subscrição de licença software (Software as a Service - SaaS);
- B. Licenciamento por Aquisição/Perpétuo;
- C. Solução gratuita e/ou open-source (Software Livre)

9.5. Assim, considerando as opções apresentadas, são apresentadas as análises referentes às Necessidade de Negócio e Tecnológicas.

9.5.1. Para as Necessidades de Negócio

Necessidades de Negócio	Soluções		
	A	B	C
Redução da complexidade dos acessos: É possível eliminar a necessidade de que os colaboradores mantenham uma grande quantidade de senhas diferentes, que normalmente são esquecidas. Por meio de uma solução de gestão de acessos, é possível realizar a integração de sistemas, simplificando o processo e, ao mesmo tempo, ampliando o controle da TI.	Atende	Atende	Atende
Hierarquização das permissões: O trabalho da TI em controlar os privilégios de cada tipo de funcionário aos ambientes é reduzido. Por meio de um sistema de gestão centralizado, você pode construir uma hierarquização de permissões de forma que cada colaborador tenha acesso apenas ao necessário.	Atende	Atende	Atende

Automação e centralização da administração: A TI perde muito tempo revendo o privilégio de acesso dos funcionários para garantir que cada um visualize apenas o permitido. Portanto, é possível automatizar todo o processo, eliminando a conta de colaboradores que deixam a organização, por exemplo. Ademais, todo o controle passa a ser feito em um único painel, simplificando a gestão para a TI.	Atende	Atende	Atende
Acesso remoto seguro: Garante que os colaboradores possam acessar os recursos de forma segura, independentemente da localização.	Atende	Atende	Atende
Prevenção contra malware e ataques cibernéticos: Como órgão do governo, o Ministério da Cultura pode ser alvo de ataques cibernéticos por diferentes motivos, incluindo espionagem, roubo de informações ou interrupção de serviços, desta forma espera-se que a solução ajude a prevenir infecções por malware e ataques de ransomware, protegendo os dispositivos e a rede contra ameaças cibernéticas. Mitigando dentre outros riscos, os associados a ameaças internas, limitando o acesso dos usuários apenas ao necessário para suas funções.	Atende	Atende	Não Atende
Conformidade regulatória: Considerando que o Ministério da Cultura esta sujeito a regulamentações específicas relacionadas à proteção de dados e segurança da informação, espera-se que a Gestão de Contas e Acessos possa ajudar a garantir a conformidade com essas regulamentações, fornecendo recursos de segurança necessários para limitar o acesso indevido aos dados e sistemas contra violações.	Atende	Atende	Atende
Transferência de conhecimento: A solução deverá ter ainda em sua composição um item para treinamento, para garantir que ocorra a transferência do conhecimento para os servidores e colaboradores que atuam na infraestrutura de TI do MinC.	Atende	Atende	Não Atende
Implementação assistida: Todos os serviços de instalação e configuração deverão ser executados pela CONTRATADA, de modo a não sobrecarregar a equipe de servidores e colaboradores do MinC, porém as atividades deverão ser acompanhadas pelos servidores e colaboradores que atuarão na operação da solução após entregue pela CONTRATADA.	Atende	Atende	Não Atende
Escalabilidade: A implantação de uma solução eficiente de Gestão de Identidades e Gestão de Acessos torna-se ainda mais crucial com o crescimento do Órgão. A necessidade de acompanhar o aumento do número de usuários, dispositivos e aplicativos, bem como a manutenção e possível ampliação do trabalho remoto por meio do Programa de Gestão do Desempenho (PGD). Assim, solução escolhida deve ser capaz de acompanhar a expansão do Órgão e se adaptar às novas demandas de segurança, garantindo que todos os acessos sejam devidamente controlados e protegidos.	Atende	Atende	Atende
Resultado da Análise	Atende	Atende	Não Atende

9.5.2. Necessidades Tecnológicas para Soluções de Gestão de Identidade

	Soluções		
Necessidades Tecnológicas	A	B	C
Proteção das Informações:			

<ul style="list-style-type: none"> Proteção das informações sensíveis e confidenciais contra acessos não autorizados. Implementação de medidas de segurança contra ataques cibernéticos. Criptografia de dados em repouso e em trânsito. 	Atende	Atende	Atende
<p>Conformidade e Governança:</p> <ul style="list-style-type: none"> Atender às exigências das legislações e normas aplicáveis, como LGPD, Lei de Acesso à Informação, e outras. Ferramentas de verificação de conformidade com regulamentos e normas. Implementação de políticas de conformidade e governança de identidade. Capacidade de gerar relatórios de conformidade para auditorias e revisões regulatórias. 	Atende	Atende	Atende
<p>Gestão de Identidades e Acessos:</p> <ul style="list-style-type: none"> Gestão completa do ciclo de vida da identidade, desde a criação até a desativação. Controles específicos para a gestão de acessos privilegiados. Implementação e gestão de políticas de acesso baseadas em funções e riscos. Automação do provisionamento e desprovisionamento de usuários e recursos. Abranger todos os tipos de acessos e identidades Gestão de permissões e perfis de acesso, inclusive os privilegiados. Controle de acesso baseado em função (RBAC) e em atributos (ABAC). Capacidade de proteção de identidades não humanas em plataformas de containerização 	Atende	Atende	Atende
<p>Eficiência Operacional:</p> <ul style="list-style-type: none"> Melhorar a eficiência operacional através da automação de processos de gestão de identidade e acesso. Integração com LDAP, Active Directory, e outros diretórios. Suporte para integração com sistemas legados e aplicações modernas (via APIs, conectores, etc.). Integração com serviços de nuvem e ambientes híbridos. Capacidade de suportar um grande número de usuários e transações. Suporte técnico contínuo e atualizações regulares. 	Atende	Atende	Atende
<p>Monitoramento e Auditoria:</p> <ul style="list-style-type: none"> Possibilitar o controle e auditoria dos acessos aos sistemas e dados da instituição. Relatórios detalhados de acessos e atividades dos usuários. Prover registros de uso de privilégios e trilhas de auditoria Capacidade de auditoria completa e geração de logs. 	Atende	Atende	Atende
<p>Segurança Avançada:</p> <ul style="list-style-type: none"> Suporte para autenticação multifator (Multiple Factor Authentication - MFA). Autenticação baseada em riscos e contexto. 	Atende	Atende	Atende
<p>Usabilidade e Experiência do Usuário:</p> <ul style="list-style-type: none"> Interface intuitiva e amigável. Portais de autosserviço para usuários e administradores. Autosserviço para redefinição de senhas. 			

<ul style="list-style-type: none"> Políticas de complexidade e expiração de senhas. Portal de Login Único Seguro para aplicações (SSO, Single Sign-On Seguro) Gestão de senhas de aplicações de negócio que não suportam Single Sign-On (login único) 	Atende	Atende	Atende
<p>Flexibilidade e Customização:</p> <ul style="list-style-type: none"> Capacidade de personalização para atender às necessidades específicas da instituição. Suporte para workflows personalizados de aprovação de acesso. 	Atende	Atende	Não Atende
<p>Infraestrutura de Identidade:</p> <ul style="list-style-type: none"> Repositório centralizado de identidades. Alta disponibilidade e resiliência. 	Atende	Atende	Não Atende
Resultado da Análise	Atende	Atende	Não Atende

9.5.3. Necessidades Tecnológicas para Soluções de Gestão de Acesso (ZTNA e SWG)

Necessidades Tecnológicas	Soluções		
	A	B	C
<p>Segurança de Acesso Remoto:</p> <ul style="list-style-type: none"> Proteção das informações sensíveis e confidenciais contra acessos não autorizados. Autenticação contínua e baseada em contexto, verificando a identidade do usuário e a integridade do dispositivo. Implementação de autenticação multifator (MFA) para acesso seguro a aplicativos e dados internos. 	Atende	Atende	Não Atende
<p>Proteção contra Ameaças da Web:</p> <ul style="list-style-type: none"> Bloqueio de sites maliciosos e prevenção de downloads perigosos. Filtragem de conteúdo e políticas de acesso para proteger os usuários durante a navegação na internet. Proteção contra ameaças da web, como malware, phishing e ataques de dia zero. 	Atende	Atende	Não Atende
<p>Visibilidade e Monitoramento:</p> <ul style="list-style-type: none"> Monitoramento contínuo das atividades na web, fornecendo visibilidade completa do tráfego. Relatórios detalhados das atividades de navegação dos usuários. Capacidade de auditoria completa e geração de logs. 	Atende	Atende	Não Atende
Conformidade e Governança:			

<ul style="list-style-type: none"> • Atender às exigências das legislações e normas aplicáveis, como LGPD, Lei de Acesso à Informação, e outras. • Ferramentas de verificação de conformidade com regulamentos e normas. • Capacidade de gerar relatórios de conformidade para auditorias e revisões regulatórias. 	Atende	Atende	Não Atende
<p>Gestão de Acessos:</p> <ul style="list-style-type: none"> • Implementação e gestão de políticas de acesso baseadas em funções e riscos. • Controle de acesso granular que garante que os usuários acessem apenas os recursos necessários para suas funções. • Automação do provisionamento e desprovisionamento de acessos. 	Atende	Atende	Não Atende
<p>Monitoramento e Auditoria:</p> <ul style="list-style-type: none"> • Possibilitar o controle e auditoria dos acessos aos sistemas e dados da instituição. • Monitoramento contínuo das atividades dos usuários e dispositivos. • Capacidade de auditoria completa e geração de logs detalhados. 	Atende	Atende	Não Atende
<p>Eficiência Operacional:</p> <ul style="list-style-type: none"> • Melhoria da eficiência operacional através da automação de processos de acesso. • Integração com sistemas de gestão de identidade (IDM) e outras infraestruturas existentes. • Suporte técnico contínuo e atualizações regulares. • Centralização da gestão das políticas de segurança web. • Integração com outros sistemas de segurança e infraestrutura existente. • Interface intuitiva e amigável para administração. 	Atende	Atende	Não Atende
<p>Segurança Avançada:</p> <ul style="list-style-type: none"> • Implementação de medidas de segurança contra-ataques cibernéticos, como detecção de anomalias, resposta a incidentes e inspeção SSL/TLS. • Criptografia de dados em trânsito para proteger as comunicações durante a navegação na web, bem como entre dispositivos e aplicativos. • Suporte para padrões de segurança como SAML, OAuth, OpenID Connect. 	Atende	Atende	Não Atende
<p>Escalabilidade e Desempenho:</p> <ul style="list-style-type: none"> • Capacidade de suportar muitos usuários e transações. • Alta disponibilidade e resiliência. • Desempenho otimizado para minimizar latências e garantir uma experiência de usuário positiva. 	Atende	Atende	Não Atende
<p>Flexibilidade e Customização:</p> <ul style="list-style-type: none"> • Capacidade de personalização para atender às necessidades específicas da instituição. • Suporte para workflows personalizados de acesso e políticas de segurança. 	Atende	Atende	Não Atende
Resultado da Análise	Atende	Atende	Não Atende

9.6. Considerando, ainda, as informações elencadas no quadro supracitado, de imediato identificamos que as alternativas atendem os requisitos básicos. Dessa maneira além desses quesitos iremos prosseguir na análise dos demais pontos.

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

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

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

9.8. Considerando que ambas as soluções em estudo possuem possibilidade de atender a demanda, verifica-se a necessidade de avaliar os cenários relacionados aos tipos de licenciamentos praticados no mercado, conforme foram elencados os pontos positivos e negativos a seguir:

9.8.1. Licenciamento Perpétuo:

- **Pontos Positivos:**
 - **Custo Único:** O pagamento é feito uma vez, e a solução pode ser usada indefinidamente, o que pode ser mais econômico a longo prazo, especialmente para organizações que planejam usar a solução por muitos anos.
 - **Propriedade Permanente:** A organização possui a licença permanentemente, o que pode proporcionar maior controle sobre os custos e o ciclo de vida da solução.
 - **Flexibilidade:** Pode ser mais flexível em termos de implantação e integração com outras ferramentas de segurança, pois não está vinculado a um contrato de assinatura.
- **Pontos Negativos:**
 - **Custo Inicial Elevado:** O custo inicial de aquisição pode ser significativamente maior do que o licenciamento anual ou por subscrição, o que pode ser um desafio para esta Pasta, além disso corre-se o risco de haver um pagamento por produtos que não sejam necessários depois de algum tempo, caso ocorra uma redução do parque ou migração de soluções
 - **Atualizações e Suporte:** Normalmente, o suporte e as atualizações estão disponíveis por um período limitado após a compra inicial, e podem exigir custos adicionais para estender esses serviços.
 - **Menos Flexibilidade de Atualização:** Pode ser mais difícil e caro atualizar para versões mais recentes da solução, pois pode exigir a compra de atualizações ou migrações adicionais.

9.8.2. Licenciamento Anual/ Subscrição por doze (12) meses:

- **Pontos Positivos:**
 - **Custo Anual Previsível:** O custo é distribuído ao longo do tempo, facilitando o planejamento financeiro e eliminando o alto custo inicial associado ao licenciamento perpétuo.
 - **Atualizações e Suporte Incluídos:** Geralmente inclui suporte técnico e atualizações de software durante o período da licença, garantindo que a solução esteja sempre atualizada.
 - **Maior Flexibilidade:** Permite uma maior flexibilidade para ajustar o número de licenças conforme as necessidades da organização mudam ao longo do tempo.

- Pontos Negativos:
 - **Custo Total a Longo Prazo:** Pode ser mais caro a longo prazo do que o licenciamento perpétuo, especialmente se a solução for usada por muitos anos.
 - **Dependência Contínua:** A organização fica continuamente dependente do fornecedor para suporte e atualizações, e a interrupção do pagamento pode resultar na perda de acesso à solução.
 - **Falta de Propriedade:** A organização não possui a licença permanentemente e pode perder o acesso à solução se não renovar a licença anualmente.

9.9. Considerando que ambas as soluções em estudo possuem possibilidade de atender a demanda, após a análise dos tipos de licenciamentos praticados no mercado, esta equipe de planejamento da contratação, **entende razoável a escolha da contratação de subscrição de licenças por doze (12) meses.**

10. Registro de soluções consideradas inviáveis

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

10.2. SOLUÇÃO B: Licenciamento por Aquisição/Perpétuo

10.2.1. A proposta dessa alternativa representa a modalidade de licenciamento em que se adquire de forma vitalícia a solução de software.

10.2.1.1. Nesta modalidade o Contratante adquire as licenças de software de forma perpétua, porém verifica-se como prática que não há o fornecimento perpétuo das atualizações das licenças, ou seja, mesmo que se tenha as licenças perpétuas, necessitam de atualizações, para que funcionem de forma correta, neste sentido os riscos de: dependência de um único fornecedor; Limitação da concorrência quando da análise de renovações contratuais, tornam este tipo de licenciamento inviável.

10.2.1.2. Neste sentido, as características do modelo de licenciamento por aquisição é extremamente rígido e não permite modificações.

10.2.2. Resumidamente, nesse tipo de contratação, há o risco de aquisição de licenças e de serviços agregados, que podem ser ou não utilizados, afetando com isso a economicidade da contratação, além de gerar gastos com produtos não utilizados, uma vez que essas licenças são pagas de forma antecipada e na modalidade à vista. Nesse sentido, trecho do entendimento esposado pelo TCU, no Acórdão 2569/2018 – Plenário, no qual recomenda a aquisição de licenças pontuais que atendam a demanda do órgão, visando a redução dos riscos na contratação, senão vejamos:

“...adquiram quantitativo de licenças estritamente necessário, vedando-se o pagamento antecipado por licenças de software, vinculando o pagamento dos serviços agregados às licenças efetivamente utilizadas, principalmente em projetos considerados de alto risco ou de longo prazo, nos quais o quantitativo deve ser atrelado à evolução do empreendimento, e devidamente documentado nos estudos técnicos preliminares, podendo ser utilizado o Sistema de Registro de Preço, que viabiliza o ganho de escala na compra ao mesmo tempo que proporciona a aquisição no momento oportuno”

10.2.3. Desta forma conclui-se que a presente alternativa é tecnicamente inviável.

10.3. SOLUÇÃO C: Solução gratuita e/ou open-source (Software Livre)

10.3.1. Não há disponibilidade de solução de software livre capaz de Software Livre atender aos requisitos técnicos nesse contexto. Esta solução apresenta alta complexidade, pois necessita de capacitação permanente da equipe de informática, falta de suporte técnico, baixa. Assim, esta opção está aos poucos sendo substituída por ferramentas pagas com suporte, gerenciamento unificado e garantia de funcionamento.

11. Análise comparativa de custos (TCO)

11.1. Para realização deste TCO, realizou-se pesquisa de preço seguindo as orientações contidas na Caderno de Logística – Pesquisa de Preços 2024 e na INSTRUÇÃO NORMATIVA SEGES /ME Nº 65, DE 7 DE JULHO DE 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

11.2. Conforme definido no Caderno de Logística – Pesquisa de Preços 2024, a pesquisa de preços deverá ser realizada diretamente no sistema Compras.gov.br. Visto isso, foi gerado a Pesquisa de Preços nº 111/2024.

11.2.1. Ademais, **o Relatório Pesquisa de Preço nº 111/2024 (SEI/MinC nº 2082617) apresenta detalhes sobre a Pesquisa de Preço realizada** como parte integrante do planejamento da contratação em questão.

11.2.2. Informações referentes à **Pesquisa de Preços Públicos** e, consequentemente, aderência aos parâmetros do artigo 5º, incisos I e II, da IN SEGES/ME nº 65/2021, são apresentadas no Relatório de Pesquisa de Preço

11.3. Pesquisa de Preços com Fornecedores de Solução

11.3.1. Para a definição do valor estimado da contratação foram utilizados os parâmetros do art. 5º, inciso IV, da IN SEGES/ME nº 65/2021, a citar: *"pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital;"*.

11.3.2. Na consulta direta com fornecedores, foi enviada comunicação às empresas enumeradas no "APÊNDICE A - Lista de fornecedores consultados", do Relatório de Pesquisa de Preço citada na seção 11.2.

11.3.3. As escolhas das empresas relacionadas se deu a partir de uma lista de contatos resultante de reuniões e apresentações acerca de soluções realizadas ao longo dos últimos doze (12) meses.

11.3.4. As empresas que responderam à solicitação de Pesquisa de Preço, estão listadas e enumeradas por ordem alfabética, bem como os valores e produtos. As informações referentes às propostas recebidas são apresentadas no Relatório de Pesquisa de Preço, Anexo a este estudo.

11.4. Pesquisa de Preços utilizando Catálogo de Soluções de TIC com Condições Padronizadas

11.4.1. Não foi encontrado Catálogo em questão em pesquisa junto à Secretaria de Governo Digital do Ministério da Economia (SGD).

11.5. Metodologia para obtenção do preço estimado

11.5.1. Em uma análise inicial a partir dos preços encontrados, foram utilizadas 3 metodologias de análise, a saber: Média Simples, Mediana e Menor Preço.

11.5.2. A obtenção do preço estimado deu-se **com base no menor dos valores obtidos** na pesquisa de preços, em razão da concordância com:

Art. 6º, § 4º Os preços coletados devem ser analisados de forma crítica, em especial, quando houver grande variação entre os valores apresentado

11.5.3. Na pesquisa realizada, foram recebidas nove (9) propostas de diferentes empresas. Destas, cinco apresentaram propostas para o Grupo 01 e quatro empresas apresentaram propostas para o Grupo 02.

11.5.4. Considerando os métodos estatísticos média simples e mediana como já citado, bem como a observação do menor preço nas respostas recebidas, a Tabela a seguir apresenta os resultados.

Grupo	Item	Descrição	Unidade	Qtde.	Valor Unitário / 12 meses (Valores em R\$)		
					Mediana	Média	Menor
1	1	Subscrição para solução de segurança para identidades e acessos - Logon único adaptativo para identidades dos usuários.	Usuários	1800	R\$615,00	R\$ 629,15	R\$ 601,29
	2	Subscrição para solução de segurança para identidades e acessos - Autenticação multifator adaptativa para identidades dos usuários.	Usuários	1800	R\$ 702,83	R\$ 712,24	R\$ 697,30
	3	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	Usuários	100	R\$ 8.204,00	R\$ 8.244,94	R\$ 7.913,32
	4	Subscrição para solução de Segurança para Armazenamento de Credenciais.	Usuários	3800	R\$ 413,70	R\$ 413,73	R\$ 397,06
	5	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Servidores Windows.	Servidor	70	R\$ 1.740,00	R\$ 1.754,71	R\$ 1.702,89
	6	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Servidores Linux/Unix.	Servidor	250	R\$ 1.730,21	R\$ 1.727,02	R\$ 1.683,43
	7	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Estações de Trabalho.	Estação de Trabalho	1800	R\$ 378,29	R\$ 378,84	R\$ 357,94
	8	Subscrição para solução de segurança para identidades e acessos - Proteção para Aplicações Containerizadas.	Cluster	01	R\$ 370.057,53	R\$ 362.038,49	R\$ 315.108,00

2	9	Subscrição para solução de segurança para identidades e acessos - Proteção para Aplicações.	Aplicação	100	R\$ 5.647,70	R\$ 5.807,42	R\$5.344,31
	10	Serviços de Instalação e Configuração das Soluções (por item / módulo)	Serviço	11	R\$ 108.766,59	R\$ 115.589,31	R\$ 97.580,00
	11	Serviço de treinamento / capacitação por (item / módulo)	Turma	11	R\$ 130.280,00	R\$ 130.631,23	R\$ 125.000,00
	12	Serviço de acesso remoto confiança zero (ZTNA)	Usuário	800	R\$ 1.148,75	R\$ 1.155,89	R\$ 958,00
2	13	Serviço de acesso seguro interno/externo (SWG)	Usuário	3700	R\$ 1.960,60	R\$ 2.146,81	R\$ 1.766,06
	14	Serviços de Instalação e Configuração das Soluções (por item / módulo)	Serviço	4	R\$ 264.034,50	R\$ 258.802,80	R\$ 208.035,00
	15	Serviço de treinamento / capacitação (por item / módulo)	Turma	4	R\$ 283.861,70	R\$ 284.203,10	R\$ 282.350,00

11.5.6. Considerando os valores unitários exibidos, a Tabela a seguir consolida os valores totais da propensa contratação para 12 meses.

Grupo	Item	Descrição	Unidade	Qtde.	Valor Total / 12 meses (Valores em R\$)		
					Mediana	Média	Menor
1	1	Subscrição para solução de segurança para identidades e acessos - Logon único adaptativo para identidades dos usuários.	Usuários	1800	R\$ 1.107.000,00	R\$ 1.132.470,00	R\$ 1.082.322,00
	2	Subscrição para solução de segurança para identidades e acessos - Autenticação multifator adaptativa para identidades dos usuários.	Usuários	1800	R\$ 1.265.094,00	R\$ 1.282.032,00	R\$ 1.255.140,00
	3	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	Usuários	100	R\$ 820.400,00	R\$ 824.494,00	R\$ 1.582.664,00
	4	Subscrição para solução de Segurança para Armazenamento de Credenciais.	Usuários	3800	R\$ 1.572.060,00	R\$ 1.572.174,00	R\$ 1.508.828,00
	5	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Servidores Windows.	Servidor	70	R\$ 121.800,00	R\$ 122.829,70	R\$ 119.202,30
	6	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Servidores Linux/Unix.	Servidor	250	R\$ 432.552,50	R\$ 431.755,00	R\$ 420.857,50
	7	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Estações de Trabalho.	Estação de Trabalho	1800	R\$ 680.922,00	R\$ 681.912,00	R\$ 644.292,00
	8	Subscrição para solução de segurança para identidades e acessos - Proteção para Aplicações Containerizadas.	Cluster	01	R\$ 370.057,53	R\$ 362.038,49	R\$ 315.108,00
	9	Subscrição para solução de segurança para identidades e acessos - Proteção para Aplicações.	Aplicação	100	R\$ 564.770,00	R\$ 580.742,00	R\$ 534.431,00
	10	Serviços de Instalação e Configuração das Soluções (por item / módulo)	Serviço	11	R\$ 1.196.432,49	R\$ 1.271.482,41	R\$ 1.073.380,00

	11	Serviço de treinamento / capacitação por (item / módulo)	Turma	11	R\$ 1.433.080,00	R\$ 1.436.943,53	R\$ 1.375.000,00
2	12	Serviço de acesso remoto confiança zero (ZTNA)	Usuário	800	R\$ 919.000,00	R\$ 924.712,00	R\$ 766.400,00
	13	Serviço de acesso seguro interno /externo (SWG)	Usuário	3700	R\$ 7.254.220,00	R\$ 7.943.197,00	R\$ 6.534.422,00
	14	Serviços de Instalação e Configuração das Soluções (por item / módulo)	Turma	4	R\$ 1.056.138,00	R\$ 1.035.211,20	R\$ 832.140,00
	15	Serviço de treinamento / capacitação (por item / módulo)	Turma	4	R\$ 1.135.446,80	R\$ 1.136.812,40	R\$ 1.129.400,00
TOTAL					R\$ 20.749.373,32	R\$ 21.563.332,71	R\$ 19.173.586,80

11.5.7. Após a realização de pesquisa de preços em conformidade com a IN SEGES/ME nº 65/2021, certifica-se que o preço estimado para a presente contratação é compatível com os praticados no mercado.

11.5.8. Em resumo, os valores são:

- A mediana gerou um valor total de R\$ 20.749.373,32 para a contratação.
- A média simples gerou um valor total de R\$ 21.563.332,71 para a contratação.
- O menor preço gerou um o valor total de R\$ 19.173.586,80 para a contratação.

11.9. Considerações finais

11.9.1. Por meio da análise dos resultados da pesquisa de preços é possível inferir que há mais de um fabricante capaz de atender a demanda e que não há exclusividade para a venda de qualquer um dos produtos dos fabricantes, fato que torna clara a viabilidade da realização de um pregão para a realização da licitação.

11.9.2. Tendo em vista o fato de que não foram identificados valores com discrepância relevante entre as propostas encaminhadas, verifica-se viável a **adoção do menor valor** obtido na pesquisa, R\$ 19.173.586,80 (**dezenove milhões, cento e setenta e três mil, quinhentos e oitenta e seis reais e oitenta centavos**), como o valor a ser adotado para a estimativa de custos para a contratação pleiteada.

12. Descrição da solução de TIC a ser contratada

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

12.2. Portanto, diante das análises qualitativa e quantitativa realizadas ao longo do presente estudo técnico preliminar, constata-se a condução de processo de contratação de uma solução no formato de serviço (SaaS / Subscrição), nos termos definidos pela Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

12.2.1. Neste sentido, no intuito de alcançar melhor conformidade com a Portaria SGD/MGI nº 5.950, verifica-se as seguintes condições:

- a) Vedada a inclusão de cláusula que direta ou indiretamente permita a cobrança retroativa de valores referentes a serviços de suporte técnico e de atualização de versões relativa ao período em que o órgão ou entidade tenha ficado sem cobertura contratual;

b) Vedada a inclusão de cláusula que direta ou indiretamente permita a cobrança de valores para reativação de serviços agregados;

c) Vedada a inclusão de cláusula que direta ou indiretamente permita a cobrança de valores relativos a serviço de correção de erros, inclusive retroativos, que devem ser corrigidos sem ônus à contratante, durante o prazo de validade técnica dos softwares, nos termos do Capítulo III da Lei nº 9.609, de 19 de fevereiro de 1998. Neste sentido, caso os erros venham a ser corrigidos em versão posterior do software, essa versão deverá ser fornecida sem ônus para a contratante; e

d) Vedada a inclusão de cláusula que direta ou indiretamente exija a contratação conjugada de serviços de suporte técnico e de atualização de versões, quando não houver a necessidade de ambos.

12.3. Desta forma deverá ser contratado os direitos de uso do software, de forma que o pagamento é realizado a partir do uso efetivo como identificada como uma das soluções. Esta modalidade de licenciamento ocorre por meio de uma assinatura para a locação de licenças de uso da solução de segurança cibernética.

12.4. Características positivas do modelo de licenciamento por subscrição:

1. Toda a necessidade atual e futura de licenças de software precisa estar descrita na formalização do contrato;
2. O pagamento é feito quando do aceite da entrega dos produtos em parcela única para a vigência de doze (12) meses;
3. O dimensionamento pode ser ajustado ao longo dos anos;
4. Qualquer atualização tecnológica já está contemplada neste modelo de licenciamento;
5. Todas as soluções tecnológicas disponíveis no modelo de licenciamento perpétuo também estão disponíveis para o modelo de subscrição;
6. O gasto no processo de assinatura é de custeio; e
7. Gestão simplificada.

12.5. De forma geral a Licenciamento por subscrição de uso de software, usualmente é menos onerosa para a Administração do que quando o bem é contratado como perpétuo.

12.5.1. Analisando as principais diferenças no modelo de licenciamento, a Alternativa B: Licenciamento por Aquisição/perpétuo, de certa forma, torna a Administração refém do fabricante durante o período contratado e após esse período. De maneira que o MinC tem a necessidade de adquirir o serviço de manutenção e suporte anual para garantir as atualizações e suporte ou mantém a solução em uso sem atualização e suporte ou, ainda, no limite, opta pelo desuso.

12.5.2. Um outro componente a ser considerado é que o prazo máximo de licenciamento no modelo perpétuo é de 60 (sessenta) meses e esse tempo é muito. Ao longo desse tempo o mercado pode mudar muito e essa solução passar a não ser mais a ideal em comparação à outras novas que porventura venham a entregar novas soluções, dessa forma o valor investido na compra da solução tende a ser perdido.

12.6. Neste sentido, observa-se nos pontos levantados que a escolha em adquirir as soluções de software no modelo perpétuo apresenta sérios riscos ao negócio, indo na contramão dos princípios balizadores das contratações públicas, quais sejam: eficiência, eficácia e economicidade.

12.7. Pelo exposto, é conveniente e/ou oportuna Contratação de serviço (SaaS / Subscrição), cujo modelo se notabiliza por pagar pelo serviço da licença durante o período que o MinC julgar necessário obtendo os benefícios e entregáveis planejados. Caso chegue o momento que determinada solução está defasada e/ou não faça mais sentido o MinC poderá deixar este licenciamento de lado visto que a contratação se dá por um modelo de prestação de serviços. Desta forma conclui-se que a presente alternativa é tecnicamente viável.

12.8. A demanda será atendida mediante a contratação de serviços e de subscrição de software contemplando-se o serviço de instalação, implantação dos softwares, garantia técnica e transferência de conhecimento necessários à

plena operação da solução. A execução dos serviços de planejamento, instalação e implantação da solução, bem como sua integração à rede e as alterações que ocorrerão no contexto do Projeto de Implementação, devem seguir o que está especificado nas etapas seguintes:

12.8.1. Etapa 01 - Planejamento e design da instalação a CONTRATADA deverá realizar uma ou mais reuniões técnicas com o corpo técnico designado pelo MinC com o objetivo de ser apresentada objetivamente ao Projeto de Serviços Gerenciados de Segurança proposto pelo MinC, devendo sinalizar quaisquer inviabilidades ou ajustes necessários, propondo as alternativas e/ou melhorias no projeto com o foco em viabilizar a implementação. Para cada reunião, deverão ser elaboradas atas para registro dos pontos abordados e consentimento global, que subsidiarão a próxima fase da dinâmica de execução. A CONTRATADA deverá entregar Documento de Instalação tomando como base todo o projeto apresentado pelo MinC e as abordagens registradas nas atas de reunião, contendo o plano de testes para validação do funcionamento pós-execução. Esse documento deverá ser entregue para avaliação e aprovação do MinC para execução dos serviços.

12.8.2. Etapa 02 - Execução dos serviços de instalação e configuração, a CONTRATADA deverá apoiar a instalação inicial e configurar a solução seguindo o Documento de Instalação e as Boas Práticas disponibilizadas pelos fabricantes da solução devidamente aprovado pelo MinC. As janelas de manutenção para execução dos serviços serão definidas pelo MinC podendo ocorrer em dias e horários que não coincidam com os horários comerciais tais como finais de semana, feriados e em janelas noturnas /madrugada.

12.8.2.1. A pretensa contratação dessa solução de tecnologia da informação deve prever o fornecimento e instalação de todos os insumos necessários para operacionalização da solução adquirida sem gerar custos adicionais para o MinC.

12.8.3. Etapa 03 - A CONTRATADA deverá realizar o plano de testes definido previamente, executando a correção de eventuais problemas encontrados, conforme cronograma aprovado de implantação.

12.8.4. Etapa 04 - A CONTRATADA deverá realizar uma sessão de transferência de conhecimento da solução de acordo com a seção "6.3. Requisitos de Capacitação" deste documento. Também deverá, após a implantação da solução, acompanhar os primeiros 30 (trinta) dias corridos o funcionamento da solução para correção imediata de eventuais problemas e, se for o caso, para realização de melhorias identificadas após a implantação. Por fim, deverá ainda realizar operação assistida nas primeiras 24 (vinte e quatro) horas corridas pós implementação da solução, corrigindo, quando necessário, eventuais problemas decorrentes da execução.

12.8.5. Etapa 05 - Elaboração e entrega da documentação (AS-BUILT) do ambiente instalado. A CONTRATADA deverá entregar ao MinC toda documentação necessária para identificação do ambiente instalado, descrevendo em detalhes todos os aspectos de configuração da solução. Passados os 30 (trinta) primeiros dias corridos da implantação da solução a CONTRATADA deverá disponibilizar suporte técnico na solução definido da seguinte forma (NMS):

ATIVIDADE	SLA DE ATENDIMENTO
Requisição de mudança para aplicação de patches e hotfixes de segurança	6 HORAS
Atualização de assinaturas (vacinas de vírus, bases de vulnerabilidades, etc.)	8 HORAS

12.9. Para a medição dos índices de nível de serviços, serão considerados os seguintes conceitos:

12.9.1. Problema: é a causa desconhecida de um ou mais incidentes ou os problemas são a causa de um ou mais incidentes;

12.9.2. Severidade: nível de prioridade/emergência atribuído ou solicitado para a realização de um atendimento a uma requisição do MinC ou do ambiente, conforme critérios descritos a seguir. Solicitações de alteração do nível de severidade poderão ser submetidas à CONTRATADA e, quando julgadas pertinentes pela mesma, serão prontamente atendidas.

- SEVERIDADE CRÍTICO: A Solução está totalmente parada ou inoperante;
- SEVERIDADE ALTO: A Solução está ativa, mas com inoperância da maioria de suas funcionalidades, causando um impacto negativo no ambiente de produção;
- SEVERIDADE MÉDIO: A Solução está operativa, mas suas funcionalidades são executadas com restrições;
- SEVERIDADE BAIXO: A Solução está operativa e a falha não compromete suas funcionalidades ou questões não tratadas pela documentação;
- SEVERIDADE AGENDADO: O atendimento está relacionado apenas a esclarecimentos de dúvidas ou necessidade de informações;

12.9.3. A cada chamado de suporte categorizado como Severidade Crítico ou Alto, o recurso humano designado para fornecer assistência deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante;

12.9.4. Referente aos chamados categorizados como Severidade Crítico ou Alto cabe ao fornecedor dar início, junto ao MinC, às providências que serão adotadas para a solução do chamado;

12.9.5. Para os chamados de suporte categorizado como Severidade Crítico ou Alto, o atendimento não pode ser interrompido até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados), de acordo com a disponibilidade do MinC.

Severidade	Descrição
Agendado	Esclarecimento de dúvidas ou similar.
Baixo	Sistemas operam sem impacto ao negócio.
Médio	Sistemas operam com degradação de desempenho.
Alto	Sistemas operam com paralisação parcial do ambiente.
Crítico	Sistemas inoperantes ou paralisação total do ambiente.

12.9.6. Tempo de Atendimento: O tempo máximo para INÍCIO de um ATENDIMENTO a uma requisição, incidente ou problema.

Severidade	Descrição	Tempo de Atendimento
Agendado	Esclarecimento de dúvidas ou similar	8 h
Baixo	Sistemas operam sem impacto ao negócio.	4 h

Médio	Sistemas operam com degradação de desempenho.	40 min
Alto	Sistemas operam com paralisação parcial do ambiente.	20 min
Crítico	Sistemas inoperantes ou paralisação total do ambiente.	10 min

12.9.7. Tempo de Solução: O tempo máximo para a SOLUÇÃO de um ATENDIMENTO a uma requisição, incidente ou problema. O tempo de solução poderá depender de fatores externos que deverão ser levados em conta durante a sua medição.

Severidade	Descrição	Tempo de Solução
Baixo	Sistemas operam sem impacto ao negócio.	2 dias
Médio	Sistemas operam com degradação de desempenho.	24h
Alto	Sistemas operam com paralisação parcial do ambiente.	12h
Crítico	Sistemas inoperantes ou paralisação total do ambiente.	6h

12.9.8. Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução;

12.9.9. Os chamados escalados para o fabricante e em tratamento por aquele não se encaixam nos prazos descritos.

12.9.10. Serão excluídos do cálculo, os tempos de paralisação, decorrentes dos seguintes eventos:

1. Falta de energia no local de prestação dos serviços;
2. Indisponibilidade da rede lógica do MinC;
3. Problemas derivados de ocorrências no ambiente do minC, onde comprovadamente a indisponibilidade não esteja sendo controlada pela CONTRATADA;
4. Ações necessárias para resolução de problemas que tenham sido autorizadas pelo MinC;
5. Indisponibilidade gerada pela operadora de telecomunicação responsável pelos links e equipamentos da rede do MinC;
6. Indisponibilidade gerada pela necessidade de reparo ou troca dos equipamentos da solução de segurança da informação da rede MinC, listadas na tabela do item 7 deste estudo técnico;
7. Fatores externos a prestação de serviços, desde que justificado e acordado com o time de segurança do MinC;
8. Indisponibilidade do ambiente virtualizado do MinC, infraestrutura computacional em que parte dos softwares que compõe a solução devem ser instalados;
9. Manutenções programadas pelo MinC;
10. Manutenções programadas pela CONTRATADA, desde que previamente autorizadas pelo MinC.

- 12.9.11.** Em um atendimento onde seja necessária uma janela para execução dos serviços solicitados, os tempos entre a necessidade do atendimento e janela de execução deverão ser excluídos.
- 12.9.12.** Entende-se que haverá uma fase inicial de transição e adequação dos processos de atendimento por parte da CONTRATADA. Sendo assim, os níveis de serviço (SLAs) não serão exigidos contratualmente durante os primeiros 30 (trinta) dias de duração do contrato. Os índices deverão ser apurados e apresentados ao MinC, no entanto, a CONTRATADA não estará sujeita a penalidades pelo seu descumprimento durante este período.

12.10. Caderno de Especificações Técnicas.

- 12.10.1.** O Caderno de Especificações Técnicas é o documento que detalha as condições e características dos serviços e portanto, caso haja informações neste Estudo Técnico Preliminar ou no Termo de Referência que contrariem as informações constantes no Caderno de Especificações Técnicas, deverão prevalecer as informações registradas no referido Caderno.
- 12.10.2.** O Caderno de Especificações Técnicas deverá constar anexo ao Edital.

13. Estimativa de custo total da contratação

Valor (R\$): 19.173.586,80

13.1. Diante do levantamento das informações por meio da pesquisa de preços, restou verificado que o custo para garantir os serviços pelo período de doze (12) meses é de **R\$ 19.173.586,80 (dezenove milhões, cento e setenta e três mil, quinhentos e oitenta e seis reais e oitenta centavos)**, conforme informações ilustradas na Tabela a seguir:

Grupo	Item	Descrição	Unidade	Qtde.	Valor Unitário (R\$)	Valor Total (R\$)
	1	Subscrição para solução de segurança para identidades e acessos - Logon único adaptativo para identidades dos usuários.	Usuários	1800	R\$ 601,29	R\$ 1.082.322,00
	2	Subscrição para solução de segurança para identidades e acessos - Autenticação multifator adaptativa para identidades dos usuários.	Usuários	1800	R\$ 697,30	R\$ 1.255.140,00
	3	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	Usuários	200	R\$ 7.913,32	R\$ 1.582.664,00
	4	Subscrição para solução de Segurança para Armazenamento de Credenciais.	Usuários	3800	R\$ 397,06	R\$ 1.508.828,00
	5	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Servidores Windows.	Servidor	70	R\$ 1.702,89	R\$ 119.202,30

1	6	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Servidores Linux/Unix.	Servidor	250	R\$ 1.683,43	R\$ 420.857,50
	7	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Estações de Trabalho.	Estação de Trabalho	1800	R\$ 357,94	R\$ 644.292,00
	8	Subscrição para solução de segurança para identidades e acessos - Proteção para Aplicações Containerizadas.	Cluster	01	R\$ 315.108,00	R\$ 315.108,00
	9	Subscrição para solução de segurança para identidades e acessos - Proteção para Aplicações.	Aplicação	100	R\$ 5.344,31	R\$ 534.431,00
	10	Serviços de Instalação e Configuração das Soluções (por item / módulo)	Serviço	11	R\$ 97.580,00	R\$ 1.073.380,00
	11	Serviço de treinamento / capacitação por (item / módulo)	Turma	11	R\$ 125.000,00	R\$ 1.375.000,00
2	12	Serviço de acesso remoto confiança zero (ZTNA)	Usuário	800	R\$ 958,00	R\$ 766.400,00
	13	Serviço de acesso seguro interno/externo (SWG)	Usuário	3700	R\$ 1.766,06	R\$ 6.534.422,00
	14	Serviços de Instalação e Configuração das Soluções (por item / módulo)	Turma	4	R\$ 208.035,00	R\$ 832.140,00
	15	Serviço de treinamento / capacitação (por item / módulo)	Turma	4	R\$ 282.350,00	R\$ 1.129.400,00
TOTAL						R\$19.173.586,80

14. Justificativa técnica da escolha da solução

14.1. Com relação aos requisitos técnicos, a solução foi especificada tanto para prover as funcionalidades mínimas para atendimento das necessidades de cibersegurança e infraestrutura tecnológica do MinC. Após análise técnica das soluções levantadas a subscrição e implantação se mostra a mais vantajosa do ponto de vista técnico.

14.2. A especificação do objeto também considerou os critérios de sustentabilidade ambiental previstos no Decreto nº 7.746, de 05 de junho de 2012, da Casa Civil da Presidência da República, no que couber.

14.3. A escolha pela contratação, foi baseada na análise com mais vantajosidade dos aspectos técnicos e econômicos da solução, se mostrando ser a mais viável, quer sob a perspectiva técnica, econômica e, especialmente, sob a ótica da segurança da informação.

14.4. Uma vez que se busca uma solução que, além de garantir a economicidade, reduza a indisponibilidade e garanta a eficiência do serviço público, o licenciamento perpétuo de software não se configura como uma escolha tecnicamente e economicamente viável, tendo em vista os riscos apontados na análise da solução, seção 11 deste Estudo Técnico, bem como o fato de ser uma opção que usualmente é mais onerosa para a Administração do que quando o bem é contratado na modalidade Subscrição.

14.5. Pelas razões acima delineadas, pelo já exposto tecnicamente no seção 12 deste estudo técnico preliminar, o cenário escolhido, mostra-se incontestado, por esse motivo, esta equipe de planejamento declara viável a contratação para viabilizar o incremento da maturidade da Segurança da Informação e a melhoria dos recursos tecnológicos do MinC, descartando-se desde já as demais opções.

14.6. Características técnicas necessárias para ao atendimento da solução objeto desse estudo técnico seguem, de maneira detalhada, no anexo “Caderno de Especificações Técnicas” deste ETP.

15. Justificativa econômica da escolha da solução

15.1. Quanto a viabilidade de parcelamento da solução de TIC (Inciso I, § 2º, art. 12, da IN SGD/ME nº 94/2022), o parcelamento foi proposto bem como os itens foram enumerados à medida que se mostraram tecnicamente viável e economicamente vantajoso, considerando:

15.2. Viabilidade Técnica:

a) Integração e Interoperabilidade: A aquisição de soluções de um único fabricante pode simplificar a integração e garantir uma maior interoperabilidade entre as diferentes soluções, proporcionando uma infraestrutura de segurança mais coesa e eficiente.

b) Desempenho e Escalabilidade: Ao adquirir soluções de um único fabricante, será possível que o Ministério da Cultura garanta que todas as partes do sistema sejam otimizadas para trabalhar em conjunto, proporcionando um desempenho consistente e com escalabilidade conforme as necessidades do Ministério da Cultura

c) Características dos recursos de Hardware e Software: Com soluções de um único fabricante, há uma maior probabilidade de que a solução atenda as características de hardware e software do parque computacional, simplificando a implementação e a gestão.

d) Facilidade de Gerenciamento: Soluções integradas de um único fabricante geralmente oferecem uma interface de gerenciamento unificada, o que facilita o monitoramento e o gerenciamento de todas as soluções a partir de uma única plataforma, neste sentido caso opte pela aquisição de vários fabricantes, certamente a gerência destes recursos será mais complexa exigindo que os servidores e colaboradores tenham que aprender a trabalhar em mais de uma plataforma de gerência.

e) Suporte Técnico e Atualizações: Ao adquirir soluções de um único fabricante, o Ministério poderá contar com um único ponto de contato para suporte técnico e atualizações, o que simplifica que o processo de resolução de problemas será mais simplificado garantindo que as soluções estejam sempre atualizadas com as últimas correções de segurança com menor esforço dos operadores da solução.

15.3. Da viabilidade Econômica:

a) Economia a longo prazo: A longo prazo, atuar com produtos padronizados, pode resultar em economias significativas devido a uma melhor integração e eficiência operacional.

b) Custo Total de Propriedade (TCO): A consolidação de um sistema de um único fabricante pode reduzir o TCO ao longo do tempo, pois simplifica o gerenciamento, reduz os custos de treinamento e suporte, e minimiza a complexidade operacional.

c) ROI (Retorno sobre o Investimento): A implementação de soluções integradas de um único fabricante pode resultar em um ROI mais rápido, devido a uma melhor eficiência operacional, redução de incidentes de segurança e custos evitados associados a paralisações ou perdas de dados.

15.4. Considerando os benefícios em termos de integração, desempenho, gerenciamento simplificado, suporte unificado e potenciais economias financeiras, recomenda-se fortemente a aquisição da Solução de Tecnologia da Informação para Gestão de Identidades e Gestão de Acessos. Isso não apenas impactará a infraestrutura de tecnológica do Ministério da Cultura, mas também os serviços providos a Sociedade Brasileira, podendo, inclusive, resultar em uma melhor eficiência operacional e custos reduzidos ao longo do tempo.

15.5. O prazo de garantia de doze (12) meses permite que a equipe de tecnologia da informação tenha apoio durante o processo de incorporação da solução na realidade organizacional, continuando com foco na atuação, com aplicação de métodos e procedimentos que agreguem valor aos recursos tecnológicos e serviços ofertados servidores e colaboradores da rede do Ministério da Cultura e para os cidadãos que utilizam os serviços ofertados pela Pasta.

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

15.7. Os itens de cada grupo foram propostos de forma a compor uma única Solução de Tecnologia da Informação. Assim, a ausência de um dos itens não resultaria no atendimento incompleto das necessidades institucionais levantadas neste estudo.

15.8. Considerando o resultado da pesquisa de preços e os levantamentos realizados neste Estudo, diversos fabricantes capazes de atender a todos os itens, neste sentido a realização do certame na forma proposta não comprometerá o melhor aproveitamento dos recursos disponíveis no mercado e nem coloca em risco a ampla competitividade sem perda da economia de escala, conforme disposto no § 2º do art. 40, e inciso II do art. 47, da Lei nº 14.133, de 2021.

16. Benefícios a serem alcançados com a contratação

16.1. De acordo com a Necessidades de Negócio e Tecnológicas apontadas neste estudo, resumidamente se espera alcançar os seguintes benefícios:

16.1.1. Redução da complexidade dos acessos: Que os servidores e colaboradores do MinC tenham, a partir da integração dos sistemas de autenticação, acesso aos sistemas necessários para suas atividades laborais possível com senha/login único.

16.1.2. Hierarquização das permissões: Que as equipes de TI do MinC possam gerenciar permissões dos vários sistemas e ambientes de TI. Com um mapeamento da hierarquização de permissões de forma que cada colaborador tenha acesso apenas ao necessário.

16.1.3. Automação e centralização da administração: Gerência eficaz da criação e exclusão de novas identidades. Sem a necessidade de acessar vários painéis/dashboards nestes processos. Otimizando o tempo e evitando erros na gestão de identidades.

16.1.4. Acesso remoto seguro: Fornecer acesso fácil e seguro para colaboradores que exerçam atividades fora das sedes do MinC.

16.1.5. Prevenção contra malware e ataques cibernéticos: Mitigando dentre outros riscos, os associados a roubo ou utilização indevida de credenciais de acesso comuns ou privilegiadas. limitando o acesso dos usuários apenas ao necessário para suas funções. Bem como, ter maior controle sobre acessos remotos originados de dispositivos pessoais, evitando acesso de cibercriminosos ao ambiente tecnológico do MinC.

16.1.6. Conformidade regulatória: Aplicar políticas de segurança no contexto de Controle de Acesso e de Identidades. A exemplo das Normas Internas de Segurança da Informação de Controle de Acesso (NISI 02/2024) e, conseqüentemente, buscar aderência ao Programa de Privacidade e Segurança da Informação (PPSI).

17. Providências a serem Adotadas

17.1. O Ministério da Cultura deverá instituir Grupo de Trabalho ou Comissão composta por agentes da área técnica de Tecnologia da Informação e da área de Negócio para mapear necessidades referentes às identidades de servidores e colaboradores visando a correta implementação da solução dos itens do Grupo 01, em concordância com item “e”, Inciso I, Art. 11, da IN SGD/ME nº 94 /2022.

17.2. Todas as adequações necessárias, incluindo instalação e configuração da solução, serão de responsabilidade da CONTRATADA.

17.3. A prestação destes serviços deverá ocorrer, preferencialmente, nos dias e horários de expediente da unidade, nada impedindo, porém, que se realizem fora do expediente, desde que haja necessidade e haja comunicado prévio da CONTRATADA e anuência do MinC nas unidades onde o serviço será executado.

17.3. A equipe de planejamento da contratação foi instituída via portaria juntada aos autos

17.4. Este estudo deverá ser aprovado e assinado por seus Integrantes Técnico e Requisitante da Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC, (§ 2º, Art. 11, da IN SGD/ME nº 94/2022).

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

18.1. Consoante o inciso V do art. 11 da Instrução Normativa SGD/ME nº 94 de 23 de dezembro de 2022, esta equipe de planejamento, instituída pela PORTARIA SPOA Nº 142, DE 19 de julho de 2024, declara viável esta contratação com base neste Estudo Técnico Preliminar.

18.2. Considerando o inciso II do § 1º do art. 18 da Lei nº 14.133, de 2021, a pretensa contratação se encontra no Plano de Contratações Anual - PCA, de modo a indicar o seu alinhamento com o planejamento da Administração, sob o nº 420001-57/2024 (SEI/MinC nº 1797566).

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](#).

WALLACE MOREIRA BASTOS

Integrante Requisitante



Assinou eletronicamente em 03/01/2025 às 13:24:27.

GUSTAVO RIBEIRO DA ROCHA

Integrante Administrativo



Assinou eletronicamente em 03/01/2025 às 13:28:48.

FERNANDO KLEBER DE ARAUJO SOUZA

Integrante Técnico



Assinou eletronicamente em 03/01/2025 às 13:31:06.