

Termo de Referência 75/2024

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
75/2024	420001-SPOA/SE/MINC	WALLACE MOREIRA BASTOS	12/11/2024 14:43 (v 3.0)
Status			
ASSINADO			

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC		01400.019209/2023-00

1. Definição do objeto

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

- 1.1. Registro de Preços para contratação de solução de segurança da informação para auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (Microsoft Active Directory), correio eletrônico (Microsoft Exchange Server) e servidores de arquivos.
- 1.2. Adiante segue a lista contendo os itens, volumes e valores totais pesquisados e considerados os valores máximos para a estimativa de custo do registro de preços:

GRUPO / LOTE	ITEM	DESCRIÇÃO	CÓDIGO CATSER	UNIDADE DE MEDIDA	QUANT.	Valor Unitário	TOTAL ESTIMADO
1	1	Solução tecnológica para atendimento das exigências da política de segurança da informação, compliance e governança de dados não estruturados, pelo período de 36 meses.	27502	Unidade	1.500	R\$ 8.493,59	R\$ 12.740.390,00
	2	Serviço de Instalação e Configuração da Solução	26972	Unidade	01	R\$ 100.837,00	R\$ 100.837,00
	3	Serviço de Treinamento	3840	Turma	01	R\$ 73.468,00	R\$ 73.468,00
VALOR TOTAL ESTIMADO DA CONTRATAÇÃO					R\$ 12.914.695,00		

- 1.3. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

**1.4.** Os itens e serviços objeto dessa contratação são caracterizados como comuns, de caráter continuado e sem fornecimento de mão de obra em regime de dedicação exclusiva, a ser contratado mediante licitação, na modalidade pregão, em sua forma eletrônica.

**1.4.1** Os serviços são de natureza contínua e crítica para o funcionamento eficiente e eficaz da organização. A continuidade desses serviços é essencial para garantir que as operações de dados e os processos sejam mantidos seguros, atualizados e otimizados regularmente.

**1.4.2** Neste sentido, uma eventual interrupção desses serviços pode ter um impacto significativo nas operações da organização, afetando a eficiência, a tomada de decisões baseada em dados e a capacidade de resposta às demandas do mercado e regulamentações. Enquanto a continuidade desses serviços garante que a Pasta mantenha a continuidade do processo de maturidade, buscando assim, um alto nível de desempenho, segurança e conformidade, resultando em melhores resultados operacionais e estratégicos.

**1.5.** A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

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

**1.7.** O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

## **2. Fundamentação da contratação**

2.1 Com a publicação do Decreto nº 10.359, de 20 de maio de 2020, foi efetivada a transferência da Secretaria Especial da Cultura (SECULT), com suas 5 Secretarias Nacionais e um legado de cerca de 89 sistemas ou portais, para o Ministério do Turismo. Somadas as 3 Secretarias Nacionais da área de Turismo, com cerca de 43 sistemas ou portais ativos, essa transferência elevou significativamente as demandas por soluções de TIC.

2.2. Após a publicação do decreto 11.336/2023, que recria o Ministério da Cultura (MinC), este novamente passa a ter o papel de planejamento, administração geral, normatização, pesquisa e tratamento de dados relacionados com a política nacional de cultura e política nacional das artes, proteção do patrimônio histórico, artístico e cultural, regulação dos direitos autorais, 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, proteção e promoção da diversidade cultural, desenvolvimento econômico da cultura e a política de economia criativa, desenvolvimento e a implementação de políticas e ações de acessibilidade cultural e formulação e implementação de políticas, de programas e de ações para o desenvolvimento do setor museal. Este grande volume de informação serve de parâmetro para planejar os recursos e ações, proporcionam o mapeamento das deficiências culturais, indicação das principais necessidades atendidas e a hierarquia dessas necessidades, proporcionando assim maior efetividade na ação pública.

2.3. O alcance dos seus objetivos está aliado a necessidade da ampla utilização, processamento e armazenamento de informações, como por exemplo: planejar, coordenar, monitorar e avaliar políticas, programas, projetos e ações para a promoção da diversidade cultural brasileira, executar ações relativas à celebração de convênios, acordos e outros instrumentos congêneres que envolvam a transferência de recursos do Orçamento Geral da União, no âmbito de sua área de atuação. Para que possa atender às inúmeras demandas depende dos recursos de Tecnologia da Informação, que possibilitam o adequado exercício de suas atribuições regulamentares, de forma a maximizar os resultados pretendidos com suas políticas à luz dos princípios da disponibilidade, da segurança e da governança de dados contidos em seus repositórios.

2.4. O uso da Tecnologia da Informação e Comunicação (TIC) como recurso para a otimização dos serviços possibilita ao ministério prover medidas que torne seus procedimentos cada vez mais ágeis, seguros, integrados, eficientes e, sobretudo, acessíveis aos usuários.

2.5. Para prover todos os serviços prestados por meio de recursos de TIC, o MinC produz e dispõe de um grande volume de documentos em meio digital. Esses documentos estão em diretórios, servidores, e-mails acessíveis na rede do Ministério e contêm dados e informações sensíveis e estratégicas, inclusive atrelados à LGPD.

2.6. Um grande risco para as atividades desenvolvidas por qualquer empresa é que os sistemas computacionais se tornem indisponíveis, colocando em risco as operações e em dúvida a confidencialidade e a integridade dos dados armazenados. Com os sistemas cada vez mais “online” e usuários acessando uma infinidade de aplicativos Web ou remotos, faz-se necessária a implementação de controles e políticas de segurança da informação que garantam a disponibilidade, confidencialidade e a integridade das informações corporativas, mitigando inclusive possíveis ataques cibernéticos, como o sequestro e criptografia de dados, conhecido como *Ransomware*.

2.7. O crescimento dos incidentes de segurança e a evolução das ameaças à rede tecnológica exigem a continuidade e elevado nível de proteção da rede de dados, minimizando os incidentes no âmbito da estrutura organizacional. Dados coletados pela Fortinet, através de sua plataforma que coleta e analisa incidentes de segurança cibernética em todo o mundo, apontaram que o Brasil é o segundo país que mais sofre ataques cibernéticos na América Latina. Foram registradas mais de 31,5 bilhões de tentativas de ataques cibernéticos no primeiro semestre de 2022, um aumento de 94% considerando o mesmo período de 2021. No total, a região da América Latina e Caribe sofreu 137 bilhões de tentativas de ataques cibernéticos.

2.8. Diante deste cenário alarmante, o governo brasileiro publicou o Decreto nº 10.222, de 5 de fevereiro de 2020, criando a Estratégia Nacional de Segurança Cibernética (E-Cyber), com o objetivo de tornar o país seguro e proteger o espaço cibernético. As normativas visam aumentar a resiliência aos ataques cibernéticos e fortalecer a atuação brasileira em segurança online no cenário internacional. Adicionalmente a essa regulamentação tem-se a necessidade de atendimento à Lei Geral de Proteção de dados pessoais e o alinhamento à Política Nacional de Segurança da Informação.

2.9. O elevado volume de informações e comunicações eletrônicas do MinC e a sua importância para planejamento, divulgação e acessibilidade da cultura no Brasil, conduzem à necessidade da preservação das informações e dos equipamentos (pelos seus valores financeiros, informativos, probatórios e históricos) com a devida segurança e qualidade e com um ambiente adequado à sua destinação.

2.10. Os últimos ataques a diversos órgãos e instituições públicas brasileiras apontam para a urgência em adotar soluções para monitoramento, governança e auditoria das ocorrências de acesso e uso das informações no ambiente tecnológico, buscando garantir a segurança das informações e o funcionamento dos serviços prestados.

2.11. A solução tecnológica a ser futuramente contratada tangencia o tema relacionado a Governança de dados, na medida em que permitirá uma complementariedade em relação a estratégia de segurança e políticas regulatórias da LGPD já adotada por essa administração. Dada a complexidade das soluções de segurança da informação disponíveis no mercado, há que se considerar uma abordagem multidimensional para garantir auditoria, controle, rastreabilidade e privacidade dos dados custodiados.

2.12. Isto porque, cada solução possui uma abordagem distinta e, embora possam tangenciar aspectos e conceitos similares para a proteção de dados, suas funcionalidades, recursos e aplicações podem ter aplicabilidades distintas e por muitas vezes complementares.

2.13. Dentre os diversos conceitos que envolvem a governança e segurança de dados, inúmeros fabricantes/desenvolvedores possuem abordagens distintas para prover:

- a) Monitoramento de Dados Sensíveis;
- b) Prevenção contra vazamento de dados;
- c) Monitoramento e Controle de Acesso ao ambiente computacional;
- d) Monitoramento e Controle de Políticas de segurança Personalizáveis;
- e) Auditoria e Relatórios; e
- f) Detecção de Ameaças Internas e Integração.

2.14. Deste modo, a abordagem das diferentes soluções disponíveis pode ser distinta em função dos mecanismos de segurança e proteção de cada ferramenta ou solução.

2.15. Tal contextualização é importante para que seja justificado, de maneira clara, que a solução pretendida na presente contratação, embora possa tangenciar determinados requisitos de soluções tecnológicas já instaladas no parque computacional dessa administração, a exemplo de soluções de software de prevenção de perda e vazamento de dados, também conhecida como soluções de DLP (Data Loss Prevention), não representa uma redundância ou sobreposição de tecnologias da mesma natureza, mas sim uma complementariedade e abordagem mais ampla no tema, já que o foco dos recursos, funcionalidades e ferramentas da solução a ser contratada está na governança, auditoria e gerenciamento de riscos voltados a segurança da informação.

2.16. De maneira objetiva, diferentemente das abordagens padrões das soluções já instaladas, que reagem passivamente às políticas de segurança já estabelecidas, a pretendida contratação permitirá um foco na prevenção de riscos por meio de uma análise preditiva e uma gestão proativa destes dados, permitindo uma suplementação na estratégia de segurança, não tratando apenas de vulnerabilidades e riscos e servindo, inclusive, ao propósito de controle e visibilidade das soluções de segurança já implementadas.

2.17. Dito de outro modo, enquanto soluções de DLP definem o perímetro de proteção, monitoram endpoints e criam rotinas e regras rígidas a serem seguidas, a solução a ser contratada fornecerá uma visão detalhada de todos os acessos, "permissionamentos", dados expostos e proprietário dos dados.

2.18. Sendo assim, ao identificar e monitorar os acessos, quais dados estão expostos e quem os utiliza, a solução incrementará o conhecimento da rede sem estar fixa em regras rígidas, monitorando o acesso legítimo e eventuais vazamentos, bem como permitindo a responsabilização assertiva destes acessos que, por mais que permitidos, por vezes podem ser utilizados de forma maliciosa.

2.19. Nesse cenário, cumpre reforçar que a solução não se limitará a reforçar políticas existentes, mas irá guiar a criação de novas políticas para as soluções já instaladas, garantindo uma inteligência proativa na governança de dados por meio de uma compreensão profunda do ecossistema de dados obtidas através da análise de comportamentos. O resultado da presente contratação, que será atingido de forma complementar às soluções e investimentos já realizados nesse campo, será uma infraestrutura de segurança de dados não apenas reativa, mas também preventiva, que não só responderá às ameaças e proibição de ações dos usuários, mas irá antecipar ações maliciosas, as neutralizando com eficiência.

2.20. Ao tratarmos da expressão governança proativa de dados, temos que considerar que soluções convencionais entram em ação depois que um risco é detectado, já a solução a ser contratada deverá oferecer uma abordagem proativa, não só alertando sobre atividades suspeitas, mas também evitando acessos não autorizados antes que eles se tornem um problema, por meio de um modelo de governança de dados e resposta a incidentes que, em caso de uma violação de segurança, deverá garantir uma resposta rápida e informada devido à sua capacidade de fornecer contextos detalhados sobre a exposição dos dados, contribuindo para mitigar danos potenciais de forma complementar e mais ágil que as soluções já instaladas, que podem não ter toda a informação necessária sobre os dados afetados.

2.21. Outras funcionalidades dentro dos conceitos básicos de proteção e segurança da informação que serão abordadas e complementares as soluções já instaladas são:

- a) identificação de permissões excessivas ou antigas;
- b) remediação de forma automática dados expostos;
- c) automatização do processo de limpeza de credenciais e permissões antigas, minimizando a exposição de dados;
- d) integração com as soluções de DLP na classificação da informação, marcando os arquivos como sensíveis, abertos ou sigilosos possibilitando ao DLP o bloqueio de envio destes arquivos;
- e) responsabilização dos responsáveis por vazamentos dos dados através da auditoria por longos períodos;
- f) capacidade de prever acessos que, embora permitidos, podem apresentar riscos;
- g) validação e aprimoramento a criação de políticas para o DLP; e
- h) consolidar as defesas contra a exposição de dados.

2.22. Pelo exposto, ratifica-se a pertinência da demanda considerando a importância do serviço para o cumprimento da missão institucional do MinC para o alcance dos objetivos estratégicos desta Pasta Ministerial.

2.23. Desta forma, a contratação está aderente às diretrizes estabelecidas no Plano Diretor de Tecnologia da Informação e Comunicação – PDTI (2023 – 2027), alinhado a estratégia do MinC, conforme segue:

ALINHAMENTO AO PDTIC 2023-2027				
NECESSIDADE	CÓD.	AÇÃO	ÁREA ESPONSÁVEL	INDICADOR

Prevenção, tratamento e respostas a incidentes de segurança	A16.1	Contratar solução para prevenir e responder a ataques cibernéticos e incidentes de segurança	CGINF, CGSOL, DISEG	% de incidentes prevenidos
Provimento de segurança de TIC adequada ao MinC	A17.1	Contratar solução para gerir a análise e correção de vulnerabilidades de ativos e sistemas corporativos	CGINF, DISEG	% de vulnerabilidades corrigidas

### 3. Descrição da solução

#### DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

**3.1.** A descrição da solução como um todo encontra-se pormenorizada em tópicos específicos dos Estudos Técnicos Preliminares, anexo II deste Termo de Referência e também no anexo I (Caderno de Especificações Técnicas).

### 4. Requisitos da contratação

#### 4.1. Requisitos Gerais

**4.1.1.** Deverão ser observadas as leis, normas e diretrizes de Governo relacionadas à Segurança da Informação e Comunicações (SIC), em especial atenção ao Decreto Federal nº 9.637/2018, à Instrução Normativa GSI/PR nº 03/2021, e suas normas complementares.

**4.1.2.** A solução não deve ser um obstáculo à adoção de Padrões de Interoperabilidade de Governo Eletrônico. Os sistemas e serviços de TI do Ministério da Cultura devem estar de acordo com normas de acessibilidade (e-Mag) e interoperabilidade do Governo Eletrônico (e-Ping), incluindo os padrões de governança.

**4.1.3.** A contratada deverá atender aos critérios de sustentabilidade ambiental estabelecidos neste documento. Destacam-se as recomendações contidas no Capítulo III, Dos Bens e Serviços, com ênfase no art. 5º da Instrução Normativa nº 01/2010 STI/MPOG, bem como, o 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.

**4.1.4.** A solução deve ser entregue em pleno funcionamento, dessa forma, serão contemplados todos os serviços de instalação e configuração de todos os componentes adquiridos, sem ônus para o contratante.

**4.1.5.** Cada produto ou serviço entregue terá garantia mínima de 36 (trinta e seis) meses a contar da data do aceite definitivo. A garantia da solução contempla o serviço de suporte técnico para correção de problemas relacionados ao software, bem como a disponibilização de atualizações (novas versões do software).

**4.1.5.** O suporte técnico deve contemplar a abertura de chamados técnicos para resolução de problemas eventualmente encontrados no uso do produto, aplicação de patches de correção e intervenções para manutenção em caso de falhas.

**4.1.6.** A solução deverá estar em conformidade com as legislações correlatas e permitir o atendimento a Lei Geral de Proteção de Dados (LGPD).

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

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

## **4.2. Requisitos de Negócio**

A solução a ser adquirida deverá possibilitar por meio do usos dos recursos e serviços ofertados o atendimento das necessidades citadas no **Estudo Técnico Preliminar 68/2024**, objetivando atender os requisitos de negocio dos quais destacam-se:

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

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

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

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

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

## **4.3. Requisitos de Capacitação**

**4.3.1** Os profissionais responsáveis por ministrar os treinamentos à CONTRATANTE deverão conhecer todos os aspectos técnicos e funcionais do objeto aqui especificado, com experiência comprovada.

**4.3.2** A CONTRATADA deverá prestar, por meio de treinamento, presencial ou por vídeo aula - a critério do Ministério, a devida capacitação aos usuários, técnicos e gestores do Ministério no que se refere à plena operação e abertura de chamados técnicos, gerenciamento, gestão, monitoramento, controle, de acordo com os requisitos estabelecidos nesta documentação.

**4.3.3** A CONTRATADA será responsável pelas despesas relativas à participação de seus instrutores, tais como hospedagem, transporte, diárias etc.

**4.3.4** A CONTRATADA deverá fornecer apostilas e vídeo aula contendo o material necessário ao treinamento ofertado.

**4.3.5** O Ministério deverá disponibilizar local, ou *link* adequado para o treinamento ocorrer de forma satisfatória.

**4.3.6** A CONTRATADA deverá fornecer certificados de conclusão do treinamento emitidos nos nomes dos colaboradores que o executarem, cujas cópias deverão ser arquivadas pelo Ministério para fins de comprovação.

#### **4.4. Requisitos Legais**

**4.4.1.** O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e as seguintes legislações aplicáveis:

I - Decreto nº 11.462/2023 e suas alterações – Regulamenta os art. 82 a art. 86 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o sistema de registro de preços para a contratação de bens e serviços, inclusive obras e serviços de engenharia, no âmbito da Administração Pública federal direta, autárquica e fundacional;

II - Instrução Normativa SLTI/MPOG nº 01/2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências;

III - Portaria SGD/MGI 5.950 de 26 de outubro de 2023, 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 - SISF do Poder Executivo Federal.

#### **4.5. Requisitos de Manutenção**

**4.5.1.** Durante a vigência do contrato, a CONTRATADA deverá fornecer garantia contra qualquer defeito ou problema apresentado, permitindo o acesso às atualizações de segurança e pacotes de correção de problemas. A CONTRATADA deverá ainda disponibilizar as versões mais atualizadas dos softwares contratados, garantindo à CONTRATANTE o acesso às novas versões dos produtos.

**4.5.2.** A CONTRATADA disponibilizará, às suas expensas, canais para abertura de chamados técnicos para realização de intervenções que deverão funcionar em regime 24x7.

**4.5.3.** Os chamados técnicos terão origem em decorrência de qualquer problema detectado pela equipe da CONTRATANTE no tocante ao pleno estado de funcionamento da solução, inclusive problemas relacionados com instalação, configuração e atualização.

**4.5.4.** Na abertura do chamado, serão fornecidas, no mínimo, as seguintes informações:

- a. Problema observado;
- b. Informações técnicas da solução e do ambiente onde se originou o problema;
- c. Nome, telefone, e-mail do profissional responsável pela solicitação;
- d. Nível de severidade do chamado.

**4.5.5.** A CONTRATADA informará o número do chamado técnico no ato da comunicação efetuada pela equipe da CONTRATANTE, a qual servirá de referência para acompanhamento do chamado, inclusive após o encerramento do chamado.



**4.5.6.** O suporte técnico deverá ser especializado, podendo ser executado remotamente ou localmente dependendo da criticidade ou dificuldade. A avaliação do chamado quanto a criticidade será feita pelos gestores da CONTRATANTE.

**4.5.7.** A documentação produzida durante a execução dos serviços, seja em papel ou meio eletrônico, será de propriedade do CONTRATANTE e não deverá ser divulgada sem sua expressa autorização.

**4.5.8.** Os chamados técnicos serão classificados de acordo com a severidade devendo atender aos respectivos prazos de solução definidos na tabela a abaixo:

Tabela de Solução do Chamado		
Severidade	Descrição	Tempo de solução
1 – Urgente	Serviço parado no ambiente de produção.	Em até 04 (quatro) horas
2 – Muito Importante	Erros ou problemas recorrentes que impactam o ambiente de produção.	Em até 08 (oito) horas
3 – Importante	Problemas contornáveis.	Em até 12 (doze) horas
4 – Informação	Consulta técnica, dúvidas em geral, monitoramento, dentre outros.	Em até 48 (quarenta e oito) horas

**4.5.9.** O prazo de solução do chamado técnico será contado a partir da comunicação, por e-mail ou registro em sistema para a abertura do chamado técnico no sistema da CONTRATADA.

**4.5.10.** A CONTRATADA deverá possuir técnico especializado na solução, com no mínimo 1 (um) técnico certificado pelo fabricante e com certificação dentro da validade.

**4.5.11.** Em caso de identificação de novas versões de softwares e firmwares, considerados estáveis pelo fabricante e que representem melhorias para o ambiente computacional da CONTRATANTE, tais como correções de vulnerabilidades ou implementação novas funcionalidades, a CONTRATADA deverá comunicar à CONTRATANTE, informando os riscos e benefícios, para avaliação e possível implementação da mudança.

**4.5.12.** As intervenções que exijam paralisação do ambiente, ou que coloquem em risco sua disponibilidade, deverão ser executadas nos finais de semana e feriados ou em dias úteis fora do horário de expediente da CONTRATANTE (antes das 6:00h ou após as 22:00h).

**4.5.13.** Sempre que solicitada, a CONTRATADA deverá enviar à CONTRATANTE um relatório contendo todas as informações referentes aos chamados já abertos até o momento. Este relatório deve conter, no mínimo, as seguintes informações:

- a. Quantidade de chamados abertos;

- b. Quantidade de chamados atendidos dentro do prazo;
- c. Prazo médio de atendimento dos chamados.

#### 4.6. Requisitos Temporais

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

**4.6.2.** A CONTRATADA deverá entregar os serviços conforme cronograma abaixo:

<b>Etapas</b>	<b>Descrição</b>	<b>Prazo (estimado) em dias</b>
<b>1</b>	Assinatura do Contrato	Estima-se até 20 (vinte) dias úteis, contados a partir da homologação do certame.
<b>2</b>	Reunião inicial	Em até 10 (dez) dias, contados a partir da assinatura do(s) contrato(s), conforme agendamento efetuado pelo gestor do contrato.
<b>3</b>	Entrega das subscrições dos softwares necessários para prestação dos serviços	Em até 10 (dez) dias úteis contados da data de emissão da Ordem de Serviço para fornecimento da solução.
<b>4</b>	Habilitação dos técnicos da STII para abertura de chamados de suporte técnico	Imediatamente após a entrega da solução
<b>5</b>	Instalação e configuração da solução	Em até 10 (dez) dias úteis contados da data de emissão da Ordem de Serviço para instalação e configuração inicial da solução.
<b>6</b>	Recebimento provisório	Em até 05 (cinco) dias corridos a contar da entrega dos produtos da Ordem de Serviço.
<b>7</b>	Emissão do Aceite Definitivo	Em até 05 (cinco) dias corridos após o recebimento provisório.
<b>8</b>	Pagamento	Em até 30 (trinta) dias após o aceite definitivo e o recebimento da Nota Fiscal.
<b>9</b>	Início para contagem do prazo de garantia técnica	Imediatamente após a emissão do Termo de Aceite Definitivo.

#### 4.7. Requisitos de Segurança e Privacidade

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

4.7.2. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação da CONTRATANTE, e alterações.

4.7.3. A CONTRATADA deverá observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação do CONTRATANTE.

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

4.7.5. A CONTRATADA deverá observar os demais requisitos de segurança que estão relacionados com procedimentos técnicos de instalações, configurações e testes dos produtos que compõem a Solução Tecnológica.

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

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

#### **4.8. Requisitos Sociais, Ambientais e Culturais**

##### **4.8.1. Requisitos Sociais:**

- a. Prezar pela urbanidade do ambiente de trabalho, evitando ruído excessivo que possa prejudicar o andamento do trabalho de outros membros ou equipes que dividem o mesmo ambiente, manter a organização e limpeza dos espaços de trabalhos individuais e comuns.
- b. Prezar pela cordialidade, disponibilidade e respeito no tratamento entre os membros da equipe e demais servidores da CONTRATANTE para os quais a contratada prestará o serviço, sem preconceito ou quaisquer formas de discriminação.
- c. Zelar pelo uso dos equipamentos e mobiliário de uso pessoal (estações de trabalho, cadeiras, gaveteiros, computadores, telefone, periféricos, etc.) e de uso comum (salas de reunião, elevadores, catracas, banheiros, refeitório, copa, geladeiras, ar-condicionado, filtros, impressoras, espaço de convivência, etc.) visando manter o bom funcionamento e a harmonia dos ambientes, aumentando a sua vida útil.
- d. Não utilizar os recursos (e-mail corporativo, impressoras, salas de reunião, telefone institucional, etc.) para fins particulares ou que possam prejudicar a CONTRATANTE.

##### **4.8.2. Requisitos Ambientais:**

- a. Os serviços prestados pela Contratada deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e material consumidos, bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pelo MinC.
- b. A Contratada deverá atender, quando da execução do objeto do contrato, os critérios de sustentabilidade ambiental previstos na legislação pertinente.
- c. As configurações de hardware e software deverão ser executadas visando alto desempenho com o uso racional de energia, evitando-se a sobrecarga de equipamentos ou dispositivos elétricos.

4.8.3. Requisitos Culturais: Toda a documentação produzida e/ou fornecida pela Contratada referente ao objeto deverá estar preferencialmente no idioma português-BR, de forma clara e objetiva.

#### **4.9. Requisitos de Arquitetura Tecnológica**

4.9.1. O detalhamento das funcionalidades a serem atendidas pelo software ofertado no âmbito da presente solução consta no Caderno de Especificações Técnicas

#### **4.10. Requisitos de Projeto e de Implementação**

4.10.1. A solução de TIC deverá ser plenamente implementada pela Contratada no ambiente do MinC nos prazos estabelecidos no item 4.6.2 deste Termo de Referência.

#### **4.11. Requisitos de Implantação**

4.11.1. Os serviços de instalação e implantação da solução serão feitos com base em um plano a ser definido pela CONTRATADA e aprovado pela CONTRATANTE, e deverá envolver, minimamente, as seguintes etapas:

- a. Cronograma de implantação;
- b. Descrição dos componentes da topologia;
- c. Ordem de instalação e configuração dos softwares e demais produtos;
- d. Lista de restrições e condições a serem atendidas;
- e. Lista de riscos envolvidos e estratégias de mitigação;
- f. Checklist de verificação;
- g. Apresentação do plano à CONTRATANTE.

4.11.2 deverá ser instalada a versão mais atualizada da solução, devendo ainda a CONTRATADA garantir a possibilidade de atualização para as versões mais recentes dos softwares, sem custos adicionais.

#### **4.12. Requisitos de Garantia e Manutenção**

4.12.1. A CONTRATADA deverá oferecer garantia dos bens e serviços fornecidos pelo prazo mínimo de 36 (trinta e seis) meses, o qual será contado após a emissão do Termo de Aceite Definitivo.

4.12.2. A garantia técnica deverá ser fornecida pela CONTRATADA durante todo o período contratual, permitindo cobertura completa e de uso operacional dos softwares e/ou equipamentos em todas as funcionalidades contratadas, incluindo correções de falhas e a atualização de versões disponibilizadas pelo fabricante da solução.

4.12.3. A CONTRATADA deverá comunicar à CONTRATANTE caso a solução contratada passar a constar em listas de End-of-Support, End-of-Sales ou End-of-Life do fabricante, e deverá substituir a solução por outra com características técnicas iguais ou superiores, devendo ser apresentada à CONTRATANTE para validação.

4.12.4. Para todos os itens da solução a garantia deverá cobrir todo o período de licenciamento e deverá ser fornecida diretamente pelo fabricante dos softwares. O acesso para downloads de patches, drivers e quaisquer outras atualizações e/ou correções necessárias devem estar disponíveis 24x7 (vinte e quatro horas por dia, sete dias por

semana), durante todo o período de garantia técnica, e podem ser feitos através de http ou ftp, no sítio do fabricante da solução.

4.12.5. O direito do MinC à garantia técnica cessará caso a solução seja alterada pela próprio MinC ou por fornecedores que não a Contratada e/ou Fabricante responsável pelo serviço em questão.

#### **4.13. Requisitos de Experiência Profissional**

4.13.1. Capacidade Técnica da Licitante: Será exigido o fornecimento, pelo proponente, de Atestado(s) de Capacidade Técnica, emitido por pessoa física ou jurídica de direito público ou privado, demonstrando que a proponente prestou serviços/fornecimentos compatíveis com o objeto pretendido, da seguinte forma:

a) Para fins de compatibilidade, considera-se atividade pertinente ao objeto licitado para o fornecimento de Solução para segurança e governança de dados com identificação e classificação de informações sensíveis, da mesma natureza e compatível com o objeto descrito no Termo de Referência, incluindo os serviços de configuração, suporte e manutenção da solução, contemplando, no mínimo 50% do volume de usuários contemplados pela presente contratação.

#### **4.14. Da Garantia de Contratação**

4.14.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5% (cinco por cento) do valor total estimado da contratação.

4.14.2. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

4.14.3. A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.

4.14.4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

#### **4.15. Informações Relevantes para o Dimensionamento/Apresentação da Proposta**

4.15.1. A proposta da LICITANTE deverá conter a especificação clara e completa da prestação de serviços, obedecida a mesma ordem constante deste Termo de Referência, sem conter alternativas de preços, ou de qualquer outra condição que induza o julgamento.

4.15.2. Entende-se por especificação clara e completa da prestação de serviços, o detalhamento do objeto, os quantitativos de produtos/serviços a serem entregues /executados, marcas/modelos de aparelhos/equipamentos a serem fornecidos e demais condições gerais de prestação dos serviços que deverão constar da proposta da LICITANTE.

4.15.3. Não serão aceitas propostas contendo cópia das exigências deste Termo de Referência no lugar da especificação clara e inequívoca dos serviços a serem executados.

4.15.5. Transferência de Conhecimento: A transferência do conhecimento deverá ser realizada observando-se o que segue:

a. A transferência de conhecimento deverá ocorrer no ambiente de trabalho da equipe da CONTRATANTE, com o passo-a-passo da operação da solução ou, quando permitido pela CONTRATANTE, em outra localidade ou de forma remota por webconferência.

b. Ficará a cargo da CONTRATADA, após a implantação de qualquer produto, a realização de transferência de conhecimento para que a documentação do projeto seja repassada e o conhecimento disseminado para a equipe da CONTRATANTE.

c. A transferência de conhecimento, além do previsto no item anterior, dar-se-á através da disponibilização de documentação técnica (manuais, guias, especificação técnica, configurações, etc.) referente aos produtos e serviços entregues, assim como na modalidade hands on, procedendo a passagem de conhecimento durante a própria configuração/confecção do produto ou serviço.

#### **4.16. Vistoria**

4.16.1. Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

#### **4.17. Subcontratação**

4.17.1. Não será admitida a subcontratação do objeto previsto neste Termo de Referência.

### **5. Modelo de execução do objeto**

#### **5. DEVERES E RESPONSABILIDADES**

##### **5.1. Responsabilidade do Contratante**

5.1.1. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta.

5.1.2. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

5.1.3. O fiscal designado não deverá, dentro das possibilidades de pessoal do órgão contratante, ter exercido a função de pregoeiro na licitação que tenha antecedido o contrato, a fim de preservar a segregação de funções (TCU, acórdão 1375/2015 – Plenário e, TCU, acórdão 2146/2011, Segunda Câmara).

5.1.4. A designação do fiscal deverá levar em conta potenciais conflitos de interesse, que possam ameaçar a qualidade da atividade a ser desenvolvida. (Acórdão TCU 3083/2010 – Plenário).

5.1.5. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas.

5.1.6. Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência.

5.1.7. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da contratada, no que couber, em conformidade com o item 6 do Anexo XI da IN SEGES/MP n. 5 /2017.

5.1.8. Não praticar atos de ingerência na administração da Contratada, tais como:

- a. exercer o poder de mando sobre os empregados da Contratada, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação prever o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;
- b. direcionar a contratação de pessoas para trabalhar na empresa Contratada;
- c. promover ou aceitar o desvio de funções dos trabalhadores da Contratada, mediante a utilização destes em atividades distintas daquelas previstas no objeto da contratação e em relação à função específica para a qual o trabalhador foi contratado; e
- d. considerar os trabalhadores da Contratada como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens.

5.1.9. Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto.

5.1.10. Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento.

5.1.11. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento das obrigações pela Contratada.

5.1.12. Fiscalizar o cumprimento dos requisitos legais, quando a contratada houver se beneficiado da preferência estabelecida pelo art. 26 da Lei nº 14.133/21.

5.1.13. Arquivar, entre outros documentos, projetos, "as built", especificações técnicas, orçamentos, termos de recebimento, contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas.

5.1.14. Assegurar que o ambiente de trabalho, inclusive seus equipamentos e instalações, apresentem condições adequadas ao cumprimento, pela Contratada, das normas de segurança e saúde no trabalho, quando o serviço for executado em suas dependências, ou em local por ela designado.

5.1.15. Proporcionar todas as facilidades para que a Contratada possa cumprir suas obrigações dentro das normas e condições contratuais.

5.1.16. Permitir ao pessoal da Contratada livre acesso às dependências do MinC, de modo a viabilizar a prestação dos serviços durante o horário de expediente do órgão, ou fora dele, quando solicitado e/ou autorizado pelo Fiscal do Contrato.

5.1.17. Aplicar as penalidades previstas neste Termo de Referência, quando for o caso, assegurando o contraditório e a ampla defesa à Contratada.

## **5.2. Responsabilidade da Contratada**

5.2.1. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das

cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste Termo de Referência e em sua proposta.

5.2.2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

5.2.3. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à União ou à entidade federal, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos.

5.2.4. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor.

5.2.5. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a empresa contratada deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT, conforme alínea "c" do item 10.2 do Anexo VIII-B da IN SEGES/MP n. 5/2017;

5.2.6. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou que se verifique no local dos serviços.

5.2.7. Prestar todo esclarecimento ou informação solicitada pela Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

5.2.8. Paralisar, por determinação da Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

5.2.9. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado.

5.2.10. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

5.2.11. Submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo.

5.2.12. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

5.2.13. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.



5.2.14. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social, bem como as regras de acessibilidade previstas na legislação, quando a contratada houver se beneficiado da preferência estabelecida pela Lei nº 13.146, de 2015.

5.2.15. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

5.2.16. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, salvo orientação legal em outro sentido.

5.2.17. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante.

5.2.18. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação.

5.2.19. Assegurar à Contratante, em conformidade com o previsto no subitem 6.1, "a" e "b", do Anexo VII – F da Instrução Normativa SEGES/MP nº 5, de 25/05/2017:

5.2.19.1 direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o recebimento de cada parcela, de forma permanente, permitindo à Contratante distribuir, alterar e utilizar os mesmos sem limitações;

5.2.19.2 Os direitos autorais da solução, do projeto, de suas especificações técnicas, da documentação produzida e congêneres, e de todos os demais produtos gerados na execução do contrato, inclusive aqueles produzidos por terceiros subcontratados, ficando proibida a sua utilização sem que exista autorização expressa da Contratante, sob pena de multa, sem prejuízo das sanções civis e penais cabíveis.

5.2.20. Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos da contratante ou da nova empresa que continuará a execução dos serviços.

5.2.21. indicar formalmente preposto apto a representá-la junto à Contratante, que deverá responder pela fiel execução do contrato;

5.2.22. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.23. reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do contrato pela Contratante;

5.2.24. propiciar todos os meios necessários à fiscalização do contrato pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.2.25. manter, durante toda a execução do contrato, as mesmas condições da habilitação.

### **5.3. Condições de Execução**

#### **5.3.1. Local e Horário da Prestação dos Serviços**

**5.3.1.1.** Todos os serviços deverão ser preferencialmente prestados remotamente ou excepcionalmente de forma presencial a critério da CONTRATANTE.

**5.3.1.2.** Caso a CONTRATANTE opte pela prestação dos serviços de forma presencial, estes deverão ser realizados em quaisquer dependências do MinC em Brasília/DF.

#### **5.3.2. Materiais a serem disponibilizados**

**5.3.2.1** Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades estabelecidas neste Termo de Referência, promovendo sua substituição quando necessário.

#### **5.3.3. Especificação da Garantia**

**5.3.3.1** Para todos os produtos resultantes dos serviços contratados a garantia será de 36 (trinta e seis) meses devendo a CONTRATADA efetuar as correções de defeitos identificados durante o período, que terá início a partir da data do recebimento definitivo de cada OS.

#### **5.3.4. Formas de Transferência de Conhecimento**

**5.3.4.1** A CONTRATADA, após instalar e configurar a solução licitada, deverá entregar toda a documentação técnica pertinente bem como realizar a transferência de conhecimento para a equipe técnica da STII dos procedimentos realizados e da configuração das ferramentas, sem ÔNUS ao CONTRATANTE. Posteriormente, poderá ser requisitada a realização de serviços profissionais de treinamento e consultoria por meio de Ordem de Serviço específica.

**5.3.4.2** Quanto aos produtos resultantes das demandas de Ordens de Serviços, a transferência do conhecimento deverá ser realizada observando-se o que segue:

- i) A transferência do conhecimento produzido pelo registro durante a execução do contrato será implementada por meio do compartilhamento de informações e documentos no repositório do software utilizado pela CONTRATANTE para o controle de versões, bem como pelo relacionamento interpessoal entre as equipes da CONTRATANTE e CONTRATADA.
- ii) Toda a documentação que a CONTRATADA estará obrigada a registrar nesse repositório constará da Ordem de Serviço. Portanto, para que a Ordem de Serviço seja aceita e liberada para pagamento, a CONTRATANTE verificará no repositório a existência de tais documentos obrigatórios.
- iii) Caso a CONTRATADA tenha falhado nesse quesito, estará sujeita ao não recebimento dos valores devidos, até que o repositório tenha sido devidamente atualizado com os documentos em questão.
- iv) Dessa forma, todo o conhecimento gerado durante a execução de cada Ordem de Serviço estará disponível e passará a fazer parte da base histórica do Órgão. Ao término do contrato, seja por decurso de vigência ou por rescisão antecipada, a CONTRATADA fica obrigada a promover a transição contratual com transferência de tecnologia e técnicas empregadas, sem perda de informações, capacitando, se solicitado, aos técnicos da CONTRATANTE ou aos da nova empresa que continuará a execução dos serviços.

v) Todos os documentos gerados deverão respeitar os critérios de sustentabilidade ambiental previstos na Instrução Normativa nº 01, de 19 de janeiro de 2010, e demais normativos relacionados e mais atuais.

### 5.3.5. Procedimentos de Transição e Finalização do Contrato

**5.3.5.1** Em caso de rescisão ou não renovação contratual, a CONTRATADA obriga-se a prestar para a CONTRATANTE ou a terceiro por ele designado, toda a assistência a fim de que os serviços continuem sendo prestados sem interrupção ou efeito adverso, e que haja uma transferência ordenada de conhecimento dos serviços para a CONTRATANTE ou a seu designado.

**5.3.5.2** As atividades de transição e finalização do contrato incluem a entrega de versões finais dos produtos e da documentação, a transferência de conhecimentos, a devolução de recursos, inclusive crachás disponibilizados pela CONTRATANTE, a revogação de perfis de acesso, a eliminação de caixas postais, dentre outras.

**5.3.5.3** Todo conhecimento adquirido ou desenvolvido, bem como toda informação produzida e/ou utilizada para a execução dos projetos e serviços contratados deverão ser disponibilizados à CONTRATANTE ou empresa por ela designada em até 30 (trinta) dias corridos após o encerramento do contrato.

**5.3.5.4** O fato da CONTRATADA ou seus representantes não cooperarem ou reterem qualquer informação ou dado solicitado pela CONTRATANTE, que venha a prejudicar, de alguma forma, o andamento da transição das tarefas e serviços para um novo prestador, constituirá quebra de contrato, sujeitando-a as obrigações em relação a todos os danos causados à CONTRATANTE, conforme estipulado no modelo de gestão do contrato deste documento.

### 5.3.6. Mecanismos Formais de Comunicação

**5.3.6.1.** Pelo MinC responderá o Gestor do Contrato, e pela CONTRATADA, sem ônus para o MinC, responderá o Preposto Contratual. Ambos (gestor e preposto) responderão sobre todas as questões administrativas do contrato a ser firmado, procurando solucionar todos os problemas dentro dos limites legais e dentro da razoabilidade.

**5.3.6.2.** A critério da CONTRATANTE poderão ocorrer reuniões para acompanhamento dos serviços, cuja responsabilidade pela elaboração da ata caberá ao Preposto, mantendo os pontos relevantes discutidos, bem como as decisões e prazos acordados. Na eventualidade de problemas fortuitos, poderão ser convocadas reuniões por qualquer uma das partes, desde que comunicadas com antecedência.

**5.3.6.3.** Os instrumentos de comunicação serão:

Descrição	Responsável	Periodicidade	Formas de Distribuição e Destinatários	Finalidade
	Execução			
Atas de Reunião	Preposto	Toda reunião	Reunião/e-mail/ Participantes das Reuniões	Registro de decisões ou resoluções de conflitos combinados em reuniões entre as partes

Ofício	Gestor ou Preposto	Sempre que necessário	SEI	Comunicar oficialmente por exemplo: <ul style="list-style-type: none"> <li>• Solicitar reajuste;</li> <li>• Solicitar pedido de renovação;</li> <li>• Advertir ou comunicar penalidades;</li> <li>• Envio de documentação contratual ou dos colaboradores;</li> <li>• Solicitar ou enviar atestados de capacidade técnica etc.</li> </ul>
Mensagem eletrônica	Gestor ou Preposto	Sempre que necessário	e-mail	Outros tipos de comunicação que necessitem registro escrito
Telefone	Gestor ou Preposto	Sempre que necessário	Telefone	Outros tipos de comunicação que não necessitem de registro escrito

### 5.3.7. Formas de Pagamento

**5.3.7.1** Os critérios de medição e pagamento dos serviços prestados serão tratados em tópico próprio do Modelo de Gestão do Contrato.

### 5.3.8. Manutenção de Sigilo e Normas de Segurança

**5.3.8.1** O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

**5.3.8.2** A CONTRATADA deverá seguir todas as normas de segurança do MinC.

**5.3.8.3** O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se no Anexo IV deste Termo de Referência.

### 5.3.9. Documentação mínima exigida

**5.3.9.1** A solução deverá estar acompanhada de sua documentação técnica completa e atualizada, compreendendo manuais, guias de instalação e outros pertinentes.

**5.3.9.2** A documentação deverá ser fornecida em sua forma original, impressa ou em mídia digital, ou deverá ser disponibilizada no site do fabricante para download.

**5.3.9.3** Os licenças de softwares fornecidos deverão ser originais do fabricante, devendo a documentação conter elementos que comprovem a sua autenticidade e validade ou serem repassadas diretamente do fabricante para os gestores da CONTRATANTE.

### **5.3.10. Prazos, Horários de Fornecimento de Bens ou Prestação de Serviços**

**5.3.10.1** A CONTRATADA deverá observar os prazos de entrega estabelecidos neste Termo de Referência.

**5.3.10.2** Os serviços deverão ser prestados no horário de expediente da CONTRATANTE, nos dias úteis, das 07:00h às 20:00h, obedecendo as portarias Federais que anualmente divulgam o cronograma de feriados nacionais e pontos facultativos no ano, a serem observadas pela CONTRATADA, sem comprometimento das atividades públicas consideradas como serviços essenciais à população.

**5.3.10.3** Os plantões (atendimentos fora do horário descrito acima) serão sem ônus adicionais para o MinC, sem prejuízo do pagamento de todos os direitos a que fizerem jus aos profissionais alocados nos plantões, observada a legislação trabalhista. Os plantões, geralmente sazonais, ocorrem principalmente no meio e no fim de cada ano e nos períodos em que for necessário realizar a carga do censo escolar, empenhos e pagamentos.

## **6. Modelo de gestão do contrato**

**6.1.** O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

**6.2.** Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

**6.3.** As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

**6.4.** O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

### **6.5. Preposto**

6.5.1. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

6.5.2. A Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade.

### **6.6. Reunião Inicial**

6.6.1. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

6.6.2. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 10 (dez) dias da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

6.6.3. A pauta desta reunião observará, pelo menos:

6.6.3.1. Presença do representante legal da contratada, que apresentará o seu preposto;

6.6.3.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

6.6.3.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

6.6.3.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

6.6.3.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste Termo de Referência

## 6.7. Fiscalização

6.7.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos ([Lei nº 14.133, de 2021, art. 117, caput](#)).

6.7.2. A fiscalização de que trata este item SERÁ EXERCIDA NO INTERESSE DA CONTRATANTE e não exclui, nem reduz a responsabilidade da CONTRATADA, até mesmo perante terceiro, por qualquer irregularidade, inclusive resultante de imperfeições técnicas, emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes e prepostos.

6.7.3. À CONTRATANTE se reserva o direito de rejeitar no todo ou em parte os objetos, se em desacordo com as especificações exigidas neste Termo de Referência, seus anexos, e das constantes na proposta comercial.

6.7.4. A CONTRATADA lançará na Nota Fiscal as especificações do objeto contratado, de modo idêntico àquela constante do Termo de Contrato.

6.7.5. A CONTRATADA é obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em partes, os objetos contratados em que se verifiquem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados.

6.7.6. Todas as comunicações relativas ao presente Contrato serão consideradas regularmente feitas desde que entregues, ou enviadas por carta protocolada, telegrama ou e-mail, devidamente confirmados.

6.7.7. Qualquer mudança de endereço deverá ser imediatamente comunicada à outra parte.

6.7.8. Quaisquer exigências da fiscalização, inerentes aos objetos do contrato deverão ser prontamente atendidas pela CONTRATADA.

6.7.9. As decisões e providências que ultrapassarem a competência da Equipe de Gestão do Contrato deverão ser solicitadas a instâncias superiores em tempo hábil para adoção das medidas convenientes.

## 6.8. Fiscalização Técnica

6.8.1. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. ([Decreto nº 11.246, de 2022, art. 22, VI](#));

6.8.2. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. ([Lei nº 14.133, de 2021, art. 117, §1º](#) e [Decreto nº 11.246, de 2022, art. 22, II](#));

6.8.3. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. ([Decreto nº 11.246, de 2022, art. 22, III](#));

6.8.4 O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. ([Decreto nº 11.246, de 2022, art. 22, IV](#));

6.8.5. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. ([Decreto nº 11.246, de 2022, art. 22, V](#));

6.8.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual ([Decreto nº 11.246, de 2022, art. 22, VII](#)).

## 6.9 Fiscalização Administrativa

6.9.1. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

6.9.2. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

## 6.10. Gestor do Contrato

6.10.1. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

6.10.2. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

6.10.3. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

6.10.4. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

6.10.5. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

6.10.6. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

6.10.7. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

## 6.11 Do Reajuste

**6.11.1.** Os preços inicialmente contratados são fixos e irredutíveis no prazo de um ano contado da data do orçamento estimado, 01/10/2024.

**6.11.2.** Após o interregno de um ano, e independentemente de pedido da CONTRATADA, os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, do índice ICTI (Índice de Custo de Tecnologia da Informação), estabelecido pelo IPEA, ou outro índice que o substitua, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, com base na seguinte fórmula (art. 5º do Decreto nº 1.054, de 1994):  $R = V (I - I^0) / I^0$ , onde: *R = Valor do reajuste procurado; V = Valor contratual correspondente à parcela dos insumos a ser reajustada; I<sup>0</sup> = índice inicial - refere-se ao índice de custos ou de preços correspondente à data fixada para entrega da proposta da licitação; I = Índice relativo ao mês do reajustamento.*

**6.11.3.** No caso de atraso ou não divulgação do índice de reajustamento, a Contratante pagará à Contratada a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a Contratada obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

**6.11.4.** Caso o índice estabelecido para o reajuste venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.



**6.11.5.** Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço, por meio de termo aditivo.

**6.11.6.** Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

**6.11.7.** O reajuste será realizado por apostilamento.

## **6.12. Sanções Aplicáveis**

**6.12.1.** Com fundamento no artigo 155 da Lei nº 14.133/2021 o licitante ou o contratado será responsabilizado (garantida a ampla defesa) administrativamente pelas seguintes infrações:

- I - dar causa à inexecução parcial do contrato;
- II - dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
- III - dar causa à inexecução total do contrato;
- IV - deixar de entregar a documentação exigida para o certame;
- V - não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
- VI - não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- VII - ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
- VIII - apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;
- IX - fraudar a licitação ou praticar ato fraudulento na execução do contrato;
- X - comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- XI - praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
- XII - praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

**6.12.2.** Sem prejuízo das sanções previstas no item anterior e ainda com fundamento na Lei nº 14.133/2021, a CONTRATADA ficará sujeita, no caso de infrações administrativas, sem prejuízo das responsabilidades civil e criminal, assegurada a prévia e ampla defesa, às seguintes penalidades:

- **Advertência por escrito**, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;
- **Multa de:**
  - 0,5% (cinco décimos por cento) por dia sobre o valor contratado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto

dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

- 0,5% (cinco décimos por cento) até 10% (dez por cento) sobre o valor contratado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem anterior ou de inexecução parcial da obrigação assumidas.
- 0,8% (oito décimos por cento) até 15% (quinze por cento) sobre o valor contratado, em caso de inexecução total da obrigação assumida.
- 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato.
- As multas não têm caráter indenizatório e seu pagamento não eximirá a CONTRATADA de ser acionada judicialmente pela responsabilidade civil derivada de perdas e danos junto ao CONTRATANTE, decorrente das infrações cometidas;
- As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.
- **Suspensão temporária** do direito de participar de licitação e impedimento de contratar com o CONTRATANTE, pelo prazo de até 3 (três) anos.
- **Declaração de inidoneidade** para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, que será concedida sempre que o CONTRATADO ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no item anterior.

**6.12.3.** Será facultada à CONTRATADA a apresentação de defesa prévia no prazo de 05 (cinco) dias, após a notificação, para as penalidades: advertência, multa e suspensão e de 10 (dez) dias para a penalidade declaração de inidoneidade.

**6.12.4.** A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa neste Termo de Referência.

**6.12.5.** As sanções de advertência, suspensão e declaração de inidoneidade poderão ser aplicadas à CONTRATADA juntamente com as de multa.

## 7. Critérios de medição e pagamento

**7.1.** A emissão da Nota Fiscal/Fatura deve ser precedida do recebimento definitivo dos serviços, nos termos a seguir:

**7.1.1** O recebimento do objeto se dará de forma única, por meio do acompanhamento e da fiscalização exercidos pela CONTRATANTE, por meio do Termo de Recebimento Definitivo.

**7.1.2** A qualquer tempo, durante o prazo de prestação dos serviços, em caso de ser identificada alguma não conformidade, a fiscalização discriminará, mediante ofício, as irregularidades encontradas e providenciará a imediata comunicação dos fatos à

CONTRATADA, ficando a mesma, cientificada de que está passível das penalidades cabíveis, devendo ser posteriormente submetida a verificações de conformidade.

**7.1.3** Caso a reparação não ocorra no prazo estabelecido, ou caso permaneça após nova verificação de conformidade, estará a empresa sujeita à aplicação das sanções previstas neste Termo de Referência.

**7.1.4** O recebimento não exclui a responsabilidade da CONTRATADA pelo perfeito desempenho do serviço prestado, cabendo-lhe sanar quaisquer irregularidades detectadas resultantes da execução dos serviços ou de materiais empregados.

**7.1.5** O procedimento de avaliação dos serviços será realizado periodicamente pela fiscalização do contrato, avaliando os documentos apresentados após a prestação de serviços executados com base nos indicadores descritos neste Termo de Referência, bem como os documentos de regularidade contratual previstos.

**7.1.6** A aceitação formal dos serviços será realizada pela fiscalização, iniciando por meio da validação das entregas pela Fiscalização (recebimento provisório), emissão do Termo de Aceite (recebimento definitivo), autorização para emissão e posterior atesto da nota fiscal referente ao adimplemento da obrigação contratual e dos demais documentos comprobatórios solicitados, desde que cumpridas as condições e exigências para a realização dos serviços, observadas as disposições contidas neste Termo de Referência e no Contrato, sem prejuízo da aplicação das sanções contratuais, se for o caso.

7.1.6.1. Registre-se, por oportuno, que o modelo de solução a ser contratada prevê como característica o pagamento da subscrição em parcela única, válido por 36 meses.

7.1.6.2. O Tribunal de Contas da União, consoante o Acórdão nº 2569/2018-Plenário, alerta para os eventuais riscos e vantagens desse modelo, senão vejamos:

*“Relatório Nota Técnica 13 (1704534) SEI 23038.001213/2021-60 / pg. 3 “Relatório ... 156. Os fabricantes costumam exigir o pagamento à vista para o fornecimento de licenças e de serviços agregados, o que pode resultar na não utilização dos itens adquiridos devido à demora para viabilizar a utilização do software ou à interrupção de projetos. Por outro lado, o pagamento parcelado costuma incluir um custo financeiro da operação no preço final obtido pelas organizações públicas” (grifei)*

7.1.6.3. Neste ponto, cabe enfatizar que as licenças envolvidas na contratação em pauta, listadas neste documento, serão utilizadas pelo MinC nas atividades diárias do Ministério, de maneira contínua, em um ambiente estabelecido. Portanto, não se verifica a possibilidade de “não utilização dos itens adquiridos devido à demora para viabilizar a utilização do software”, restando afastado um grave risco mencionado no julgado referido.

7.1.6.4. No tópico “Análise das evidências”, item 157 do mencionado Acórdão, as ações de prevenção para os riscos acima destacados ficam melhor esclarecidas:

*“... Tanto as licenças quanto os serviços agregados possuem peculiaridades que devem ser consideradas pelos gestores na decisão de optar-se pelo pagamento à vista ou parcelado durante o processo da contratação. Além disso, a compra de licenças e de serviços agregados deve ocorrer em momento oportuno dos projetos para evitar que haja dispêndio de recursos em período no qual não há utilização desses itens”.*

7.1.6.5. Diante do acima exposto, é possível concluir que não há proibição absoluta quanto ao pagamento em parcela única, pois o próprio Acórdão fala em decisão, opção do gestor, desde que ponderados os riscos. Ademais, não se está contratando serviços agregados, mas apenas as subscrições de licenças. Por fim, como explanado

nos tópicos anteriores, o uso contínuo das licenças nas atividades cotidianas do MinC elimina a possibilidade de “dispêndio de recursos em período no qual não há utilização desses itens”.

7.1.6.6. Ainda quanto ao aspecto financeiro, prossegue o supracitado Acórdão:

*“167.1. a exigência de pagamento parcelado pode resultar na inclusão de custos financeiros no preço, pois os revendedores e os fabricantes tendem a financiar o valor para viabilizar essa forma de pagamento (peça 69, p. 4, questão 6.b; peça 96, p. 4, questão 6.2; peça 92, p. 4, questão 6.2; peça 97, p. 3, questão 6.2; peça 112, questão 4.e.ii)” (grifei)*

## 7.4. Do Recebimento

**7.4.1** Os serviços serão recebidos provisoriamente, no prazo estabelecido no item 4 deste Termo de Referência, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a, da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

**7.4.2** O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda da CONTRATADA com a comprovação da prestação dos serviços a que se referem.

**7.4.3.** O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022).

**7.4.4** O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022).

**7.4.5** A CONTRATADA fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

**7.4.6** A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021).

**7.4.7** O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

**7.4.8** Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

**7.4.9** Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

**7.4.10** Os serviços serão recebidos definitivamente, no prazo estabelecido no item 4 deste Termo de Referência, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

- I. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pela CONTRATADA, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme (art. 21, VIII, Decreto nº 11.246, de 2022). Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, as respectivas correções;
- II. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e,
- III. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.
- IV. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.
- V. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução.

## **7.5. Procedimentos de Teste e Inspeção**

**7.5.1** Para fins de recebimento provisório e definitivo, deverão ser considerados os prazos previstos neste Termo de Referência.

**7.5.2** O Fiscal Técnico do contrato realizará o recebimento provisório desde que haja a entrega e ativação/instalação dos produtos e documentação aplicável referente aos serviços realizados ou bens fornecidos.

**7.5.3** Caso sejam verificados produtos incompletos ou inconsistentes, o Fiscal Técnico comunicará à CONTRATADA para que realize os ajustes necessários, sem prejuízo do prazo de entrega definido na Ordem de Serviço.

**7.5.4** A Ordem de Serviço não será recebida provisoriamente enquanto os produtos não forem entregues por completo. Havendo justificativa pelo não atendimento dos critérios de aceitação, a CONTRATADA deverá apresentar a justificativa ao Gestor que decidirá quanto à aceitação.

**7.5.5** Após o Recebimento Provisório, os Fiscais Técnico e Requisitante do contrato promoverão a avaliação da qualidade dos serviços realizados (homologação).

**7.5.6** Havendo conformidade com a execução do serviço e atendidos os critérios de aceitação, o Fiscal Requisitante e o Gestor do contrato emitirão o Aceite Definitivo. Na hipótese do aceite definitivo não ser procedido dentro do prazo fixado neste Termo de Referência, reputar-se-á como realizado, salvo justificativa em contrário.

**7.5.7** O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato nos termos da lei.

**7.5.8** O Fiscal Administrativo verificará a aderência aos termos contratuais. Caso não haja aderência, o Fiscal Administrativo deve indicar os termos que não estão aderentes ao

contrato, e o Gestor deve então encaminhar as devidas propostas de sanções para Área Administrativa proceder aos trâmites legais, resguardando sempre a ampla defesa e o contraditório.,

**7.5.9** De posse do Aceite Definitivo o Gestor do contrato autorizará a CONTRATADA a emitir a(s) Nota(s) Fiscal(is), por meio de aviso formal ao Preposto, via instrumentos de comunicação previstos neste Termo de Referência.

## 7.6 Níveis Mínimos de Serviço Exigidos

**7.6.1** Para efeito de mensuração dos serviços, foram estabelecidos os indicadores abaixo, bem como outros parâmetros que serão utilizados para controle de qualidade. Estes integrarão os Níveis Mínimos de Serviço e servirão para que a fiscalização do contrato realize o acompanhamento dos serviços prestados, bem como a aferição do cumprimento das metas estabelecidas.

01 – IST – Indicador de Suporte Técnico (Solução)	
Tópico	Descrição
Finalidade	Medir o tempo de atendimento dos chamados de suporte técnico da solução.
Meta a cumprir	<b>IST &lt;= 0,10</b> A meta definida visa garantir o atendimento dos chamados de suporte técnico dentro do prazo previsto
Instrumento de medição	Com base em relatório de atendimento de chamados emitido pela CONTRATADA.
Forma de acompanhamento	Por meio das ferramentas disponíveis para a gestão de demandas, por controle próprio da CONTRATANTE.
Periodicidade	Mensal.
Mecanismo de Cálculo (métrica)	<p><b>IST = TRFP / TRRM</b></p> <p>Onde:</p> <p><b>IST</b> – Indicador de Suporte Técnico.</p> <p><b>TRFP</b> – Total de Requisições Fora do Prazo – corresponde ao total de requisições do mês de referência não atendidas ou atendidas fora do prazo.</p> <p><b>TRRM</b> – Total de Requisições Registradas no Mês – corresponde ao total de requisições abertas no mês de referência.</p> <p>O prazo de solução do chamado técnico será contado a partir da comunicação, por telefone, e-mail ou registro em sistema para a abertura do chamado técnico na central de atendimento da CONTRATADA.</p>

<b>Observações</b>	<p>Obs 1: Não se aplicará este indicador as requisições interrompidas ou canceladas por solicitação da CONTRATANTE.</p> <p>Obs 2: Não serão contabilizados os atrasos nos quais a CONTRATANTE tenha contribuído para tal.</p> <p>Obs 3: Caso a CONTRATADA dependa de alguma ação do fabricante da solução, o tempo poderá ser descontado desde que evidenciado no processo.</p>
<b>Início de Vigência</b>	A partir da instalação da solução.
<b>Faixas de ajuste no pagamento e Sanções</b>	<p>Para valores do indicador IST:</p> <p>De 0 a 0,10 – Meta atingida.</p> <p>De 0,11 a 0,20 – Multa de 0,1% sobre o valor do contrato.</p> <p>De 0,21 a 0,30 – Multa de 0,3% sobre o valor do contrato.</p> <p>De 0,31 a 0,50 – Multa de 0,5% sobre o valor do contrato.</p> <p>De 0,51 a 1,00 – Multa de 0,7% sobre o valor do contrato.</p> <p>Acima de 1 – Será aplicada multa de 5% sobre o valor do contrato, garantida ampla defesa e o contraditório.</p>

## 7.7. Liquidação

7.7.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

7.7.2. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.,

7.7.3. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

1. o prazo de validade;
2. a data da emissão;
3. os dados do contrato e do órgão contratante;
4. o período respectivo de execução do contrato;
5. o valor a pagar; e
6. eventual destaque do valor de retenções tributárias cabíveis.

7.7.4. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante.

7.7.5. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

7.7.6. A Administração deverá realizar consulta ao SICAF para:

- a) verificar a manutenção das condições de habilitação exigidas no edital;
- b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas. (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018)

7.7.7. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

7.7.8. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.7.9. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

7.7.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

## **7.8. Prazo de pagamento**

7.8.1. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior.

7.8.2. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do Índice Geral de Preços Mercado (IGP-M) de correção monetária.

## **7.9. Forma de pagamento**

7.9.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

7.9.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.



7.9.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

7.9.4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

7.9.5. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

## **7.10. Cessão de Crédito**

7.10.1. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.

7.10.2. As cessões de crédito não fiduciárias dependerão de prévia aprovação do contratante.

7.10.3. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

7.10.4. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, tudo nos termos do Parecer JL-01, de 18 de maio de 2020.

7.10.5. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

7.9.6. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do contratado.

## **8. Critérios de seleção do fornecedor**

**8.1.** O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, para REGISTRO DE PREÇOS com adoção do critério de julgamento pelo MENOR PREÇO GLOBAL.

**8.2.** Considerando que a presente contratação se baseia no licenciamento pelo número de usuários ativos, o que pode variar no tempo, a depender das chegadas e saídas de colaboradores em

decorrência da situação de Ministério “recém-criado” vivenciada pelo MinC, entendemos que a adoção do Sistema de Registro de Preços é a que mais se adequa à “imprevisibilidade” do consumo, nos termos dos incisos II e V do art. 3º do Decreto nº 11.462/2023, a saber (grifo nosso):

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

*II - quando for conveniente a **aquisição de bens com previsão de entregas parceladas** ou contratação de serviços remunerados por unidade de medida, como quantidade de horas de serviço, postos de trabalho ou em regime de tarefa;*

*(...)*

*V - quando, pela natureza do objeto, **não for possível definir previamente o quantitativo a ser demandado** pela Administração.*

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

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

**8.4.1.** O prazo de vigência da Ata de Registro de Preços será de um ano, e poderá ser prorrogado por igual período, desde que comprovado que o preço é vantajoso, conforme dispõe o art. 22 do Decreto nº 11.462/2023.

#### **8.5. Da Adesão a Ata de Registro de Preços**

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

### **Deveres e Responsabilidades do Órgão Gerenciador da Ata de Registro de Preços**

**8.6.** Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços.

**8.7.** Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados.

**8.8.** Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

- a. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e
- b. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável.

**8.9.** Definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

- a. definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;
- b. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participante
- c. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a re

**8.10.** Aplicar as penalidades por descumprimento do pactuado na Ata de Registro de Preços.

### **Regime de execução**

**8.11.** O regime de execução do contrato será o de empreitada por preço unitário

**Exigências de habilitação**

**8.12.** Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

**Habilitação jurídica**

**8.13. Pessoa física:** cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

**8.14. Empresário individual:** inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

**8.15. Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

**8.16. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI:** inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

**8.17. Sociedade empresária estrangeira:** portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme [Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020](#).

**8.18. Sociedade simples:** inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

**8.19. Filial, sucursal ou agência de sociedade simples ou empresária:** inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

**8.20. Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o [art. 107 da Lei nº 5.764, de 16 de dezembro 1971](#).

**8.21.** Ato de autorização para o exercício da atividade de licenciamento/subscrição de licenças, expedido pelo fornecedor/fabricante dos softwares.

**8.22.** Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

**Habilitação fiscal, social e trabalhista**

**8.23.** Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

**8.24.** Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da [Portaria Conjunta nº 1.751, de 02 de outubro de 2014](#), do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

**8.25.** Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

**8.26.** Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo [Decreto-Lei nº 5.452, de 1º de maio de 1943](#);

**8.27.** Prova de inscrição no cadastro de contribuintes Estadual/Distrital ou Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

**8.28.** Prova de regularidade com a Fazenda [Estadual/Distrital] ou [Municipal/Distrital] do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

**8.29.** Caso o fornecedor seja considerado isento dos tributos Estadual/Distrital ou Municipal/Distrital relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

**8.30.** O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

### **Qualificação Econômico-Financeira**

**8.31.** Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação ([art. 5º, inciso II, alínea "c", da Instrução Normativa Seges/ME nº 116, de 2021](#)), ou de sociedade simples;

**8.31.1** A exigência da certidão negativa de insolvência civil visa garantir que os licitantes estejam em boa situação financeira e não tenham pendências civis que possam comprometer a execução do contrato. Isso assegura que a pessoa jurídica ou sociedade simples participante da licitação possui a capacidade financeira necessária para cumprir com as obrigações contratuais, minimizando riscos de inadimplência ou interrupção dos serviços contratados, condição importante uma vez que trata-se de uma contratação que tem possibilidade de durar mais de um exercício financeiro.

**8.32.** Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - [Lei nº 14.133, de 2021, art. 69, caput, inciso II](#));

**8.32.1** A certidão negativa de falência é fundamental para confirmar que o fornecedor não está em processo de falência, o que poderia comprometer sua capacidade de executar o contrato. A verificação da saúde financeira da empresa contratada é essencial para garantir a continuidade e a qualidade dos serviços prestados, prevenindo riscos de interrupções devido a dificuldades financeiras, uma vez que a contratada deverá garantir uma boa relação com o fornecedor da solução a ser licenciada e disponibilizada para esta Pasta, arcando com renovações e ampliações dos serviços ao longo dos exercícios que perdurarem a contratação.

**8.33.** Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

**8.33.1.** Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

**8.33.1.1** Ressalta-se que ao exigir índices de liquidez e solvência superiores a 1 demonstra que a empresa possui uma boa saúde financeira, com capacidade para

honrar suas obrigações de curto e longo prazo. Isso é crucial para assegurar que a empresa tem recursos financeiros suficientes para realizar o contrato de forma eficiente e sem interrupções.

**8.33.2.** As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura;

**8.33.2.1** Permitir que empresas recém-criadas substituam os demonstrativos contábeis pelo balanço de abertura promove a inclusão de novas empresas no processo licitatório, incentivando a competição e a inovação. No entanto, essas empresas ainda precisam atender às demais exigências de habilitação, garantindo que possuem estrutura e capacidade financeira para executar o contrato.

**8.33.3.** Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.,

**8.33.3.1** Para empresas constituídas há menos de dois anos, a limitação da exigência de documentos contábeis ao último exercício é uma medida razoável, visto que essas empresas podem não ter um histórico financeiro completo. Isso visa equilibrar a necessidade de verificação financeira com a viabilidade de participação dessas empresas no processo licitatório.

**8.33.4.** Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

**8.33.4.1** Alinhar a exigência de documentos contábeis aos limites definidos pela Receita Federal garante conformidade com as normas fiscais e tributárias brasileiras. a exigência visa facilitar a auditoria e verificação das informações financeiras, assegurando a transparência e a legalidade do processo licitatório.

**8.34.** Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido mínimo de 10% do valor total estimado da contratação.

**8.34.1** A exigência de patrimônio líquido mínimo de 10% do valor total da contratação para empresas com índices financeiros abaixo de 1 visa mitigar riscos financeiros. Essa medida garante que, mesmo que os índices de liquidez ou solvência estejam abaixo do ideal, a empresa tem uma reserva financeira suficiente para suportar as obrigações contratuais, reduzindo o risco de inadimplência ou falha na execução do contrato.

**8.35.** As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

**8.35.1** A permissão para que empresas recém-criadas utilizem o balanço de abertura em vez dos demonstrativos contábeis visa garantir com que essas novas empresas possam participar da licitação, promovendo a competição. No entanto, essas empresas ainda devem cumprir todas as demais exigências de habilitação, assegurando que possuem a capacidade técnica e financeira para executar o contrato.

**8.36.** O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

**8.36.1** A exigência de uma declaração assinada por um profissional habilitado da área contábil garante a veracidade e a precisão das informações financeiras fornecidas pela empresa licitante. Isso assegura que os dados apresentados são auditáveis e confiáveis, proporcionando maior segurança e transparência no processo de avaliação da capacidade financeira dos licitantes.

### **Habilitação Técnica**

**8.37.** Apresentar Atestado de Capacidade Técnico-Operacional, fornecido por pessoa jurídica de direito público ou privado, demonstrando que a proponente prestou serviços/fornecimentos compatíveis com o objeto pretendido, da seguinte forma:

8.37.1 Para fins de compatibilidade, considera-se atividade pertinente ao objeto licitado para o fornecimento de Solução para segurança e governança de dados com identificação e classificação de informações sensíveis, da mesma natureza e compatível com o objeto descrito no Termo de Referência, incluindo os serviços de configuração, suporte e manutenção da solução, contemplando 50% do volume de usuários previstos pela presente contratação.

8.37.2 Para a comprovação do atendimento das especificações técnicas, a LICITANTE deverá apresentar, juntamente com sua proposta comercial, documento detalhando as informações, local, site, páginas, documento, etc, necessários para aferição e atendimento de todos os itens da especificação técnica, ou seja, deverá apresentar uma espécie de índice ou planilha ponto-a-ponto, indicando o item, o documento que atende a especificação (nome do mesmo), o local onde está disponibilizado o documento (URL, Site, ou outro disponibilizado de forma digital), a página, e o texto que comprova o atendimento ao item.

a) A exigência de um documento detalhando as informações necessárias para a verificação das especificações técnicas garante transparência e facilita a validação das capacidades da empresa, assegurando que todos os critérios exigidos serão atendidos.

8.37.3. O(s) atestado(s)/declaração(ões) solicitados deverá(ão) ser apresentado (s) em papel timbrado, assinado(s) por autoridade ou representante de quem o(s) expediu, com a devida identificação.

a) A apresentação de atestados ou declarações em papel timbrado, assinados por autoridade competente, adiciona um nível de autenticidade e credibilidade às informações fornecidas pela empresa, garantindo a veracidade dos dados apresentados.

**8.38.** Declaração emitida pelo fabricante, especifica para este certame, de que a LICITANTE é uma parceira autorizada, demonstrando, desta forma, estar habilitada comercializar o objeto deste Termo de Referência e prestar serviços de instalação e suporte técnico.

**8.38.1** A declaração do fabricante confirmando que a licitante é uma parceira autorizada demonstra que a empresa está oficialmente capacitada para comercializar, instalar e prestar suporte técnico para a solução proposta, garantindo a legitimidade e a capacidade operacional da empresa contratada.

**8.39.** O CONTRATANTE reserva-se o direito de realizar diligências, a qualquer momento, com o objetivo de verificar se a(s) declaração(s) e demais documentos são adequados e atendem às exigências contidas neste documento. A realização de diligências buscará sanar eventuais dúvidas no entendimento das informações atestadas.

**8.40.** No caso de participação de cooperativas, será exigida a seguinte documentação complementar:

8.40.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos [arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971](#);

8.40.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

8.40.3. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

8.40.4. O registro previsto na [Lei n. 5.764, de 1971, art. 107](#);

8.40.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

8.40.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa:

- a) ata de fundação;
- b) estatuto social com a ata da assembleia que o aprovou;
- c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia;
- d) editais de convocação das três últimas assembleias gerais extraordinárias;
- e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e
- f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

8.40.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o [art. 112 da Lei n. 5.764, de 1971](#), ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

## **Dos Consórcios**

**8.41.** Conforme disposto no art. 15 da Lei nº 14.133, a regra é a permissão de participação de empresas consorciadas, senão vejamos:

*"Art. 15. Salvo vedação devidamente justificada no processo licitatório, pessoa jurídica poderá participar de licitação em consórcio, observadas as seguintes normas:"*

**8.42.** Desta forma, não há óbice técnico ou legal para justificar a referida vedação, ficando, portanto, permitida a participação de empresas reunidas em consórcio ou ainda em forma de sociedade cooperativa, desde que atendidos todos os requisitos legais.

## **Da Prova de Conceito**

**8.43.** A critério do MinC, poderá ser solicitado à licitante vencedora que realize prova de conceito, a fim de verificar se a Solução de TIC apresentada pela Licitante detém os requisitos mínimos necessários para realização dos serviços a serem contratados, conforme definido no Apêndice III deste Termo de Referência.

**8.44.** A solução apresentada que não atender as exigências do Estudo Técnico Preliminar e deste Termo de Referência e seus anexos, será considerada inapta, estando, portanto, desclassificada a licitante vencedora, sendo convocada a licitante seguinte na ordem classificatória para realização de prova de conceito e assim sucessivamente até que uma das licitantes participantes apresente solução que atenda plenamente às exigências deste documento.

**8.45.** A Prova de Conceito – POC consiste na validação das informações da Proposta - Nível de Atendimento aos Requisitos da PROPONENTE classificada em primeiro lugar na etapa de lances, a partir da observação do funcionamento prático da Solução ofertada (software), demonstrado pela PROPONENTE, sem ônus ao MinC.

**8.46.** O Licitante declarado vencedor da etapa de lances deverá efetuar, no terceiro dia útil seguinte à realização da sessão pública de pregão eletrônico, demonstração técnica da solução ofertada, objeto deste certame, que deverá contemplar os requisitos previstos no Apêndice III deste Termo de Referência.

**8.47.** A demonstração técnica da solução deverá apresentar plena operacionalidade, no ato da apresentação, sem a necessidade de customizações ou adequações posteriores.

**8.48.** A Prova de Conceito deverá ser realizada nas instalações do MinC, em Brasília/DF.

**8.49.** A proponente terá à sua disposição ponto de banda larga de internet, sendo os equipamentos necessários à demonstração de responsabilidade da proponente.

**8.50.** O tempo máximo de demonstração técnica será de 02 (duas) horas, prorrogáveis, a critério da Comissão Técnica avaliadora, se esta o julgar necessário.

**8.51.** A validação das informações constantes da Proposta dar-se-á por meio da demonstração prática da execução das atividades relacionadas no Apêndice III deste Termo de Referência.

**8.52.** Para a sessão pública virtual da prova de conceito, o MinC deverá disponibilizar sala virtual, sem necessidade de senha de acesso a qualquer interessado em acompanhar a POC.

**8.53.** Embora o acesso seja livre para qualquer pessoa, esta deverá se identificar pelo chat no momento do acesso, informando o nome completo, CPF, e-mail e telefone de contato e o CNPJ e a razão social caso esteja representando alguma empresa, mantendo também a câmera de vídeo ligada durante o acesso.

**8.54.** A comissão de licitação gerenciará a abertura de áudio e a coordenação dos trabalhos e participações, sendo assegurado o registro de manifestação no chat da sala de reunião por escrito, que deverá ser lavrada em ata, sempre que solicitado.

**8.55.** A PROPONENTE que não cumprir os requisitos do Estudo Técnico Preliminar (Apêndice I deste Termo de Referência), do Caderno de Especificações Técnicas (Apêndice II deste Termo de Referência) e do roteiro de POC (Apêndice III deste Termo de Referência) será desclassificada pela Comissão Técnica avaliadora e não terá direito a qualquer indenização.

**8.56.** A PROPONENTE não comparecendo em dia e hora previamente agendados para a realização da Sessão Pública da Prova de Conceito – POC, será automaticamente reprovada pela Comissão Técnica avaliadora.

**8.57.** Ao final da Prova de Conceito – POC, a Comissão Técnica avaliadora do MinC registrará em Ata o resultado e encaminhará ao Pregoeiro e à sua Equipe de Apoio.



## 9. Estimativas do Valor da Contratação

**Valor (R\$):** 12.914.695,00

**9.1.** O custo estimado total do registro de preços é de **R\$ 12.914.695,00** (doze milhões, novecentos e quatorze mil, seiscentos e noventa e cinco reais).

**9.2.** Em se tratando de licitação para Registro de Preços, os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

9.2.1. em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

9.2.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

9.2.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o Índice de Custo da Tecnologia da Informação (ICTI);

9.2.4. os reajustes a que a Contratada fizer jus e não forem solicitados durante a vigência do contrato, serão objeto de preclusão com a assinatura da prorrogação contratual ou com encerramento do contrato.

## 10. Adequação orçamentária

**10.1.** As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

10.1.1. A contratação será atendida pela seguinte dotação:

I) Gestão/Unidade: 420020-00001;

II) Fonte de Recursos: 100;

III) Programa de Trabalho: 42101.13.122.0032.2000.0001 – Administração da Unidade;

IV) Elemento de Despesa: 33.90.40.06 (LOCACAO DE SOFTWARES) e 44.90.40.03 (SERVIÇOS TÉCNICOS PROFISSIONAIS DE TIC);

V) Plano Interno: a CGOFC informará o PI para cada empresa (contrato);

**10.2.** A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

## 11. Responsáveis

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

Despacho: PORTARIA SPOA Nº 141, DE 19 DE JULHO DE 2024

**WALLACE MOREIRA BASTOS**

Integrante Requisitante



*Assinou eletronicamente em 12/11/2024 às 14:38:47.*

Despacho: PORTARIA SPOA Nº 141, DE 19 DE JULHO DE 2024

**RAMON LEONN VICTOR MEDEIROS**

Integrante Técnico



*Assinou eletronicamente em 12/11/2024 às 14:43:00.*

Despacho: PORTARIA SPOA Nº 141, DE 19 DE JULHO DE 2024

**GUSTAVO RIBEIRO DA ROCHA**

Integrante Administrativo



*Assinou eletronicamente em 12/11/2024 às 14:41:15.*

## Lista de Anexos

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

- Anexo I - Apendice I - ETP68\_2024.pdf (589.04 KB)
- Anexo II - Apendice II - Caderno de Especificacoes Tecnicas.pdf (326.01 KB)
- Anexo III - Apendice III - Roteiro POC.pdf (141.62 KB)

**Anexo I - Apendice I - ETP68\_2024.pdf**

# Estudo Técnico Preliminar 68/2024

## 1. Informações Básicas

Número do processo: 01400.019209/2023-00

## 2. Descrição da necessidade

**Solução de segurança da informação para auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (Microsoft Active Directory), correio eletrônico (Microsoft Exchange Server) e servidores de arquivos.**

2.1 Com a publicação do Decreto nº 10.359, de 20 de maio de 2020, foi efetivada a transferência da Secretaria Especial da Cultura (SECULT), com suas 5 Secretarias Nacionais e um legado de cerca de 89 sistemas ou portais, para o Ministério do Turismo. Somadas as 3 Secretarias Nacionais da área de Turismo, com cerca de 43 sistemas ou portais ativos, essa transferência elevou significativamente as demandas por soluções de TIC.

2.2. Após a publicação do decreto 11.336/2023, que recria o Ministério da Cultura (MinC), este novamente passa a ter o papel de planejamento, administração geral, normatização, pesquisa e tratamento de dados relacionados com a política nacional de cultura e política nacional das artes, proteção do patrimônio histórico, artístico e cultural, regulação dos direitos autorais, 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, proteção e promoção da diversidade cultural, desenvolvimento econômico da cultura e a política de economia criativa, desenvolvimento e a implementação de políticas e ações de acessibilidade cultural e formulação e implementação de políticas, de programas e de ações para o desenvolvimento do setor museal. Este grande volume de informação serve de parâmetro para planejar os recursos e ações, proporcionam o mapeamento das deficiências culturais, indicação das principais necessidades atendidas e a hierarquia dessas necessidades, proporcionando, assim, maior efetividade na ação pública.

2.3. O alcance dos seus objetivos está aliado a necessidade da ampla utilização, processamento e armazenamento de informações, como por exemplo: planejar, coordenar, monitorar e avaliar políticas, programas, projetos e ações para a promoção da diversidade cultural brasileira, executar ações relativas à celebração de convênios, acordos e outros instrumentos congêneres que envolvam a transferência de recursos do Orçamento Geral da União, no âmbito de sua área de atuação. Para que possa atender às inúmeras demandas depende dos recursos de Tecnologia da Informação, que possibilitam o adequado exercício de suas atribuições regulamentares, de forma a maximizar os resultados pretendidos com suas políticas à luz dos princípios da disponibilidade, da segurança e da governança de dados contidos em seus repositórios.

2.4. O uso da Tecnologia da Informação e Comunicação (TIC) como recurso para a otimização dos serviços possibilita ao ministério prover medidas que torne seus procedimentos cada vez mais ágeis, seguros, integrados, eficientes e, sobretudo, acessíveis aos usuários.

2.5. Para prover todos os serviços prestados por meio de recursos de TIC, o MinC produz e dispõe de um grande volume de documentos em meio digital. Esses documentos estão em diretórios, servidores, e-mails acessíveis na rede do Ministério e contêm dados e informações sensíveis e estratégicas, inclusive atrelados a LGPD.

2.6. Um grande risco para as atividades desenvolvidas por qualquer empresa é que os sistemas computacionais se tornem indisponíveis, colocando em risco as operações e em dúvida a confidencialidade e a integridade dos dados armazenados. Com os sistemas cada vez mais “online” e usuários acessando uma infinidade de aplicativos Web ou remotos, faz-se necessária a implementação de controles e políticas de segurança da informação que garantam a disponibilidade, confidencialidade e a integridade das informações corporativas. Mitigando inclusive possíveis ataques cibernéticos, como o sequestro e criptografia de dados, conhecido como: *Ransomware*.

2.7. O crescimento dos incidentes de segurança e a evolução das ameaças à rede tecnológica, exigem a continuidade e elevado nível de proteção da rede de dados, minimizando os incidentes no âmbito da estrutura organizacional. Dados coletados pela Fortinet, através de sua plataforma que coleta e analisa incidentes de segurança cibernética em todo o mundo, apontaram que o Brasil é o segundo país que mais sofre ataques cibernéticos na América Latina, foram registradas mais de 31,5 bilhões de tentativas de ataques cibernéticos no primeiro semestre de 2022, um aumento de 94% considerando o mesmo período de 2021. No total, a região da América Latina e Caribe sofreram 137 bilhões de tentativas de ataques cibernéticos.

2.8. Diante deste cenário alarmante, o governo brasileiro publicou o Decreto nº 10.222, de 5 de fevereiro de 2020, criando a Estratégia Nacional de Segurança Cibernética (E-Cyber), com o objetivo de tornar o país seguro e proteger o espaço cibernético. As normativas visam aumentar a resiliência aos ataques cibernéticos e fortalecer a atuação brasileira em segurança online no cenário internacional. Adicionalmente a essa regulamentação tem-se a necessidade de atendimento a Lei Geral de Proteção de dados pessoais e o alinhamento a Política Nacional de Segurança da Informação.

2.9. O elevado volume de informações e comunicações eletrônicas do MinC e a sua importância para planejamento, divulgação e acessibilidade da cultura no Brasil, conduzem à necessidade da preservação das informações e dos equipamentos (pelos seus valores financeiro, informativo, probatório e histórico) com a devida segurança e qualidade com um ambiente adequado à sua destinação.

2.10. Os últimos ataques a diversos órgãos e instituições públicas brasileiras apontam para a urgência em adotar soluções para monitoramento, governança e auditoria das ocorrências de acesso e uso das informações no ambiente tecnológico, buscando garantir a segurança das informações e o funcionamento dos serviços prestados.

2.11. A solução tecnológica a ser futuramente contratada tangencia o tema relacionado a Governança de dados, na medida em que permitirá uma complementariedade em relação a estratégia de segurança e políticas regulatórias da LGPD já adotada por essa administração. Dada a complexidade das soluções de segurança da informação disponíveis no mercado, há que se considerar uma abordagem multidimensional para garantir auditoria, controle, rastreabilidade e privacidade dos dados custodiados.

2.12. Isto porque, cada solução possui uma abordagem distinta e, embora possam tangenciar aspectos e conceitos similares para a proteção de dados, suas funcionalidades, recursos e aplicações podem ter aplicabilidades distintas e por muitas vezes complementares.

2.13. Dentre os diversos conceitos que envolvem a governança e segurança de dados, inúmeros fabricantes/desenvolvedores possuem abordagens distintas para prover:

a. 1.

Monitoramento de Dados Sensíveis;

b. 2.

Prevenção contra vazamento de dados;

c. 3.

Monitoramento e Controle de Acesso ao ambiente computacional;

d. 4.

Monitoramento e Controle de Políticas de segurança Personalizáveis;

e. 5.

Auditoria e Relatórios;

f. 6.

Detecção de Ameaças Internas e Integração

2.14. Deste modo, a abordagem das diferentes soluções disponíveis pode ser distinta em função dos mecanismos de segurança e proteção de cada ferramenta ou solução.

2.15. Tal contextualização é importante para que seja justificado, de maneira clara, que a solução pretendida na presente contratação, embora possa tangenciar determinados requisitos de soluções tecnológicas já instaladas no parque computacional dessa administração, a exemplo de soluções de software de prevenção de perda e vazamento de dados, também conhecida como soluções de DLP (Data Loss Prevention), não representa uma redundância ou sobreposição de tecnologias da mesma natureza, mas sim uma complementariedade e abordagem mais ampla no tema, já que o foco dos recursos, funcionalidades e ferramentas da solução a ser contratada está na governança, auditoria e gerenciamento de riscos voltados a segurança da informação.

2.16. De maneira objetiva, diferentemente das abordagens padrões das soluções já instaladas, que reagem passivamente as políticas de segurança já estabelecidas, a pretendida contratação permitirá um foco na prevenção de riscos por meio de uma análise preditiva e uma gestão proativa destes dados, permitindo uma suplementação na estratégia de segurança, não tratando apenas de vulnerabilidades e riscos e servindo, inclusive, ao propósito de controle e visibilidade das soluções de segurança já implementadas.

2.17. Dito de outro modo, enquanto soluções de DLP definem o perímetro de proteção, monitoram endpoints e criam rotinas e regras rígidas a serem seguidas, a solução a ser contratada fornecerá uma visão detalhada de todos os acessos, "permissionamentos", dados expostos e proprietário dos dados.

2.18. Sendo assim, ao identificar e monitorar os acessos, quais dados estão expostos e quem os utiliza, a solução incrementará o conhecimento da rede sem estar fixa em regras rígidas, monitorando o acesso legítimo e eventuais vazamentos, bem como permitindo a responsabilização assertiva destes acessos que, por mais que permitidos, por vezes podem ser utilizados de forma maliciosa.

2.19. Nesse cenário, cumpre reforçar que a solução não se limitará a reforçar políticas existentes, mas irá guiar a criação de novas políticas para as soluções já instaladas, garantindo uma

inteligência proativa na governança de dados por meio de uma compreensão profunda do ecossistema de dados obtidas através da análise de comportamentos. O resultado da presente contratação, que será atingido de forma complementar as soluções e investimentos já realizados nesse campo, será uma infraestrutura de segurança de dados não apenas reativa, mas também preventiva, que não só responderá às ameaças e proibição de ações dos usuários, mas irá antecipar ações maliciosas, as neutralizando com eficiência.

2.20. Ao tratarmos da expressão governança proativa de dados, temos que considerar que soluções convencionais entram em ação depois que um risco é detectado, já a solução a ser contratada deverá oferecer uma abordagem proativa, não só alertando sobre atividades suspeitas, mas também evitando acessos não autorizados antes que eles se tornem um problema, por meio de um modelo de governança de dados e resposta a incidentes que, em caso de uma violação de segurança, deverá garantir uma resposta rápida e informada devido à sua capacidade de fornecer contextos detalhados sobre a exposição dos dados, contribuindo para mitigar danos potenciais de forma complementar e mais ágil que as soluções já instaladas, que podem não ter toda a informação necessária sobre os dados afetados.

2.21. Outras funcionalidades dentro dos conceitos básicos de proteção e segurança da informação que serão abordadas e complementares as soluções já instaladas são:

- a. 1.  
identificação de permissões excessivas ou antigas;
- b. 2.  
remediação de forma automática dados expostos;
- c. 3.  
automatização do processo de limpeza de credenciais e permissões antigas, minimizando a exposição de dados
- d. 4.  
integração com as soluções de DLP na classificação da informação, marcando os arquivos como sensíveis, abertos ou sigilosos possibilitando ao DLP o bloqueio de envio destes arquivos;
- e. 5.  
responsabilização dos responsáveis por vazamentos dos dados através da auditoria por longos períodos;
- f. 6.  
capacidade de prever acessos que, embora permitidos, podem apresentar riscos;
- g. 7.  
validação e aprimoramento a criação de políticas para o DLP;
- h. 8.  
consolidar as defesas contra a exposição de dados.



2.22. Pelo exposto, ratifica-se a pertinência da demanda considerando a importância do serviço para o cumprimento da missão institucional do MinC para o alcance dos objetivos estratégicos da empresa.

2.23. Desta forma, a contratação está aderente às diretrizes estabelecidas no Plano Diretor de Tecnologia da Informação e Comunicação – PDTI (2023 – 2027), alinhado a estratégia do MinC.

### 3. Área requisitante

Área Requisitante	Responsável
Divisão de Segurança da Informação	Ramon Medeiros

### 4. Necessidades de Negócio

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

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

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

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

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

### 5. Necessidades Tecnológicas

1.

5.1. Os dados não estruturados, tais como, arquivos e e-mails, estão dispostos no ambiente computacional em base de armazenamento de informação sobre usuários, dispositivos e sistemas (Active Directory), Servidores de arquivos (Windows File Services). Sendo assim, é necessário que a solução tecnológica possibilite gerir, monitorar, automatizar e remediar os acessos dados não estruturados.

2. 5.2. Aprimorar a política de Classificação de dados baseada em conteúdo e análise da segurança com base no comportamento do usuário correlacionando-os de forma a possibilitar a identificação de riscos e ajuste das mesmas com informações de quem utiliza e como utiliza as informações sensíveis do Ministério

3.

5.3. Gestão centralizada e possibilidade de automação de procedimentos de segurança.

4.

5.4. Monitoramento, governança e auditoria aplicada à proteção de dados.

5.

5.5. Garantia de atualização e correção de falhas identificadas na solução durante o período do contrato.

5.6. Suporte técnico para apoio na solução de ocorrências e na operação da solução.

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

### **6.1. Requisitos Legais**

6.1.1. Este Estudo se baseia, dentre outras, nas seguintes legislações e respectivas alterações posteriores:

1.

a. 1.1.

Lei n.º 14.133/2021 – Lei de Licitações e Contratos Administrativos;

b. 1.2.

Decreto nº 11.462/2023 e suas alterações – Regulamenta os art. 82 a art. 86 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o sistema de registro de preços para a contratação de bens e serviços, inclusive obras e serviços de engenharia, no âmbito da Administração Pública federal direta, autárquica e fundacional;

c. 1.3.

Lei nº 13.709/2018: Lei Geral de Proteção de Dados Pessoais (LGPD)

d. 1.4.

Decreto n.º 10.024/2019 - Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal;

e. 1.5.

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 - SISP do Poder Executivo Federal;

f. 1.6.

Portaria SGD/MGI 5.950 de 26 de outubro de 2023, 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;

g. 1.7.

Instrução Normativa SLTI/MPOG nº 01/2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências;

h. 1.8.

Instrução Normativa SEGES/ME nº 73, de 5 de agosto de 2020 – Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

## **6.2. Requisitos Gerais**

6.2.1. A solução deverá estar em conformidade com as legislações correlatas e permitir o atendimento a Lei Geral de Proteção de Dados (LGPD).

6.2.2. A solução deve ser entregue em funcionamento, dessa forma, serão contemplados todos os serviços de instalação e configuração de todos os componentes adquiridos, sem ônus para o contratante.

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

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

6.2.5. Deverá ser considerado no Termo de Referência a possibilidade de apresentação de uma prova de conceito/teste de bancada para assegurar o atendimento aos requisitos funcionais indicados no projeto.

## **6.3. Requisitos Temporais**

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

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

## **6.4. Requisitos de Segurança**

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

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

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

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

## **6.5. Requisitos Sociais, Ambientais e Culturais**

6.5.1. Requisitos Sociais: Na execução de tarefas no ambiente do MinC, os funcionários da Contratada deverão observar, no trato com os servidores e o público em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público. Deverão ainda portar identificação pessoal, conforme as normas internas da Instituição.

### **6.5.2. Requisitos Ambientais**

a) Os serviços prestados pela Contratada deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e material consumidos, bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pelo MinC.

b) A Contratada deverá atender, quando da execução do objeto do contrato, os critérios de sustentabilidade ambiental previstos na legislação pertinente, quando couber.

c) As configurações de hardware e software deverão ser executadas visando alto desempenho com o uso racional de energia, evitando-se a sobrecarga de equipamentos ou dispositivos elétricos.

6.5.3. Requisitos Culturais: Toda a documentação produzida e/ou fornecida pela Contratada referente ao objeto deverá estar preferencialmente no idioma português-BR, de forma clara e objetiva.

## **6.6. Requisitos de Projeto e Implementação**

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

## **6.7. Requisitos de Garantia Técnica**

6.7.1. O prazo de garantia dos serviços, que não envolvam reposição de componentes ou dispositivos, será de 90 (noventa) dias. Caso o serviço tenha que ser refeito dentro deste período, o ônus correrá por conta da Contratada.

6.7.2. O direito do MinC à garantia técnica cessará caso a solução seja alterada pela próprio MinC ou por fornecedores que não a Contratada e/ou Fabricante responsável pelo serviço em questão.

6.7.3. Para todos os itens da solução a garantia será de por todo o período de licenciamento diretamente pelo fabricante dos softwares. O acesso para downloads de patches, drivers e quaisquer outras atualizações e/ou correções necessárias devem estar disponíveis 24x7 (vinte e quatro horas por dia, sete dias por semana), durante todo o período de garantia técnica, e podem ser feitos através de http ou ftp, no sítio do fabricante da solução.

. 1.

6.8. Requisitos de Experiência Profissional

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

- Para fins de compatibilidade, considera-se atividade pertinente ao objeto licitado para o fornecimento de Solução para segurança e governança de dados com identificação e classificação de informações sensíveis, da mesma natureza e compatível com o objeto descrito no Termo de Referência, incluindo os serviços de configuração, suporte e manutenção da solução, contemplando, no mínimo 50% do volume de usuários contemplados pela presente contratação.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. O Ministério da Cultura possui em seu Data Center diversas soluções para desempenho de suas atividades, atendendo aos 1.313 usuários e contas ativas, conforme levantamento realizado na ferramenta de gestão em 26/07/2024.

7.2. Deste modo, há que se considerar a possibilidade de expansão eventual do projeto, na medida em que novos usuários podem surgir ao longo do contrato, isto porque, quanto maior o volume de usuários protegidos pela solução, maior a garantia da estratégia de governança e segurança de dados.

7.3. Sendo assim, consideramos uma margem de crescimento eventual de 15% no número usuários ao longo da vigência da ARP, totalizando um volume de 1500 usuários.

ITEM	DESCRIÇÃO	CATSER	MÉTRICA	QTDE
1	Solução de segurança da informação para auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (Microsoft Active Directory), correio eletrônico (Microsoft Exchange Server) e servidores de arquivos pelo período de 36 meses.	27502	Licença de Uso (por usuário)	1.500
2	Serviços de Instalação e Configuração da solução.	26972	Serviço	01
3	Serviço de Treinamento.	3840	Turma	01

## **8. Levantamento de soluções**

### **8.1. Identificação das Soluções**

8.1.1. Após pesquisas realizadas, apresentamos abaixo os resultados de processos em que houve a contratação de soluções análogas, podendo ser utilizadas para fins comparativos de execução, modelo de contratação e valores praticados, respeitadas as particularidades de integração, implementação e manutenção necessárias ao projeto desenvolvido por este Ministério, conforme abaixo:

- a) Solução 1: Contratação de solução de segurança da informação para auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (Microsoft Active Directory), correio eletrônico (Microsoft Exchange Server) e servidores de arquivos.
- b) Solução 2: Software Livre.
- c) Solução 3: Contratação de fábrica de software para desenvolvimento de solução proprietária para atendimento à demanda indicada.

## **9. Análise comparativa de soluções**

**9.1. Solução 1: Contratação de solução de segurança da informação para auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (Microsoft Active Directory), correio eletrônico (Microsoft Exchange Server) e servidores de arquivos.**

**9.1.1. Descrição:** Este modelo prevê a contratação de licenças de uso da solução, a serem instaladas no parque computacional da contratante.

### **9.1.2. Análise da Solução:**

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

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

9.1.2.3. Nesta modalidade de solução, para assegurar tal proteção, a licença da solução deve ser totalmente integrada ao ambiente tecnológico do MinC, incluindo aí todos os módulos e componentes que a compõem, visando a instituição de um ambiente homogêneo de monitoração, prevenção, análise, investigação, inteligência, defesa e resposta a incidentes.

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

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

### 9.1.3. Análise da Mercado:

9.1.3.1. Em relação ao estudo de soluções capazes de atender aos requisitos tecnológicos, apresentamos abaixo o resumo dos pontos analisados e a aderência das soluções de mercado.

9.1.3.2. Por meio do estudo analisado foi possível concluir que existem soluções capazes de atender as necessidades dessa administração em sua integralidade e outras que, embora tangenciem recursos e funcionalidades, não atendem integralmente o que se espera da solução.

9.1.3.3. O comparativo não pretende esgotar o levantamento das soluções disponíveis no mercado, mas sim oferecer informações suficientes quando a existência de soluções com características suficientes para atender a demanda.

		Safetica	SailPoint	Varonis	Netwrix /Stealthbits	Spirion
<b>Solução tecnológica para inspeção e segurança de informações institucionais on-premise</b>						
Geral	monitoramento, gerenciamento e inspeção dos dados não estruturados contidos e armazenados no ambiente físico	Sim	Sim	Sim	Sim	Sim
Active Directory	Auditoria de contas, computadores e grupos, auditoria de sites	Sim	Sim	Sim	Sim	Sim
	Descoberta de usuários, grupos e permissões nos repositórios de dados	Sim	Sim	Sim	Sim	Sim
	Visibilidade de arquivos expostos	Sim	Sim	Sim	Sim	Sim
	Descoberta de arquivos com informações sensíveis para proteção de dados	Sim	Sim	Sim	Sim	Sim
	Trilha forense de acesso aos dados, arquivos e pastas	Sim	Sim	Sim	Sim	Sim
	Trilha forense das atividades administrativas da equipe de TI e administradores da rede	Sim	Sim	Sim	Sim	Não
	GPO - Group Policy	Sim	Sim	Sim	Sim	Sim
	Execução de ações proativas com base na auditoria	Sim	Sim	Sim	Sim	Sim
	Execução ações em múltiplos objetos	Sim	Sim	Sim	Sim	Não

	Alertas com base nas informações auditadas	Sim	Sim	Sim	Sim	Sim
	Automatizar tarefas repetitivas comuns	Sim	Sim	Sim	Sim	Sim
	Automatizar tarefas repetitivas complexas	Sim	Sim	Sim	Sim	Sim
	Delegação de gerenciamento sobre grupos de segurança aos proprietários	Sim	Sim	Sim	Sim	Sim
	Monitoramento e análise de comportamento de usuários	Sim	Não	Sim	Sim	Sim
Servidores de Arquivos	Auditoria de acesso de arquivos e pastas	Sim	Sim	Sim	Sim	Sim
	Auditoria de modificação de arquivos e pastas	Sim	Sim	Sim	Sim	Sim
	Auditoria de remoção de arquivos e pastas	Sim	Sim	Sim	Sim	Sim
	Execução de ações proativas com base na auditoria	Sim	Sim	Sim	Sim	Sim
	Execução ações em múltiplos objetos	Sim	Sim	Sim	Sim	Sim
	Alertas com base nas informações auditadas	Sim	Sim	Sim	Sim	Sim
	Automatizar tarefas repetitivas comuns	Sim	Sim	Sim	Sim	Sim
	Automatizar tarefas repetitivas complexas	Sim	Sim	Sim	Sim	Sim
	Delegação de gerenciamento sobre grupos de segurança aos proprietários	Sim	Sim	Sim	Sim	Sim
	Monitoramento e análise de comportamento de usuários	Sim	Não	Sim	Sim	Sim
<b>Solução tecnológica para inspeção e segurança de informações institucionais em nuvem</b>						
Geral	monitoramento, gerenciamento e inspeção dos dados não estruturados contidos e armazenados no ambiente em nuvem Microsoft	Sim	Sim	Sim	Sim	Sim
	Monitoramento de todas as caixas postais	Sim	Sim	Sim	Sim	Sim
	Trilha forense de uso de uso dos repositórios em nuvem - Caixa postal	Sim	Sim	Sim	Sim	Sim



Arquivos em nuvem	Trilha forense de uso de uso dos repositórios em nuvem - SharePoint	Sim	Sim	Sim	Sim	Sim
	Trilha forense de uso de uso dos repositórios em nuvem - One Drive	Sim	Sim	Sim	Sim	Sim
	Identificação dos arquivos sensíveis exportados para a nuvem	Sim	Sim	Sim	Sim	Sim
	Estatísticas de uso dos arquivos, pastas, quantidade de usuários com acesso e efetivamente utilizam os repositórios da nuvem	Sim	Sim	Sim	Sim	Sim
	Monitoramento em console única e centralizada das permissões concedidas por meio da plataforma Teams, sem a necessidade de abertura de diversas interfaces	Sim	Sim	Sim	Sim	Sim
Exchange	Auditoria de acesso, modificação e remoção de caixas postais e listas	Sim	Sim	Sim	Sim	Sim
	Execução de ações proativas com base na auditoria	Sim	Sim	Sim	Sim	Sim
	Execução ações em múltiplos objetos	Sim	Sim	Sim	Sim	Sim
	Alertas com base nas informações auditadas	Sim	Sim	Sim	Sim	Sim
	Monitoramento e análise de comportamento de usuários	Sim	Não	Sim	Sim	Sim
	Descoberta e classificação de arquivos em repositórios não estruturados	Sim	Sim	Sim	Sim	Sim
	Identificação e classificação de conteúdos sensíveis	Sim	Sim	Sim	Sim	Sim
<b>Solução tecnológica para inspeção de comportamentos suspeitos, notificação e tomada de ações em tempo real</b>						
	Monitoramento de ações no ambientes on-premise e em nuvem	Sim	Sim	Sim	Sim	Sim
	Contextualização das ações nos repositórios tanto online e em nuvem	Sim	Sim	Sim	Sim	Não
	Identificação de abusos de uso	Sim	Sim	Sim	Sim	Não
	Alerta de comportamento de usuários, suspeitos, excessivos e abusivos dos repositórios de arquivos	Sim	Sim	Sim	Sim	Sim

Geral	Monitoramento dos tráfegos de web proxy	Sim	Sim	Sim	Sim	Não
	Auditoria e análise de comportamento de todas as requisições do DNS	Sim	Sim	Sim	Sim	Não
	Identificação de ameaças de túneis DNS	Sim	Sim	Sim	Sim	Não
	Monitoramento de todo o tráfego VPN, inclusive mapeando usuários, localidades e equipamentos comumente utilizados	Sim	Sim	Sim	Não	Sim
	Integração de visibilidade de ambientes em nuvem e on-premise em interface única	Sim	Sim	Sim	Sim	Sim
	Mapeamento de tentativas de movimentação lateral por meio de requisições DNS	Sim	Sim	Sim	Sim	Não
	Escalação de privilégio via AD	Sim	Sim	Sim	Sim	Não
<b>Atendimento aos requisitos mínimos</b>		<b>100%</b>	<b>94%</b>	<b>100%</b>	<b>98%</b>	<b>81%</b>

Fontes:

<https://www.safetica.com/products/products-features>

<https://www.sailpoint.com/platform/>

<https://www.varonis.com/pt-br/produtos/plataforma-de-seguranca-de-dados/>

<https://stealthbits.com/stealthintercept-product/>

<https://www.spirion.com/resources/?type=solutions-overview>

## 9.2. Solução 2: Software Livre

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

**9.2.2. Análise da Solução:** Após análise de mercado e com base nos requisitos técnicos funcionais da solução que se pretende contratar temos que soluções livres e softwares de código aberto, de igual modo não poderiam atender a integralidade do projeto, uma vez que demandariam integrações e modificações, sem contar os riscos associados a vazamento de bases de dados expostos em plataformas “open source”. Em consulta ao portal do software público brasileiro (<https://softwarepublico.gov.br/social>), realizada em Julho/2024, não foram identificadas soluções que atendessem aos requisitos técnicos e de negócio necessários.

## 9.3. Solução 3: Fábrica de Software

**9.3.1. Descrição:** Este modelo prevê desenvolvimento de solução proprietária.

**9.3.2. Análise da Solução:** Em relação ao desenvolvimento proprietário, utilizando recursos humanos e materiais do próprio Ministério, para composição de uma solução com base em softwares livres e/ou a contratação de fábrica de software que possa atender a demanda do presente estudo, cabe aqui justificar a inviabilidade de se projetar o investimento financeiro, neste cenário, haja vista que o desenvolvimento proprietário ou mesmo a fábrica de software levará em conta recursos humanos e materiais que, comprovadamente, não podem ser previstos em D-0 (momento antes de seu início), dada a complexidade e multidisciplinariedade desse escopo, sendo considerado neste cenário o custo/prejuízo que pode ser imputado ao Ministério ao longo do tempo de desenvolvimento, a exemplo de multas e riscos institucionais de não se implementar uma ferramenta que possa atender no curto prazo a demanda do projeto.

1.

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

**9.4.1 Pesquisa no Pannel de Preços**

9.4.1.1. Foi executada pesquisa de preços em Órgãos da Administração Pública, no site Pannel de Preços (<https://paineldepregos.planejamento.gov.br/>) e complementarmente no Portal de Compras (<https://www.gov.br/compras/pt-br>) , em conformidade com o disposto no art. 5º da IN SEGES/ME nº 73/2020, e no art. 11, incisos I e II da IN SGD/ME nº 1/2019 – previsões legais que visam garantir a observância dos princípios da economicidade e eficiência nas contratações de soluções de TI –, no período compreendido entre os dias 01/07 /2024 e 19/07/2024, sob responsabilidade da Equipe de Planejamento da Contratação, a fim de averiguar a existência de contratações similares à pretendida, e cuja execução ou conclusão não tenha ultrapassado 1 (um) ano ao período da pesquisa. Cite-se, portanto, a pesquisa realizada, para fins de cumprimento da norma e verificação posterior da vantajosidade do procedimento de contratação escolhido pelo MinC.

9.4.1.2 A pesquisa executada no site do Pannel de Preços teve como resultado:

ÓRGÃO	UASG	PREGÃO
Agência Nacional de Aviação Civil - ANAC	113214	29/2019
Agência Nacional de Águas e Saneamento Básico - ANA	443001	24/2020
Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES	154003	Contrato 46/2022
Tribunal Superior do Trabalho	80001	58/2021
Fundação Nacional de Saúde - FUNASA	2550	11/2022

9.5. Examina-se nesta seção, para cada solução identificada no item 8 deste Estudo Técnico, os aspectos previstos na IN SGD/ME nº 94/2022 que devem ser avaliados em uma contratação de TIC. Para efeito de estudo, foi realizada consulta ao catálogo de Software Público Brasileiro ([https://softwarepublico.gov.br/social/search/software\\_infos](https://softwarepublico.gov.br/social/search/software_infos)), onde efetivamente não foi possível identificar solução que pudesse vir a ser utilizada para atendimento às necessidades negociais do MinC, bem como aos requisitos tecnológicos identificados no presente Estudo Técnico, conforme observado nas figuras a seguir que apresenta o resultado da pesquisa no portal:

--	--	--	--	--

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

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

## 10. Registro de soluções consideradas inviáveis

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

10.1.1. **Solução 2: Software Livre:** Não há disponibilidade de solução de software livre capaz de atender aos requisitos técnicos nesse contexto. Esta solução apresenta alta complexidade, pois necessita de capacitação permanente da equipe de informática, falta de suporte técnico, baixa cobertura para malwares e não prevenção de novos incidentes de segurança. Além dessas dificuldades, o volume de tráfego de rede vem crescendo cada ano exigindo hardwares dedicados para essa função. Assim, esta opção está aos poucos sendo substituída por ferramentas pagas com suporte, gerenciamento unificado e garantia de funcionamento.

10.1.2. **Solução 3: Fábrica de Software:** Em relação ao desenvolvimento proprietário, utilizando recursos humanos e materiais do próprio Ministério, para composição de uma solução com base em softwares livres e/ou a contratação de fábrica de software que possa atender a demanda do presente estudo, cabe aqui justificar a inviabilidade de se projetar o investimento financeiro, neste cenário, haja vista que o desenvolvimento proprietário ou mesmo a fábrica de software levará em conta recursos humanos e materiais que, comprovadamente, não podem ser previstos em D-0 (momento antes de seu início), dada a complexidade e multidisciplinariedade desse escopo, sendo considerado neste cenário o custo/prejuízo que pode ser imputado ao Ministério ao longo do tempo de desenvolvimento, a exemplo de multas e riscos institucionais de não se implementar uma ferramenta que possa atender no curto prazo a demanda do projeto.

## 11. Análise comparativa de custos (TCO)

11.1. Das soluções apresentadas, a **Solução 1** - Contratação de solução de segurança da informação para auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (Microsoft Active Directory), correio eletrônico (Microsoft Exchange Server) e servidores de arquivos baseado em serviço foi considerada a melhor alternativa dentre as opções elencadas. Esta solução trata do licenciamento do software por meio de recursos orçamentários de investimentos com suporte e garantia.

### 11.2. Do Modelo de Licenciamento

1.

11.2.1 O mercado de soluções tecnológicas baseadas em software possui dois modelos de comercialização, o primeiro modelo licencia softwares perpétuos, pagos integralmente após o recebimento, que podem ser utilizados indefinidamente, mas que não contam com atualizações periódicas e suporte após a vigência do contrato.

11.2.2. No segundo modelo, de licença de uso, paga-se pelo direito de uso dos softwares pelo período contratado, e conta-se com atualizações periódicas, suporte técnico e garantia durante esse período.

11.2.3 É do interesse dessa administração contratar a solução tecnológica no segundo modelo de licenciamento, qual seja o modelo de licença de uso, pois tal opção é justificável economicamente, na medida em que a licença já contempla os upgrades e atualizações necessárias ao longo de todo o contrato e que, ao considerarmos o avanço dos métodos de

ataques cibernéticos e soluções tecnológicas, o modelo de subscrição garante a contratante uma constante atualização.

11.2.4. Dessa forma, concluímos que a contratação de licenças na modalidade “Licença de uso” possibilita maior gestão do uso de softwares licenciados, permitindo a adequação do quantitativo de licenças ao longo da execução contratual, permitindo anualmente a redução de licenças não necessárias, ou ainda, permitindo ainda a expansão dos quantitativos contratados.

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

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

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

- I - composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços em saúde, observado o índice de atualização de preços correspondente;*
  - II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;*
  - III - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;*
  - IV - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou UASG 420001 Estudo Técnico Preliminar 3/2023;*
  - V - pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.*
- § 1º Deverão ser priorizados os parâmetros estabelecidos nos incisos I e II, devendo, em caso de impossibilidade, apresentar justificativa nos autos."*

11.3.2 Conforme orienta a referida Instrução Normativa e devidamente exposto no item 9.4.1.2 anterior, foi realizada pesquisa no Painel de Preços (disponível em <https://paineldepregos.planejamento.gov.br/>) no período de 01/07/2024 a 19/07/2024 e verificou-se que 05 órgãos/entidades adquiriram bem similar ao objeto deste estudo, conforme segue:

1.

ÓRGÃO	UASG	PREGÃO
-------	------	--------

Agência Nacional de Aviação Civil - ANAC	113214	29/2019
Agência Nacional de Águas e Saneamento Básico - ANA	443001	24/2020
Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES	154003	Contrato 46/2022
Tribunal Superior do Trabalho	80001	58/2021
Fundação Nacional de Saúde - FUNASA	2550	11/2022

#### 11.4. Análise dos Pregões encontrados

11.4.1. O **Pregão 28/2019/ANAC**, teve por objeto a *“Aquisição de licenças perpétuas de software para solução de auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (Microsoft Active Directory), correio eletrônico (Microsoft Exchange Server) e servidores de arquivos (Microsoft File Server)”*.

1.

A contratação incluiu licenciamento, instalação, treinamento, garantia e suporte técnico para a solução.

2.

A análise do pregão referenciado teve a comparação prejudicada uma vez que o projeto contemplou aquisição de licenças na modalidade "perpétua", modalidade esta considerada inadequada conforme item 11.2 deste Estudo Técnico .

3.

Além disso, o lapso temporal decorrido desde a licitação, pouco mais de 4 (quatro) anos, também prejudica a utilização desta referência, consoante inciso II do art. 5º da Instrução Normativa nº 65, de 07 de Julho de 2021.

11.4.2. O **Pregão 24/2020/ANA** teve por objeto a *“fornecimento e implantação de solução de tecnologia da informação e comunicação de auditoria e governança para controle e gerência de permissionamento dos serviços de AD (Microsoft Active Directory), servidor de arquivos (Windows File Server), mensageria eletrônica (Microsoft Exchange Server), identificação e classificação de informações sensíveis, e análise em tempo real e prevenção de comportamentos suspeitos, contemplando a execução de serviços de instalação, apoio técnico especializado pós-implantação e transferência de conhecimentos, com garantia (manutenção e suporte técnico) pelo período de 12 (doze) meses”*.

1.

Este pregão, embora tenha tido seu escopo mais próximo do pretendido pelo MinC, também não pode ser considerado na análise dado o lapso temporal decorrido desde a licitação, pouco mais de 3 (três) anos, também prejudica a utilização desta referência, consoante inciso II do art. 5º da Instrução Normativa nº 65, de 07 de Julho de 2021.

11.4.3. O **Contrato 045/2022/CAPES** teve por objeto é "Aquisição de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento."

1.

Este contrato, embora também tenha tido seu escopo mais próximo do pretendido pelo MinC, também não pode ser considerado na análise dado o lapso temporal decorrido desde a licitação, pouco mais de 3 (três) anos, também prejudica a utilização desta referência, consoante inciso II do art. 5º da Instrução Normativa nº 65, de 07 de Julho de 2021.

11.4.4. O **Pregão nº 58/2021/TST** teve por objeto é o "Registro de preços para aquisição de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento".

1.

Este Pregão, embora também tenha tido seu escopo mais próximo do pretendido pelo MinC e também similar ao contrato CAPES anteriormente analisado, também não pode ser considerado na análise dado o lapso temporal decorrido desde a licitação, pouco mais de 2 (dois) anos, também prejudica a utilização desta referência, consoante inciso II do art. 5º da Instrução Normativa nº 65, de 07 de Julho de 2021.

11.4.5. O **Pregão nº 11/2022/FUNASA** teve por objeto é o "Registro de preços para aquisição de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento".

1.

Este Pregão, embora também tenha tido seu escopo mais próximo do pretendido pelo MinC e também similar aos contratos CAPES e TST anteriormente analisados, também não pode ser considerado na análise dado o lapso temporal decorrido desde a licitação, pouco mais de 1 (um) ano e meio, também prejudica a utilização desta referência, consoante inciso II do art. 5º da Instrução Normativa nº 65, de 07 de Julho de 2021.

11.4.6. Desta forma, a fim de complementar e ampliar a pesquisa supracitada e se chegar ao valor estimado da contratação, o mais próximo possível da realidade de mercado, foi também realizada pesquisa de preços com fornecedores do ramo, conforme segue:

11.4.6.1 - Considerando cenário de subscrição para 12 meses

Item	Descrição	Unidade	Qtde	ARVVO	PETACORP	OMTX	NTSEC	PLANCK	GUARDTI	MÉDIA
				Valor Unitário Anual	Valor Unitário Anual	Valor Unitário Anual	Valor Unitário Anual	Valor Unitário Anual	Valor Unitário Anual	Valor Unitário Anual Médio
	Solução tecnológica									



1	para atendimento das exigências da política de segurança da informação, compliance e governança de dados não estruturados, pelo período de 36 meses.	Un	1.500	3.781,00	3.309,98	3.120,00	3.981,00	3.580,77	5.553,60	3.887,73
2	Serviços de Instalação e Configuração da solução.	Un	01	108.000,00	58.030,00	72.800,00	108.000,00	138.800,00	119.392,00	100.837,00
3	Serviço de Treinamento.	Turma	01	94.440,00	42.270,00	42.200,00	94.440,00	98.250,00	69.208,00	73.468,00
<b>VALOR TOTAL ANUAL</b>										<b>6.005.892,50</b>

## 11.4.6.2. Considerando cenário de subscrição por 36 meses

Item	Descrição	Unidade	Qtde	ARVVO	PETACORP	OMTX	NTSEC	PLANCK	GUARDTI	MÉDIA
				Valor Unitário Anual	Valor Unitário Anual	Valor Unitário Anual	Valor Unitário Anual	Valor Unitário Anual	Valor Unitário Anual	Valor Unitário Anual Médio
1	Solução tecnológica para atendimento das exigências da política de segurança da informação, compliance e governança de dados não estruturados, pelo período de 36 meses.	Un	1.500	7.210,00	6.984,41	6.778,00	7.182,00	10.742,31	12.064,84	8.493,59
2	Serviços de Instalação e Configuração da solução.	Un	01	108.000,00	58.030,00	72.800,00	108.000,00	138.800,00	119.392,00	100.837,00

3	Serviço de Treinamento.	Turma	01	94.440,00	42.270,00	42.200,00	94.440,00	98.250,00	69.208,00	73.468,00
VALOR TOTAL para 36 MESES										12.914,695,00

11.4.7. Dados os valores pesquisados (médias aritméticas), conclui-se que, economicamente, a contratação por 36 meses se mostra mais vantajosa.

11.4.7.1. Ainda que, por exercício, considerássemos apenas as propostas de menor valor, ainda assim conclui-se que a contratação por 36 meses se mostra mais vantajosa.

11.4.8. Além das questões econômicas, a contratação com prazo de 36 meses também se justifica tecnicamente, considerando os seguintes aspectos:

1.

**Risco de mudanças tecnológicas:** Na vigência de curto prazo, a exemplo de 12 meses, tem-se o risco de ser insuficiente dada a complexidade de soluções desta natureza, a necessidade de absorção da solução pelo corpo técnico, planejamento de sua implantação e uso de forma adequada em cada departamento ou demanda.

2.

**Flexibilidade para a entidade contratante:** permite que ela se adapte às mudanças tecnológicas e às necessidades em constante evolução da organização, possibilitando revisar e atualizar as soluções.

3.

**Economicidade:** em relação a economicidade é cediço que não há necessidade de pesquisa de mercado específica para concluir que contratações de maior período tendem a ter seus custos diluídos se comparados às contratações de menor período, representando valores das licenças mais reduzidos, haja vista que o fornecedor também possui vantagem econômica no ganho de escala em relação ao período de maior vigência, ou seja, contratações de softwares no formato de licenças de uso por períodos mais longos, representarão valores de licenciamento mais baixos quando comparados a períodos menores.

4.

**Atualização e manutenção evolutiva:** um contrato de 36 meses no modelo de licenciamento de uso, garante que o fornecedor irá atualizar a solução em relação a novas ameaças que surjam ao longo do período contratado.

11.4.9. Diante do exposto, visando mitigar riscos no alcance dos resultados pretendidos em um cenário de vigência curta e buscando menor dependência do fornecedor e tecnologia naturais de vigências mais longas, acima de 36 meses, definiu-se que a vigência de 36 meses é a mais adequada.

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

12.1. Fornecimento e implantação de Solução de segurança da informação para auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (Microsoft Active Directory), correio eletrônico (Microsoft Exchange Server) e servidores de arquivos, pelo período de 36 meses, conforme detalhamento técnico constante no Apêndice I deste Estudo Técnico.

## 13. Estimativa de custo total da contratação

Valor (R\$): 12.914.695,00

Item	Descrição	Unidade	Qtde.	Valor Unitário	Valor Total
1	Solução tecnológica para atendimento das exigências da política de segurança da informação, compliance e governança de dados não estruturados, pelo período de 36 meses.	Un	1.500	R\$ 8.493,59	R\$ 12.740.390,00
2	Serviços de Instalação e Configuração da solução.	Un	01	R\$ 100.837,00	R\$ 100.837,00
3	Serviço de Treinamento.	Turma	01	R\$ 73.468,00	R\$ 73.468,00
VALOR TOTAL					R\$ 12.914.695,00

## 14. Justificativa técnica da escolha da solução

14.1. Após o levantamento de mercado realizado, conclui-se pela escolha da **Solução 1** com a contratação de empresa para fornecimento da solução, em razão da justificativa já apresentada e pela contratação de empresa capaz de fornecer integralidade do presente projeto e seus serviços correlatos.

14.2. A escolha pela contratação de empresa especializada no fornecimento das soluções indicadas, levou em consideração:

1.

Melhor eficiência em relação a utilização de corpo técnico, podendo direcionar os recursos humanos para gestão do processo e desenvolvimento de novos projetos;

2.

Custo reduzido de capacitação e energia em relação a contratação de profissionais com background específico para desenvolvimento;

3.

Celeridade na implementação do projeto e alcance dos benefícios esperados;

4.

Curva de experiência e maturação da equipe de curto prazo;

5.

Garantia de upgrades e atualizações em função das mudanças da tecnologia e aplicações;

6.

Mitigação de riscos associados a indisponibilidade de servidores externos.

7.

Possibilidade de gerenciamento centralizado e integrado;

8.

Solução unificada e integrada em suas funcionalidades, contribuindo para reduzir o risco institucional e eventuais vazamentos de dados;

9.

Maior eficiência na gestão do contrato;

10.

Menor investimento em integrações entre diversas aplicações.

## 15. Justificativa econômica da escolha da solução

15.1. Conforme demonstrado no item 11 - Análise comparativa de custos (TCO), após a realização da pesquisa de mercado, apurou-se a média dos preços obtidos junto à empresas de mercado, e verificou-se que o valor médio está em conformidade com os preços praticados no mercado.

## 16. Parcelamento - Aspectos Técnicos

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

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

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

*(...)*

*V - atendimento aos princípios:*

(...)

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

1.

1.1.

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

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

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

1.

1.1.

16.5. Deste modo, para a pretendida aquisição se faz necessário a contratação de **solução única de TIC**, que reunirá todos os serviços necessários ao atendimento das necessidades do MinC.

16.6. Importante justificar que a contratação considera o licenciamento de uma solução **única** baseada em software e seus serviços de instalação e configuração e treinamento, não cabendo a divisão dos itens em lotes distintos, uma vez que a empresa a ser contratada para licenciamento deverá ser responsável pelos serviços de forma integrada.

16.7. Deste modo, conclui-se que o parcelamento do objeto não é tecnicamente viável, uma vez que não se pode licitar os serviços que são associados ao software de forma apartada, a serem executados por outra empresa, que não que fornecerá os softwares.

16.8. Tal definição não afetará a competitividade do certame, pois empresas que atuam neste setor já operam com camadas de serviço além do fornecimento das licenças.

## 17. Parcelamento - Aspectos Econômicos

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

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

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

## **18. Justificativa Registro de Preços**

18.1. A presente contratação se baseia no licenciamento pelo número de usuários ativos, o que pode variar no tempo, a depender das chegadas e saídas de colaboradores em decorrência da situação de Ministério "recém-criado" vivenciada pelo MinC.

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

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

*(...)*

*V - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.*

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

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

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

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

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

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

19.1. Por meio da contratação de uma solução de tecnologia que permitirá o atendimento das exigências da política de segurança da informação, compliance e governança de dados não

estruturados, elevando o nível de proteção das informações no ambiente tecnológico do Ministério da Cultura (MinC), de forma a atender ao que cabe a LGPD no tocante a dados não estruturados, espera-se:

1.

eleva a eficácia na gestão de riscos e governança de dados;

2. alinhamento estratégico aos objetivos elencados no PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO - PDTIC

3. solidificar a imagem institucional do Ministério da Cultura, mitigando riscos associados a Governança e Gestão de TI;

4. adequações atreladas ao atendimento às diretrizes e dispositivos legais trazidos pela Lei Geral de Proteção de Dados (LGPD) e demais padrões de segurança recomendados para órgãos da administração pública;

5. melhoraria no relacionamento com os agentes internos e externos através da confiabilidade e respeito à privacidade;

6. avanços voltados para auditoria e governança do uso das informações e dados pessoais;

7. preservar a integridade, confidencialidade e disponibilidade das informações custodiadas por essa administração;

8. permitir e viabilizar uma maior autonomia da área de segurança da informação em relação ao gerenciamento dos acessos aos sistemas e aplicações;

9. buscar uma melhoria de performance e disponibilidade das aplicações;

10. melhoria na infraestrutura e no controle da segurança da informação;

11. identificação de permissões excessivas ou antigas;

12. remediação de forma automática de dados expostos;

13. automatização do processo de limpeza de credenciais e permissões antigas, minimizando a exposição de dados

14. integração com as soluções de DLP na classificação da informação, marcando os arquivos como sensíveis, abertos ou sigilosos possibilitando ao DLP o bloqueio de envio destes arquivos;

15. responsabilização dos responsáveis por vazamentos dos dados através da auditoria por longos períodos;

16. capacidade de prever acessos que, embora permitidos, podem apresentar riscos;

17. validação e aprimoramento a criação de políticas para o DLP;

18. consolidar as defesas contra a exposição de dados;

19. análise do comportamento do usuário em relação aos dados, permitindo a detecção de atividades suspeitas baseadas em desvios dos padrões normais;

20. automatização e remediação dos privilégios de acesso, garantindo que apenas as pessoas certas tenham acesso aos dados;

21. garantir o acesso a ferramentas para rastreamento contínuo e revisão de permissões, garantindo que a organização permaneça em conformidade com regulamentações em constante mudança.

22. aumento da proteção dos dados contra alterações, exclusões e atividades não autorizadas, com consequente diminuição do tempo de resposta as falhas, paralizações e desastres;

23. visão completa da estrutura *on-prem* do AD, com possível administração de seu repositório de usuários e grupos de segurança através de uma interface única, juntamente com a gestão de seus servidores de arquivos;

24. auditoria eficiente do Active Directory, File Server Exchange, que por meio do registro de eventos (logs) de auditoria possibilitando a visibilidade de todas as ocorrências

25. possibilidade de identificação de arquivos sensíveis distribuídos nos repositórios de dados e monitoração do seu uso e dos logs de todas as plataformas monitoradas em uma única console, com alertas de modificação, quando alguma ação for disparada;

26. melhoria no nível de segurança e integridade dos dados e informações manipulados e armazenados no ambiente do MinC.

## 20. Providências a serem Adotadas

20.1. Não há providências a serem adotadas, uma vez que se trata de uma licença de uso a ser instalada no parque computacional, sem requerer recursos físicos, seja humanos ou materiais, além dos que essa administração já dispõe para instalação da solução.

## 21. Declaração de Viabilidade

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

### 21.1. Justificativa da Viabilidade

Por todo o exposto ao longo deste Estudo Técnico, esta Equipe de Planejamento da Contratação, declara viável a contrataç

## 22. 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 02/08/2024 às 10:09:11.

**GUSTAVO RIBEIRO DA ROCHA**

Integrante Administrativo



Assinou eletronicamente em 02/08/2024 às 10:12:20.

**RAMON LEONN VICTOR MEDEIROS**

Integrante Técnico





*Assinou eletronicamente em 02/08/2024 às 10:16:52.*

## Lista de Anexos

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

- Anexo I - Caderno de Especificação Técnica.pdf (326.01 KB)

## **Anexo I - Caderno de Especificação Técnica.pdf**

## **ESPECIFICAÇÃO TÉCNICA MÍNIMA DA SOLUÇÃO**

**1. LOTE 01 (ÚNICO) - ITEM 1 – Solução tecnológica para atendimento das exigências da política de segurança da informação, compliance e governança de dados não estruturados, pelo período de 36 meses.**

- 1.1. Solução de tecnologia que permitirá o atendimento das exigências da política de segurança da informação, compliance e governança de dados não estruturados, elevando o nível de proteção das informações no ambiente tecnológico do Ministério da Cultura (MinC), de forma a atender ao que cabe a LGPD no tocante a dados não estruturados.
- 1.2. Permitir a detecção de comportamentos suspeitos em diretórios de usuários e servidores de arquivos. Além disso, a solução poderá ser migrada para a nuvem, modelo SAS, conforme necessidade futura ou preferência do contratante, desde que observadas as regulamentações legais referentes à localização dos dados e à privacidade das informações.
- 1.3. A solução tecnológica proposta será licenciada pelo período de 36 meses, para garantir a governança e conformidade dos ambientes de dados não estruturados presentes nos servidores AD, NAS, Windows da organização e aplicações web. Adicionalmente, será possível modificar o licenciamento durante o período contratual para se adequar a plataformas em nuvem, plataforma SAS, conforme as especificações detalhadas no termo de referência.
- 1.4. Requisitos Mínimos Gerais**
- 1.5. A solução de proteção de credenciais deverá ser capaz de analisar em tempo real e prevenir comportamentos suspeitos em aplicações web, mesmo que estas não estejam integradas ao Active Directory;
- 1.6. Comunicar-se através de API HTTP REST ou UDP com a aplicação web protegida, calculando e fornecendo em tempo real um score de risco e o nível de risco que este score representa, para cada evento de autenticação que ocorre em uma dada aplicação;

- 1.7. Assegurar a comunicação entre a solução de proteção de credenciais e a aplicação web protegida através de criptografia de chaves simétricas;
- 1.8. Possibilitar a criação e configuração de políticas de risco, possuindo no mínimo 4 níveis de risco parametrizáveis a serem definidos em cada política;
- 1.9. Fornecer para cada autenticação analisada o score de risco processado acompanhado da ação (permitir, notificar, desafiar ou bloquear) indicada para o nível de risco do evento em questão, de acordo com a política definida;
- 1.10. Possibilitar o agrupamento de credencias, de modo que uma credencial possa estar associada a mais de uma aplicação web protegida;
- 1.11. Não exigir tokens, dispositivos móveis, códigos ou outras informações adicionais para o processamento de eventos;
- 1.12. Ser capaz de processar e fornecer o score de risco tanto para autenticações com a credencial e senha corretos como para autenticações com credencial e/ou senha incorretos;
- 1.13. Possuir uma base de inteligência de segurança para ser utilizada na mensuração do risco dos acessos, construída com informações próprias e públicas (OSINT), de modo a identificar IPs de má reputação e/ou utilizados para serviço de proxy;
- 1.14. Realizar a mensuração de risco no processo de autenticação sem armazenar e sem ter acesso a senha da credencial em questão, em nenhuma hipótese.
- 1.15. Construir padrão de comportamento de uma credencial com base no histórico de seu uso, composto minimamente por navegador, dispositivo, localização geográfica (cidade e país), sistema operacional, identificador do provedor de internet;
- 1.16. Identificar desvios no padrão de comportamento de uma credencial, possibilitando o envio de notificações, apresentação de desafios (token, captcha ou similares) e bloqueio de acesso, a depender da política de risco definida;
- 1.17. Realizar a mensuração de risco de todos os acessos levando em consideração o padrão de comportamento da credencial e a base de inteligência de segurança;

- 1.18. Todos os eventos processados e armazenados pela solução deverão ser georreferenciados de acordo com o endereço IP de origem, contendo minimamente país, cidade, latitude e longitude;
- 1.19. Permitir a notificação de usuários com base em política de risco, através do disparo via SMTP de e-mail, possibilitando a redação de mensagem personalizada em editor HTML, contendo detalhes do evento em questão como cidade de acesso, data e hora, ip de origem, navegador e um link para que o usuário responda se reconhece o acesso ou não;
- 1.20. Inserir no padrão de comportamento da credencial novas informações quando o usuário confirma através da notificação recebida a veracidade do acesso;
- 1.21. Possibilitar o envio de e-mail para administrador quando um usuário nega a veracidade de um acesso através da notificação recebida;
- 1.22. Ser capaz de bloquear o processo de autenticação de usuários com base no score de risco do evento, mesmo quando a credencial e a senha forem corretamente imputadas no ato da autenticação;
- 1.23. Identificar ataques do tipo “força bruta”, elevando de forma automática e proporcional o score de risco do IP de origem do acesso com base no número de tentativas de autenticações fracassadas em um curto intervalo de tempo;
- 1.24. A reputação das origens detectadas como geradores de ataques de força bruta deverá decair após determinado tempo, e o tempo de decaimento da reputação deverá aumentar em função da recorrência de tentativas de ataques de força bruta;
- 1.25. Enviar eventos, cifrados nativamente com chave simétrica, via webhook para URL a ser configurada em interface gráfica, com base na política de risco definida;
- 1.26. Elevar o score de risco de uma credencial ao detectar mudança geográfica de longa distância;

- 1.27. Identificar os top 10 usuários que representam maior atividade de risco acumulado em um intervalo de tempo escolhido, informando o nome do usuário (credencial) e score de risco acumulado;
- 1.28. Segmentar os eventos processados por credencial, possibilitando navegar por todos os eventos de uma dada credencial, informando no mínimo os seguintes detalhes de cada evento: Cidade, coordenadas geográficas, nome do navegador utilizado, nome do dispositivo utilizado no acesso, endereço ip de origem, score de risco e resultado da ação com base na política definida, código identificador do ISP (internet service provider) e descritivo com análise do evento;
- 1.29. Possuir gráfico que represente os eventos de uma credencial específica em um intervalo de tempo escolhido, distinguindo-os pelos níveis de risco definidos em política;
- 1.30. Possuir dashboard para visualização de eventos no formato de representação de mapa geográfico que possibilite distinguir diferentes níveis de risco, detalhando informações como cidade, usuário, score de risco do evento, data e hora do evento;
- 1.31. Possuir dashboard para visualização do risco organizacional em um intervalo de tempo escolhido, segmentado por aplicação protegida ou não, distinguindo o volume de eventos que representam o risco mitigado, o risco em mitigação (pendente) e o risco assumido;
- 1.32. Possuir dashboard para identificação e análise de ataques, contendo minimamente as seguintes estatísticas:
  - 1.32.1. Endereços IPs com maior incidência de credenciais únicas autenticadas com sucesso e com falha na autenticação;
  - 1.32.2. Credenciais com maior incidência de acessos originados em cidades distintas autenticados com sucesso e com falha na autenticação;
  - 1.32.3. Credenciais com maior incidência de eventos de autenticação com sucesso e com falha na autenticação;



- 1.32.4. Endereços IPs com maior número de eventos de autenticação com sucesso e com falha na autenticação;
- 1.32.5. Cidades com maior número de eventos;
- 1.32.6. Países com maior número de eventos;
- 1.32.7. Gráfico com quantidade de eventos classificados por resposta da política de risco em razão do tempo;
- 1.32.8. Possuir integração com soluções do tipo “single-sign-on”, disponibilizando no mínimo, de forma nativa, o RH-SSO e Keycloak;
- 1.32.9. Possuir integração nativa com a autenticação de tecnologias de mercado, sendo minimamente wordpress, openssh, cloudflare, moodle e keycloak;
- 1.32.10. Ser capaz de processar eventos originados em IPv4 e IPv6;
- 1.32.11. Possuir identificador único para todos os eventos processados pela solução;
- 1.32.12. Possuir mecanismo de processamento e armazenamento de eventos baseado em tecnologias escaláveis;
- 1.32.13. Possuir mecanismo de dissuasão de ataques de força-bruta baseado em desafio criptográfico a ser decifrado pelo navegador cliente, sem necessidade de interação dos usuários da aplicação protegida;
- 1.33. O nível de dificuldade do desafio criptográfico deverá ser parametrizável;
- 1.34. Deverá ser fornecido um painel para visualização e análise de eventos, inspeção e segurança de credenciais/usuários;
- 1.35. O painel deverá possuir um mecanismo nativo para gestão de usuários que podem acessá-lo, incluindo integração nativa com os seguintes sistemas de diretório de usuários: Active Directory, LDAP e Keycloak/RH-SSO;
- 1.36. O painel deverá ser desenvolvido em tecnologia web based, acessível através de protocolo https;

- 1.37. O painel deverá criptografar toda a comunicação com as fontes geradoras de eventos, e ao armazenar eventos em base de dados, anonimizar o campo que contém a informação de nome de usuário, seja este um CPF, matrícula, e-mail ou uma string (ex: nome.sobrenome);
- 1.38. As informações disponibilizadas no painel de visualização deverão ser orientadas a intervalo de datas, e fornecer estatísticas dos eventos de segurança que são protegidas pela solução, sendo minimamente: Usuários que mais geram eventos de segurança no ambiente protegido; Endereços IPs que mais geram eventos de segurança no ambiente protegido; Incidentes de segurança mais frequentes;
- 1.39. O painel deverá permitir visualizar detalhes de cada evento de segurança coletado;
- 1.40. Permitir filtrar eventos por usuário (credencial);
- 1.41. Permitir filtrar eventos por endereço IP de origem;
- 1.42. Todos os softwares fornecidos deverão ser licenciados pelo período mínimo de 36 (trinta e seis) meses, e contemplar garantia, suporte e atualização dos respectivos fabricantes. A solução deverá ser dimensionada para o volume de usuários indicados no quadro de itens do presente termo de referência, devendo ser considerado o período contratual de 36 (trinta e seis) meses para a licença de uso que integra a solução;
- 1.43. O fabricante ou a solução ofertada de governança de dados, deverá possuir certificação de compliance como ISO 27001 ou similar, garantindo que seus produtos atendam aos rígidos padrões da indústria e sejam auditados e revisados regularmente;
- 1.44. Por se tratar de solução entregue como serviço na nuvem, modelo SAS, o fabricante deve adotar abordagem baseada em risco para seu sistema de gestão de segurança da informação (SGSI), a implantação de um SGSI, reduz o risco de divulgação, modificação ou destruição não autorizada, acidental ou intencional das informações, além de constantemente, realizar testes de penetração de terceiros no

tenant e varredura automatizada para garantir a segurança do software; Por se tratar de software de proteção de dados sensíveis com análise comportamental de usuários para ambientes computacionais o fabricante ou a solução de governança de dados deverá ser certificada ISO/IEC 27017;

- 1.45. A solução deve suportar a utilização de servidores virtualizados para os componentes;
- 1.46. A solução deve possibilitar a configuração de credencial diferente para cada servidor/serviço a ser monitorado;
- 1.47. Por se tratar de software de proteção de dados sensíveis o fabricante ou a solução de governança de dados deverá ser certificada ISO/IEC 27701 que trata do gerenciamento de privacidade da informação dentro da organização;
- 1.48. A solução deverá monitorar múltiplos domínios e servidores de arquivos Windows e NAS (Network Attached Storage) do ambiente, incluindo: Contas, estruturas de diretórios, permissões e eventos;
- 1.49. A solução a ser fornecida deverá possuir compatibilidade comprovada no site dos fabricantes dos storage Netapp e EMC para que tenha compatibilidade com a Infraestrutura do órgão;
- 1.50. Caso a solução necessite da instalação de agente para o monitoramento dos eventos do Active Directory e servidores de arquivos, os agentes não devem gerar nenhuma queda de performance nos servidores;
- 1.51. O gerenciamento da solução deverá ser centralizado para todos os módulos;
- 1.52. A solução deverá monitorar todos os domain controllers instalados em qualquer versão do Windows Server 2003 até 2022;
- 1.53. A solução deverá monitorar todos os servidores de arquivos instalados em Windows Server 2012 até Windows Server 2022;
- 1.54. A solução deverá monitorar no mínimo, os seguintes eventos do Microsoft Active Directory: Conta habilitada e desabilitada; Autenticação de conta (TGT); Renovação

de acesso (TGS); Replicação de AD; Logon de conta no DC; Criação, deleção, renomeação, modificação, remoção e adição de membros no objeto do DS; Requisição de acesso NTLM; Alteração de senha de usuário; Conta de usuário bloqueada; Conta de usuário desbloqueada; Netlogon vulnerável; Criação, deleção e modificação de GPO; Tentativa de reset de senha; Criação, atualização, deleção, habilitação e desabilitação de tarefa agendada dentro do DC; Alteração de política de kerberos;

- 1.55. A solução deverá monitorar no mínimo, os seguintes eventos do servidor de Arquivos Windows: Arquivo criado; Arquivo deletado; Arquivo aberto; Arquivo renomeado; Arquivo modificado; Mudança de proprietário do arquivo; Permissões adicionadas no arquivo; Permissões removidas no arquivo; Proteção adicionado no arquivo; Proteção removida no arquivo; Pasta criada; Pasta deletada; Pasta renomeada; Mudança de proprietário da pasta; Permissões adicionadas na pasta; Permissões removidas na pasta; Proteção adicionada na pasta; Proteção removida na pasta;
- 1.56. Deverá ser possível definir os proprietários das pastas através da console;
- 1.57. A solução deverá exibir uma lista com todas as contas de usuários monitoradas, indicando no mínimo, o tipo de conta (serviço, executiva ou administrativa) e grupos que fazem parte;
- 1.58. A solução deverá exibir o repositório monitorado em formato hierárquico, expandindo as pastas e sub-pastas até o nível do arquivo, permitindo a visualização de quais usuários tem acesso a cada recurso e as permissões concedidas;
- 1.59. A solução deverá possuir uma visão bi-direcional indicando através de uma visualização gráfica e interativa, todas as permissões dos usuários e grupos, e quais as permissões aplicadas nos objetos (arquivos e pastas);
- 1.60. A solução deverá disponibilizar a visibilidade de permissões, sejam elas NTFS ou share;

- 1.61. A solução deverá realizar a classificação do conteúdo do arquivo, fornecendo visibilidade sobre onde residem os dados confidenciais e sensíveis no sistema de arquivos;
- 1.62. A solução deverá utilizar múltiplos fatores para realizar a classificação do conteúdo do arquivo, incluindo: Metadados, padrões, dicionários, palavras-chave e expressão regular;
- 1.63. A solução deverá indicar para qualquer arquivo e pasta no servidor monitorado, uma visualização gráfica contendo o nível de exposição e indicando se o arquivo é sensível ou não a partir da classificação realizada;
- 1.64. A solução deverá fornecer filtros para visualizar apenas determinados objetos de dados em exibição gráfica interativa, incluindo pastas protegidas e pastas únicas;
- 1.65. A solução deverá incluir informações de classificação de dados na tela das permissões, incluindo: nome da regra classificada, e quantidade de instâncias sensíveis encontradas no arquivo;
- 1.66. A solução deverá fornecer para as permissões, tipos de exibição diferentes, incluindo exibições hierárquicas e de lista;
- 1.67. A solução deverá realizar a classificação de imagens através de OCR ou tecnologia similar;
- 1.68. A solução deverá possibilitar a criação de regras customizadas para que os administradores possam definir o que deve ser encontrado dentro do conteúdo do arquivo, de acordo com a necessidade organizacional;
- 1.69. Deve ser possível realizar o agendamento do escaneamento das regras de classificação, podendo especificar: horário, dia e tempo de duração;
- 1.70. Deve ser possível exportar eventos e informações apenas referente aos dados classificados como sensíveis;

- 1.71. Deve ser possível definir o escopo do ambiente que vai ser classificado, podendo definir: repositório, arquivo, pasta, tipo de arquivo, quantidade mínima de hits e outros;
- 1.72. A solução deverá auxiliar na conformidade com a LGPD, identificando aonde os dados pessoais (CPF, RG, CNH e outros) são armazenados, quem tem acesso aos dados e quais são as atividades em cima destes dados;
- 1.73. A solução deverá escanear e classificar no mínimo os seguintes tipos de arquivos: doc, docx, dwg, rtf, ppt, xls, txt, csv, pdf, xml, log, eml, jpg, jpeg, gif, png, rar e zip;
- 1.74. A solução deverá encontrar em arquivos com formato tabular, palavras chaves em cabeçalhos e colunas;
- 1.75. Deve ser possível limitar escopo dentro dos sistemas de arquivos a ser analisado;
- 1.76. Deve ser possível definir partes específicas do arquivo a serem analisadas no escopo como: Colunas específicas de arquivos do tipo Microsoft Excel, cabeçalho, rodapé e marca d'água de arquivos Microsoft Office, links de arquivos Microsoft Office e PDF;
- 1.77. A solução deverá indicar no painel de diretórios: o nome da regra, a quantidade de hits do termo sensível encontrado nos arquivos e pastas e a quantidade de hits incluindo sub-pastas;
- 1.78. A solução deverá ser entregue utilizando a infraestrutura em nuvem disponibilizada pelo fabricante, e poderá ser ofertada e instalada localmente desde que não retenha os logs nativos e não seja baseada em software livre.
- 1.79. A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar acesso a dados que o usuário não costuma acessar;

- 1.80. Nos alertas em tempo real, deve ser possível configurar para que, um usuário, uma pasta, um período ou uma ação específica seja alertada, caso ocorra ação que os envolva;
- 1.81. A solução deverá notificar os administradores através de alertas para qualquer tipo de atividade incomum e comportamentos suspeitos de usuários;
- 1.82. Os alertas da solução deverão ser encaminhados via SMTP e SNMP;
- 1.83. A solução deverá suportar a configuração de respostas automáticas para os alertas gerados, possibilitando a execução automática de scripts ou comandos pré-configurados;
- 1.84. A solução deverá realizar a análise comportamental dos usuários de forma automática, através de machine learning, entendendo o comportamento e rotina de todos os usuários, o que acessam, quando acessam e onde;
- 1.85. A solução deverá contemplar a assinatura de uma base de conhecimentos do fornecedor com mais de 150 modelos de alertas pré-configurados de eventos suspeitos tais como: Ataques de sequestro de dados (ransomware); Detecção de ferramentas nocivas ao ambiente; Ações com acessos negados; Ações de escalasões de privilégios; Excesso de tentativas de autenticação ou contas bloqueadas; Atividades suspeitas em dados parados e/ou inativos; Alterações anormais em GPO; Ataques de golden ticket; Ataques de injeção de códigos maliciosos; Ataques de descoberta de contas com NTLM e Kerberos; Ataques de força bruta;
- 1.86. Os modelos de alertas devem ser atualizados de forma automática;
- 1.87. A solução deverá detectar ameaças em todos os estágios de um ataque cibernético, incluindo dashboard que indica algumas categorias como: Reconhecimento, intrusão, exploração, escalação de privilégio, movimento lateral, negação de serviço e exfiltração de dados;
- 1.88. A solução deverá monitorar a atividade do usuário para construir perfis de comportamento e usar os modelos de ameaça baseados em comportamento para alertar quando uma atividade anormal no Active Directory é detectada;

- 1.89. A solução deverá construir perfis de comportamento comparando as atividades dos usuários e entidades e identificando a relação entre eles;
- 1.90. A solução deverá possuir um período de aprendizado, para que seja feito a coleta de eventos e identificação do comportamento dos usuários para a criação do perfil comportamental;
- 1.91. A solução deverá realizar a descoberta de contas privilegiadas de forma automática, identificando contas executivas, contas de serviço e contas administrativas baseado no seu comportamento e nos grupos de segurança que a conta está inserida;
- 1.92. A solução deverá exibir uma lista com todas as contas de usuários monitoradas, indicando no mínimo, o tipo de conta (serviço, executiva ou administrativa) e grupos que fazem parte;
- 1.93. A solução deverá possuir dashboard de alertas indicando os usuários mais alertados, dispositivos e modelos de alertas gerados;
- 1.94. A solução deverá possuir política de automação para remediação de exposição de dados para toda a organização, removendo as permissões globais das pastas e arquivos;
- 1.95. A solução deverá possuir política de automação para remediar permissões inconsistentes, garantindo que não exista permissão quebrada e aplicando as entradas de permissão corretamente para as sub-pastas e arquivos;
- 1.96. As políticas de automação para remediação devem ser executadas de forma manual e automática;
- 1.97. A solução deverá possuir política de automação para remediar permissões inconsistentes, garantindo que não exista permissão quebrada e aplicando as entradas de permissão corretamente para as sub-pastas e arquivos;



- 1.98. Para análise forense do usuário mais alertado, o dashboard deve possuir página que agregue dados importantes do comportamento daquele usuário. Isso permite que se identifique o cenário do possível ataque;
- 1.99. No dashboard, a partir de um alerta selecionado, a solução deve exibir página que liste todos os eventos ocorridos que motivaram a ferramenta a gerar o alerta. A lista desses eventos deve ser customizável podendo ser filtrada, exibidas ou ocultas colunas e agregada por valores das colunas exibidas;
- 1.100. A solução deverá suportar na busca dos eventos a utilização de operadores relativos, auxiliando na investigação e nos resultados esperados;
- 1.101. Deve ser possível salvar uma pesquisa customizada, agendando para que ela possa ser executada de forma automática e que os administradores recebam as informações necessárias de forma periódica;
- 1.102. A solução deverá suportar a criação e utilização de flags para serem aplicadas as contas de usuários e aos recursos monitorados, essas flags podem ser utilizadas nos filtros e na aba de eventos;
- 1.103. A solução deverá identificar dados que não foram acessados por um período, podendo especificar a quantidade de dias desejado;
- 1.104. A solução deverá disponibilizar dashboard das informações correlacionadas dos dados do Active Directory, com painéis, indicando no mínimo: Usuários com senha que nunca expira, contas de usuários obsoletas, contas executivas, contas desabilitadas e contas habilitadas com a senha expirada;
- 1.105. A solução deverá disponibilizar dashboard com painéis dos dados correlacionados dos servidores de arquivos Windows, indicando no mínimo: Arquivos sensíveis expostos para toda organização, pastas expostas, permissões obsoletas, permissões direta nas pastas, pastas com permissões inconsistentes e pastas com dados obsoletos;

- 1.106. Deve possuir visualização de indicadores de risco para o Active Directory com configurações que podem ser exploradas por usuários maliciosos, como: Admins com SPNs, contas habilitadas, porém sem uso e contas sem senha;
- 1.107. Deve ser possível comparar os gráficos do dashboard através da console, indicando a diferença dos valores atuais com o período anterior;
- 1.108. Os widgets devem ser configuráveis e customizáveis, podendo alterar o modo de visualização, para alguns tipos, como: widgets de métrica única, widgets de porcentagem e widgets com linha do tempo;
- 1.109. Os alertas devem ser apresentados também em dashboard web que apresente: quantidade de alertas e suas severidades em determinado período, usuários mais alertados em determinado período, tipos de comportamentos suspeitos que mais ocorreram, máquinas que foram mais utilizadas para as ações suspeitas, classificação dos alertas dentro de um cenário de ataque cibernético;
- 1.110. A solução deverá possuir Widget de geolocalização com mapa indicando a origem da ação para os alertas gerados;
- 1.111. A solução deverá possuir uma tela de visualização de eventos, podendo realizar pesquisas e filtros à cerca de todas as atividades e dados do ambiente;
- 1.112. Todos os eventos podem ser filtrados e organizados no mínimo por: tipo de evento, ID do evento, operação, status e plataforma;
- 1.113. A solução ofertada deve manter o log das operações de abrir, criar, apagar, modificar, renomear e acesso negado aos arquivos e pastas;
- 1.114. A solução deverá fornecer a visão das permissões efetivas, ou seja, agregando permissões de Share e NTFS;
- 1.115. A solução deve fornecer método para assinalar ou associar um ou mais usuários como "Proprietário(s)" de uma pasta ou grupo;
- 1.116. Deve ser possível definir uma data e horário para busca dos eventos;

- 1.117. A solução deverá possuir filtro para última atividade registrada do usuário, facilitando a busca de contas que estão atualmente inativas;
- 1.118. Os logs apresentados pela solução ofertada devem conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto, caminho (path) dos dados, domínio, arquivo impactado e nome do usuário;
- 1.119. A solução deverá fornecer relatório dos níveis de exposição das permissões, no contexto de dados sensíveis para qualquer pasta e arquivo;
- 1.120. A solução deverá permitir filtragem gráfica, ordenação e agrupamento dos logs;
- 1.121. A solução deverá permitir que os usuários realizem pesquisas baseadas em critérios como: data do evento, servidor ou plataforma em que o evento ocorreu, tipo de evento, arquivos ou diretórios acessados;
- 1.122. Deve ser possível alterar o conjunto de dados (colunas) retornados da consulta aos logs de acordo com a necessidade da informação;
- 1.123. A solução deve ser capaz de identificar qual dado ou arquivo contém informações sensíveis ou confidenciais por meio de busca em seu conteúdo por informações definidas em dicionários fornecidos pelo fabricante ou por informações definidas e customizadas pelo usuário;
- 1.124. A solução deverá fornecer relatório das permissões, incluindo dados da classificação;
- 1.125. A solução deverá fornecer relatório das atividades de acesso dos usuários aos arquivos e pastas;
- 1.126. A solução deverá fornecer relatório dos resultados da classificação dos dados, incluindo o número de hit e regra classificada;
- 1.127. A solução deverá fornecer relatório dos dados que estão com permissões de grupos globais e quem está utilizando estas permissões para acessar as informações;
- 1.128. A solução deve exibir na mesma interface gráfica das informações sobre os permissionamentos e ACL's, a quantidade de informações sensíveis e qual tipo de

informação sensível classificada para facilitar a identificação de potenciais repositórios e pastas superexpostos;

- 1.129. A solução deverá fornecer relatório para SID não resolvido em ACLs;
- 1.130. A solução deverá fornecer relatório sobre grupos de segurança não utilizados ou vazios;
- 1.131. A solução deverá fornecer relatório para usuários desabilitados;
- 1.132. Deve ser possível exportar o relatório em no mínimo 3 tipos de formatos: CSV, Excel e PDF;
- 1.133. Deverá ser possível realizar o agendamento de relatórios;
- 1.134. Deverá ser possível encaminhar o relatório apenas para o proprietário do dado;
- 1.135. A solução deverá coletar informações de ferramentas de perímetro para monitorar atividades na borda da organização de forma e adicionar contexto a segurança dos dados não estruturados e usuários internos;
- 1.136. A solução deverá ser totalmente compatível e integrada ao módulo de análise de comportamento dos usuários e alerta em tempo real;
- 1.137. A solução deverá coletar eventos de auditoria das ferramentas de borda monitoradas através de integração nativa ou syslog;
- 1.138. A solução deverá suportar criptografia para receber os dados de auditoria da borda;
- 1.139. A solução deverá suportar a coleta de eventos de DNS, VPN e Web Proxies;
- 1.140. A solução deverá coletar no mínimo os seguintes eventos e metadados das ferramentas de borda:
  - 1.140.1. DNS: Client DNS query, Upstream DNS query, DNS Zone Transfer e DNS Client Update;
  - 1.140.2. Tipo de evento;

- 1.140.3. Nome da máquina ou objeto para quem a requisição foi feita;
- 1.140.4. Categoria da URL;
- 1.140.5. Reputação da URL
- 1.140.6. DNS record type;
- 1.140.7. Status do evento e motivo do status;
- 1.140.8. VPN: Login e Logout/Disconnect;
- 1.140.9. IP Externo;
- 1.140.10. Tipo de evento;
- 1.140.11. Nome de usuário;
- 1.140.12. Status do evento e Razão do status;
- 1.140.13. Agente
- 1.140.14. Sistema operacional
- 1.140.15. Endereço MAC
- 1.140.16. Tipo de conexão
- 1.140.17. IP de destino
- 1.140.18. Dispositivo de destino
- 1.140.19. Reputação do IP Externo;
- 1.140.20. Web proxies: Proxy access/HTTP Request
- 1.140.21. URL da requisição HTTP;
- 1.140.22. Categorização da URL;
- 1.140.23. Reputação da URL;
- 1.140.24. IP de origem;

- 1.140.25. Nome de usuário;
  - 1.140.26. Tamanho do Upload;
  - 1.140.27. Tamanho do Download
  - 1.140.28. Duração da sessão;
  - 1.140.29. Código do status HTTP;
- 1.141. A solução deverá ter pesquisas pré-definidas de eventos do tipo:
- 1.141.1. Requisições DNS feitas para sites malicioso;
  - 1.141.2. Falhas de requisições web para sites maliciosos;
  - 1.141.3. Falhas de logins de VPN a noite;
  - 1.141.4. Falhas de logins de VPN durante o fim de semana;
  - 1.141.5. Falhas de logins de VPN partindo de fontes suspeitas;
  - 1.141.6. Falhas de logins de VPN feitos por usuários desabilitados ou inativos;
  - 1.141.7. Lista de todas as conexões VPN abertas por mais de um dia esse mês;
  - 1.141.8. Login de VPN a partir de país listado em Blacklist;
  - 1.141.9. Login de VPN a partir de fonte suspeita;
  - 1.141.10. Login de VPN a partir de fonte anonima;
  - 1.141.11. Falhas de requisições web feitas por usuários desabilitados ou inativos;
  - 1.141.12. Maior download de sites de storage na semana;
  - 1.141.13. Maior upload de sites de storage na semana;
  - 1.141.14. Maior download de site web suspeito no dia e na semana;
  - 1.141.15. Maior upload de site web suspeito no dia e na semana;
  - 1.141.16. Requisições a sites web suspeitos;

- 1.141.17. A solução deverá suportar receber eventos syslog de dispositivos que utilizem TLS;
- 1.141.18. A solução deverá identificar e alertar eventos originados em geolocalização suspeita para a organização que serão identificadas a partir do IP externo do usuário, quando coletado;
- 1.142. A solução deverá oferecer proteção e alerta para ataques do tipo:
  - 1.142.1. Mudança entre localização física distante em curto período;
  - 1.142.2. Credentials stuffing;
  - 1.142.3. Força bruta;
  - 1.142.4. Tunelamento por DNS;
  - 1.142.5. Reconhecimento por DNS Zone Transfer;
  - 1.142.6. DNS Cache Snooping;
  - 1.142.7. DNS Cache poisoning

## **2. ITEM 2: SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO**

- 2.1.Os serviços de instalação e configuração deverão compreender, no mínimo:
- 2.2.a implantação completa do projeto, ou seja, deverão contemplar todos os componentes no ambiente tecnológico dessa administração;
- 2.3.responsabilização por todos os instrumentais necessários durante o período de implantação e testes de aceitação;
- 2.4.instalação e configuração de todo ferramental tecnológico fornecido para atender as funcionalidades e requisitos descritos.
- 2.5.providenciar o planejamento de testes, fornecendo um “Plano de Homologação e Testes” contendo todo o processo de homologação dos produtos e detalhamento dos testes que serão executados para validar a solução implementada;

- 2.6. execução de uma série de testes funcionais básicos para verificar o perfeito funcionamento do ambiente, seguindo os procedimentos definidos no “Plano de Homologação e Testes”, sendo tais testes a serem obrigatoriamente executados nos componentes de hardware e software envolvidos no projeto;
- 2.7. elaboração da “Documentação e Finalização do Projeto”, que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e ou gerencial.
- 2.8. Caberá à Contratada a disponibilização de todos os recursos necessários à instalação da solução.

### **3. ITEM 3: SERVIÇO DE TREINAMENTO**

- 3.1. Os treinamentos deverão contemplar a explanação teórica e prática para administradores da solução adquirida.
- 3.2. Os treinamentos poderão ser remotos ou a CONTRATANTE disponibilizará em seu ambiente uma sala para a execução dos treinamentos, com infraestrutura e apoio básicos (mesas, cadeiras, projetor, tela de projeção, computadores); em caso de impossibilidade de realização no ambiente da CONTRATANTE, caberá à Contratada arcar com toda a infraestrutura (salas, instalações e equipamentos, recursos audiovisuais, coffee-break etc.).
- 3.3. O treinamento a ser ofertado não possui obrigatoriedade de ser oficial do Fabricante da solução, contudo deve ser baseado em documentação oficial ou autorizado por ele.
- 3.4. A carga mínima exigida para este treinamento é de 20 horas.
- 3.5. A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 4 (quatro) horas de instrução diária, com a possibilidade de dividir a turma em dois períodos.
- 3.6. Poderão ser demandadas a quantidade de até 2 (duas) turmas, sendo cada uma com no máximo 10 (dez) participantes.



3.7.A CONTRATANTE resguardar-se-á do direito de acompanhar e avaliar o treinamento com instrumento próprio e, caso a mesma não atinja os requisitos mínimos especificados, esta deverá ser reestruturada e aplicada novamente, sem nenhum custo adicional à CONTRATANTE.

3.8.O conteúdo programático do treinamento deverá contemplar, no mínimo, mas não se restringindo, informações necessárias a:

3.9.Procedimentos de instalação física e lógica;

3.10. Procedimentos necessários à configuração técnica e a completa operação do produto;

3.11. Procedimentos de manutenção do produto que devem ser realizados pelos técnicos do Órgão;

3.12. Apresentação geral da solução fornecida;

3.13. Descrição detalhada das partes e componentes de toda a solução, apresentando suas características funcionais;

3.14. Introdução do conceito de classificação, monitoramento e auditoria de dados e comportamento de usuários;

3.15. Visão completa da estrutura do AD, com possibilidades de administrar seu repositório de usuários e grupos de segurança utilizando uma interface única, juntamente com a gestão de seus servidores de arquivos;

3.16. Auditoria eficiente do Active Directory e File Server, fornecendo à equipe de TI visibilidade de todos os eventos ocorridos;

3.17. Gestão e controle de Permissionamento, de Registro de Eventos, de Análise Comportamental e Forense de todas as plataformas monitoradas;

3.18. Criação e/ou emissão de Relatórios, visando facilitar o controle sobre o que acontece em todos os ambientes;

3.19. Alertas de eventos, quando alguma ação for disparada;

- 3.20. Consultas e pesquisas de eventos fora de comportamento normal.
- 3.21. Auditoria de autenticação em aplicações web.
- 3.22. Outros tópicos da solução necessários ao pleno domínio da solução e suas Integrações poderão ser explanados em comum acordo ente as partes na Reunião Inicial de Projeto.
- 3.23. Quando da conclusão do treinamento, a Contratada disponibilizará à CONTRATANTE relatório da execução do evento, contendo no mínimo os seguintes dados:
  - 3.24. Nomes dos participantes e respectivo controle de frequência;
  - 3.25. Conteúdo do treinamento aplicado;
  - 3.26. Data e Hora;
  - 3.27. Carga horaria executada.

#### **4. DA GARANTIA E SUPORTE TÉCNICO**

- 4.1.A contratada deverá prover a garantia, atualização e suporte técnico da solução durante toda a vigência contratual, a partir da data de emissão do Termo de Recebimento Definitivo referente à implantação e operacionalização da solução no ambiente tecnológico do MinC, e deverá contemplar obrigatoriamente no mínimo:
  - 4.2.Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;
  - 4.3.Atualização dos softwares fornecidos se houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos;
  - 4.4.Correções de falhas (bugs) de software durante o período contratual, sendo executadas pela Contratada e/ou pelo Fabricante da solução, sem ônus adicionais;

- 4.5. Entrega, por parte da Contratada, de manuais técnicos e/ou documentação da solução fornecida, já entregues anteriormente, em caso de alterações dos mesmos, sem ônus adicionais para a Contratante;
- 4.6. As novas versões do objeto contratado deverão ser disponibilizadas em até 5 (cinco) dias corridos, a partir do lançamento oficial da versão.
- 4.7. Caso os serviços de manutenção e suporte técnico para todos os componentes da solução não sejam executados diretamente pela Contratada, mas sim pelo próprio Fabricante ou por empresa(s) representante(s) ou credenciada(s) por este, a Contratada deverá comunicar tal fato ao MinC, e assegurar que todos os padrões de atendimento e demais requisitos contratuais serão cumpridos. O aceite por parte dessa administração do atendimento não exime a Contratada da responsabilidade integral pelo atendimento e cumprimento dos prazos acordados.
- 4.8. Somente serão aceitas soluções originais do fabricante dos componentes da solução.
- 4.9. A Contratada deverá disponibilizar acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (website) para todos os produtos que compõem a solução, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, "troubleshootings", com pesquisa efetuada através de ferramentas de busca) e atualizações.
- 4.10. O atendimento deverá ser sob o regime 24x7 (24 horas por dia, 7 dias na semana), com disponibilidade de Central de Atendimento para abertura de chamados via sistema, e-mail, ligação gratuita ("0800") ou por Ordem de Serviço (O.S.).
- 4.11. O acesso para 'downloads' de 'patches', 'fixes', 'drivers' e quaisquer outras atualizações necessárias, devem estar disponíveis 24x7 (vinte e quatro horas por dia, sete dias por semana), durante todo o período de suporte, e podem ser feitos através de http ou ftp, no sítio do fabricante do 'software';
- 4.12. A Contratante deve ter o direito de realizar a atualização do software durante todo o período de suporte técnico, por uma versão mais recente quando disponibilizada, e

sempre que julgar necessário. As novas versões devem estar disponíveis para ‘download’, no sítio do fabricante do ‘software’;

4.13. Caso seja necessária a utilização de senha para ‘download’ de ‘patches’, ‘fixes’, ‘drivers’ e quaisquer outras atualizações no sítio do fabricante do ‘software’, esta deverá ser fornecida diretamente à Contratante, durante todo o período de manutenção;

4.14. Todo e qualquer licenciamento deverá ser feito em nome da Contratante, durante todo o período de manutenção;

4.15. A vigência contratual abrangerá a prestação de suporte, manutenção e atualização da solução pelo período contratual a partir da emissão do Termo de Recebimento Definitivo da solução.

4.16. Durante o período de vigência contratual, o licitante vencedor deverá atender às solicitações da CONTRATANTE, em qualquer horário, respeitando as condições e níveis de serviço especificados.

4.17. Entende-se por “Garantia” ou “Suporte” ou “Manutenção”, doravante denominada unicamente como “Garantia”, toda atividade do tipo “corretiva” não periódica que variavelmente poderá ocorrer, durante todo o período de garantia; esta possui suas causas em falhas e erros no software, e trata da correção dos problemas atuais e não iminentes de desenvolvimento do mesmo. Esta “Garantia” inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, devendo contemplar, sem nenhum ônus, as seguintes atividades incluindo, mas não se limitando a:

4.18. recuperação de desastres, desinstalações, reconfigurações ou reinstalações decorrentes de falhas de software;

4.19. atualização da versão de software – toda e qualquer evolução incluindo correções em bibliotecas, “patches”, “fixes”, “service packs”, “releases”, “versions”, “builds”, vacinas extras específicas, “updates”, “upgrades”, e englobando inclusive versões

não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado;

4.20. qualquer correção decorrente de erros ou falhas cometidas na execução dos serviços contratados e/ou decorrentes de integração e adequação sistêmica, desde que, comprovadamente, não tenham se dado em função de falhas nas especificações feitas pelo MinC.

4.21. Os serviços de manutenção e suporte técnico deverão ser executados com base nos seguintes parâmetros:

Modalidade	Descrição
Atendimento Telefônico (Help Desk)	Chamados abertos através de ligação telefônica, e-mail ou sistema Web, em regime de 24x7: 24 horas por dia, 7 dias por semana.
Atendimento Remoto	Atendimento remoto de chamados técnicos, por meio de acesso remoto via VPN, "TeamViewer", "Cisco Webex" "SysAid" ou outra ferramenta similar, desde que tecnicamente viável e mediante autorização expressa da dessa administração conforme os padrões de segurança do Órgão, objetivando análise e solução remota dos problemas apresentados.
Atendimento Presencial (on-site)	Atendimentos técnicos executados nas dependências da dessa administração, através de visita de profissional especializado, com a finalidade de resolver os chamados.

4.22. Quando couber, no caso de atendimento remoto por meio de ferramenta adequada (via VPN, por exemplo), este deverá ser comunicado previamente à CONTRATANTE, que efetuará o cadastramento do responsável pelo atendimento, e disponibilizará os recursos necessários para a execução da demanda.

4.23. Todo o serviço de suporte técnico/manutenção deve ser solicitado inicialmente via Help Desk, ficando a transferência do atendimento para o Atendimento Remoto condicionado à autorização da dessa administração.

4.24. Todo o serviço de suporte técnico/manutenção solicitado inicialmente via Help Desk, deve ser transferido para o Atendimento Presencial quando o atendimento do Help Desk não for suficiente para solução do problema sem a intervenção presencial de um técnico.

#### 4.25. Definição de prazos:

Prazo	Descrição
Início de Atendimento	Período que compreende o tempo entre o registro de abertura do chamado técnico até o primeiro contato do técnico e/ou comparecimento de um técnico ao local (quando necessário).
Solução de Contorno	Período compreendido entre o “Início de Atendimento” e a apresentação de solução de contorno, sendo definida como uma alternativa que viabilize a operacionalização do ambiente até o tratamento definitivo do incidente.
Solução Definitiva	Período decorrente entre o “Início de Atendimento” até o momento em que a solução for disponibilizada em plena e perfeita condição de funcionamento no local onde está implantada, estando condicionada à aprovação e ateste da equipe técnica da dessa administração, conforme o caso.

4.26. A critério dessa administração o Início do Atendimento, assim como sua execução poderá ser agendado ou adiado e, nestes casos, a contagem de horas para a resolução do chamado fica prorrogada para ser contabilizada a partir da data do novo agendamento.

4.27. A Contratada poderá solicitar a prorrogação de qualquer dos prazos de início e término de atendimento de chamados, desde que o faça antes do seu vencimento e com a devida justificativa.

#### 4.28. Níveis de Severidade:

Severidade	Descrição	Atendimento
CRÍTICA	Incidente que ocasiona a inoperância total da solução ou de algum componente, com a indisponibilidade para qualquer tipo de funcionalidade, comprometendo de forma crítica o ambiente negocial da dessa administração.	Os chamados de Severidade CRÍTICA deverão ser atendidos a qualquer hora do dia ou da noite (cobertura 24 x 7), seja em dia útil, final de semana ou feriado, e não poderão ser interrompidos até a recuperação plena do funcionamento da Solução, mesmo que se estenda para períodos noturnos e dias não úteis como sábados, domingos e feriados.

		O atendimento cuja severidade for classificada como CRÍTICA deverá ser realizado obrigatoriamente ON-SITE.
ALTA	Incidente que ocasiona a inoperância parcial da solução ou de algum componente, com o comprometimento do funcionamento e/ou performance da solução, porém sem interrupção completa.	Os chamados de Severidade ALTA deverão ser atendidos a qualquer hora do dia ou da noite (cobertura 24 x 7), seja em dia útil, final de semana ou feriado e não poderão ter o atendimento interrompido até a recuperação plena do funcionamento da Solução, mesmo que se estenda para períodos noturnos e dias não úteis como sábados, domingos e feriados.  Os chamados de Severidade ALTA poderão ser opcionalmente atendidos on-site a critério da dessa administração.
MÉDIA	Incidente que não ocasiona indisponibilidade do sistema, contudo afeta de modo significativo a performance desta, sendo preliminarmente solucionado temporariamente mediante aplicação de solução de contorno disponível.	Os chamados de Severidade MÉDIA deverão ser atendidos em dias úteis, em horário comercial (das 8:00 às 18:00), e opcionalmente em final de semana ou feriado, conforme agendamento prévio.
BAIXA	Atividades que não impactam na disponibilidade da solução, como diagnósticos, configurações, consultas técnicas, esclarecimentos.	Os chamados de suporte de Severidade BAIXA opcionalmente poderão ser atendidos em dias úteis, em horário comercial (das 8:00 às 18:00).

4.29. A severidade do chamado poderá ser reavaliada quando verificado que esta foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e resolução.

4.30. Para o atendimento das atividades demandadas, a Contratada deverá atender os seguintes prazos constantes no quadro a seguir, conforme o nível de severidade aplicado (Acordo de Níveis de Serviço):

Severidade	Início de Atendimento	Solução de Contorno	Solução Definitiva
CRÍTICA	Até 2 horas.	Até 24 horas.	Até 72 horas.
ALTA	Até 4 horas.	Até 48 horas.	Até 96 horas.
MÉDIA	Até 8 horas.	Até 72 horas.	Até 120 horas.
BAIXA	Até 12 horas.	Até 96 horas.	Até 240 horas.

- 4.31. Casos em que a Contratada não puder executar os serviços de suporte até o limite dos prazos de atendimento, tais chamados não atendidos deverão ser devidamente documentados, contendo a justificativa da Contratada e o aceite do Gestor, observando-se o preceito da razoabilidade e considerando-se os prejuízos à Contratante. Em caso de não aceite da justificativa por parte da Contratante, serão aplicadas as penalidades cabíveis à Contratada.
- 4.32. O não atendimento a um chamado técnico somente poderá ser justificado em casos de motivo de força maior ou por dependência da CONTRATANTE; neste caso, a Contratada deverá formalizar antecipadamente ao Gestor do Contrato ou ao Fiscal Técnico os motivos que impedem a execução do serviço demandado.
- 4.33. Todos os serviços deverão ser prestados em consonância com as melhores práticas e recomendações de mercado e do Fabricante da solução.
- 4.34. Um chamado técnico só poderá ser dado como concluído após verificação e aceite do responsável da CONTRATANTE.
- 4.35. Chamados fechados sem anuência da Contratante ou sem que a(s) demanda(s) tenha(m) sido de fato resolvida(s) deverão ser reabertos e os prazos contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.
- 4.36. A Contratada deverá manter um cadastro das pessoas indicadas pela Contratante, as quais poderão efetuar abertura e autorizar o fechamento de chamados.
- 4.37. Cada pessoa cadastrada no sistema deverá receber identificação e senha que permitam acesso seguro ao sistema de informação da Contratada, de maneira a evitar que pessoas não autorizadas possam acionar o serviço.



- 4.38. A conclusão do atendimento técnico se dará quando ocorrer a “Solução Definitiva” do problema mencionado no chamado (Severidades CRÍTICA, ALTA e MÉDIA), e/ou sanando a dúvida (Severidade BAIXA), estando a conclusão condicionada à aprovação do Fiscal Técnico do Contrato.
- 4.39. É vedado à Contratada interromper o atendimento até que o serviço seja recolocado em pleno estado de funcionamento, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados, não cabendo custos adicionais à Contratante.
- 4.40. Em caso de vício(s) insanável(is) nos componentes da solução que impossibilitem o funcionamento da solução de segurança, o(s) componente(s) defeituoso(s) deverá(ão) ser substituído(s) definitivamente em até 10 (dez) dias úteis após a notificação da Contratante, juntamente com a descrição sucinta e precisa do problema ocorrido.
- 4.41. Sempre que houver quebra de Acordo de Nível de Serviços, a Contratante emitirá notificação à Contratada, que terá prazo máximo de 5 (cinco) dias corridos, contados a partir do recebimento do ofício, para apresentar as justificativas para as falhas verificadas. Caso não haja manifestação dentro desse prazo ou caso a Contratante entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação de penalidades previstas, conforme o nível de serviço transgredido.
- 4.42. Na ocorrência de uma situação emergencial na qual já exista chamado técnico aberto, é esperado que tanto o atendimento quanto o restabelecimento da solução sejam feitos de forma imediata, sem a necessidade de abertura de novo chamado técnico.
- 4.43. Chamados fechados sem anuência da Contratante ou sem que a(s) demanda(s) tenha(m) sido de fato resolvida(s) deverão ser reabertos e os prazos contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.
- 4.44. Os chamados técnicos só poderão ser encerrados após expressa anuência do Gestor do Contrato ou do Fiscal Técnico.

- 4.45. Chamados fechados sem anuência da dessa administração ou sem que a(s) demanda(s) tenha(m) sido de fato resolvida(s) deverão ser reabertos e os prazos contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.
- 4.46. A Contratada deverá manter um cadastro das pessoas indicadas pela dessa administração, as quais poderão efetuar abertura e autorizar o fechamento de chamados.
- 4.47. Cada pessoa cadastrada no sistema deverá receber identificação e senha que permitam acesso seguro ao sistema de informação da Contratada, de maneira a evitar que pessoas não autorizadas possam acionar o serviço.
- 4.48. No fechamento do chamado deverá ser emitido, por parte da Contratada, um "Relatório Técnico de Atendimento", a ser encaminhado à dessa administração, apresentando no mínimo as seguintes informações:
- 4.49. Número de identificação do chamado;
- 4.50. Data e hora do chamado;
- 4.51. Data e hora do início e do término do atendimento;
- 4.52. Total de horas utilizadas para atendimento completo;
- 4.53. Severidade da ocorrência;
- 4.54. Identificação do problema/incidente;
- 4.55. Solução de contorno aplicada (quando couber);
- 4.56. Solução definitiva aplicada.



## **Anexo II - Apendice II - Caderno de Especificacoes Tecnicas.pdf**

## **ESPECIFICAÇÃO TÉCNICA MÍNIMA DA SOLUÇÃO**

**1. LOTE 01 (ÚNICO) - ITEM 1 – Solução tecnológica para atendimento das exigências da política de segurança da informação, compliance e governança de dados não estruturados, pelo período de 36 meses.**

- 1.1. Solução de tecnologia que permitirá o atendimento das exigências da política de segurança da informação, compliance e governança de dados não estruturados, elevando o nível de proteção das informações no ambiente tecnológico do Ministério da Cultura (MinC), de forma a atender ao que cabe a LGPD no tocante a dados não estruturados.
- 1.2. Permitir a detecção de comportamentos suspeitos em diretórios de usuários e servidores de arquivos. Além disso, a solução poderá ser migrada para a nuvem, modelo SAS, conforme necessidade futura ou preferência do contratante, desde que observadas as regulamentações legais referentes à localização dos dados e à privacidade das informações.
- 1.3. A solução tecnológica proposta será licenciada pelo período de 36 meses, para garantir a governança e conformidade dos ambientes de dados não estruturados presentes nos servidores AD, NAS, Windows da organização e aplicações web. Adicionalmente, será possível modificar o licenciamento durante o período contratual para se adequar a plataformas em nuvem, plataforma SAS, conforme as especificações detalhadas no termo de referência.
- 1.4. **Requisitos Mínimos Gerais**
- 1.5. A solução de proteção de credenciais deverá ser capaz de analisar em tempo real e prevenir comportamentos suspeitos em aplicações web, mesmo que estas não estejam integradas ao Active Directory;
- 1.6. Comunicar-se através de API HTTP REST ou UDP com a aplicação web protegida, calculando e fornecendo em tempo real um score de risco e o nível de risco que este score representa, para cada evento de autenticação que ocorre em uma dada aplicação;

- 1.7. Assegurar a comunicação entre a solução de proteção de credenciais e a aplicação web protegida através de criptografia de chaves simétricas;
- 1.8. Possibilitar a criação e configuração de políticas de risco, possuindo no mínimo 4 níveis de risco parametrizáveis a serem definidos em cada política;
- 1.9. Fornecer para cada autenticação analisada o score de risco processado acompanhado da ação (permitir, notificar, desafiar ou bloquear) indicada para o nível de risco do evento em questão, de acordo com a política definida;
- 1.10. Possibilitar o agrupamento de credencias, de modo que uma credencial possa estar associada a mais de uma aplicação web protegida;
- 1.11. Não exigir tokens, dispositivos móveis, códigos ou outras informações adicionais para o processamento de eventos;
- 1.12. Ser capaz de processar e fornecer o score de risco tanto para autenticações com a credencial e senha corretos como para autenticações com credencial e/ou senha incorretos;
- 1.13. Possuir uma base de inteligência de segurança para ser utilizada na mensuração do risco dos acessos, construída com informações próprias e públicas (OSINT), de modo a identificar IPs de má reputação e/ou utilizados para serviço de proxy;
- 1.14. Realizar a mensuração de risco no processo de autenticação sem armazenar e sem ter acesso a senha da credencial em questão, em nenhuma hipótese.
- 1.15. Construir padrão de comportamento de uma credencial com base no histórico de seu uso, composto minimamente por navegador, dispositivo, localização geográfica (cidade e país), sistema operacional, identificador do provedor de internet;
- 1.16. Identificar desvios no padrão de comportamento de uma credencial, possibilitando o envio de notificações, apresentação de desafios (token, captcha ou similares) e bloqueio de acesso, a depender da política de risco definida;
- 1.17. Realizar a mensuração de risco de todos os acessos levando em consideração o padrão de comportamento da credencial e a base de inteligência de segurança;

- 1.18. Todos os eventos processados e armazenados pela solução deverão ser georreferenciados de acordo com o endereço IP de origem, contendo minimamente país, cidade, latitude e longitude;
- 1.19. Permitir a notificação de usuários com base em política de risco, através do disparo via SMTP de e-mail, possibilitando a redação de mensagem personalizada em editor HTML, contendo detalhes do evento em questão como cidade de acesso, data e hora, ip de origem, navegador e um link para que o usuário responda se reconhece o acesso ou não;
- 1.20. Inserir no padrão de comportamento da credencial novas informações quando o usuário confirma através da notificação recebida a veracidade do acesso;
- 1.21. Possibilitar o envio de e-mail para administrador quando um usuário nega a veracidade de um acesso através da notificação recebida;
- 1.22. Ser capaz de bloquear o processo de autenticação de usuários com base no score de risco do evento, mesmo quando a credencial e a senha forem corretamente imputadas no ato da autenticação;
- 1.23. Identificar ataques do tipo “força bruta”, elevando de forma automática e proporcional o score de risco do IP de origem do acesso com base no número de tentativas de autenticações fracassadas em um curto intervalo de tempo;
- 1.24. A reputação das origens detectadas como geradores de ataques de força bruta deverá decair após determinado tempo, e o tempo de decaimento da reputação deverá aumentar em função da recorrência de tentativas de ataques de força bruta;
- 1.25. Enviar eventos, cifrados nativamente com chave simétrica, via webhook para URL a ser configurada em interface gráfica, com base na política de risco definida;
- 1.26. Elevar o score de risco de uma credencial ao detectar mudança geográfica de longa distância;



- 1.27. Identificar os top 10 usuários que representam maior atividade de risco acumulado em um intervalo de tempo escolhido, informando o nome do usuário (credencial) e score de risco acumulado;
- 1.28. Segmentar os eventos processados por credencial, possibilitando navegar por todos os eventos de uma dada credencial, informando no mínimo os seguintes detalhes de cada evento: Cidade, coordenadas geográficas, nome do navegador utilizado, nome do dispositivo utilizado no acesso, endereço ip de origem, score de risco e resultado da ação com base na política definida, código identificador do ISP (internet service provider) e descritivo com análise do evento;
- 1.29. Possuir gráfico que represente os eventos de uma credencial específica em um intervalo de tempo escolhido, distinguindo-os pelos níveis de risco definidos em política;
- 1.30. Possuir dashboard para visualização de eventos no formato de representação de mapa geográfico que possibilite distinguir diferentes níveis de risco, detalhando informações como cidade, usuário, score de risco do evento, data e hora do evento;
- 1.31. Possuir dashboard para visualização do risco organizacional em um intervalo de tempo escolhido, segmentado por aplicação protegida ou não, distinguindo o volume de eventos que representam o risco mitigado, o risco em mitigação (pendente) e o risco assumido;
- 1.32. Possuir dashboard para identificação e análise de ataques, contendo minimamente as seguintes estatísticas:
  - 1.32.1. Endereços IPs com maior incidência de credenciais únicas autenticadas com sucesso e com falha na autenticação;
  - 1.32.2. Credenciais com maior incidência de acessos originados em cidades distintas autenticados com sucesso e com falha na autenticação;
  - 1.32.3. Credenciais com maior incidência de eventos de autenticação com sucesso e com falha na autenticação;

- 1.32.4. Endereços IPs com maior número de eventos de autenticação com sucesso e com falha na autenticação;
- 1.32.5. Cidades com maior número de eventos;
- 1.32.6. Países com maior número de eventos;
- 1.32.7. Gráfico com quantidade de eventos classificados por resposta da política de risco em razão do tempo;
- 1.32.8. Possuir integração com soluções do tipo “single-sign-on”, disponibilizando no mínimo, de forma nativa, o RH-SSO e Keycloak;
- 1.32.9. Possuir integração nativa com a autenticação de tecnologias de mercado, sendo minimamente wordpress, openssh, cloudflare, moodle e keycloak;
- 1.32.10. Ser capaz de processar eventos originados em IPv4 e IPv6;
- 1.32.11. Possuir identificador único para todos os eventos processados pela solução;
- 1.32.12. Possuir mecanismo de processamento e armazenamento de eventos baseado em tecnologias escaláveis;
- 1.32.13. Possuir mecanismo de dissuasão de ataques de força-bruta baseado em desafio criptográfico a ser decifrado pelo navegador cliente, sem necessidade de interação dos usuários da aplicação protegida;
- 1.33. O nível de dificuldade do desafio criptográfico deverá ser parametrizável;
- 1.34. Deverá ser fornecido um painel para visualização e análise de eventos, inspeção e segurança de credenciais/usuários;
- 1.35. O painel deverá possuir um mecanismo nativo para gestão de usuários que podem acessá-lo, incluindo integração nativa com os seguintes sistemas de diretório de usuários: Active Directory, LDAP e Keycloak/RH-SSO;
- 1.36. O painel deverá ser desenvolvido em tecnologia web based, acessível através de protocolo https;

- 1.37. O painel deverá criptografar toda a comunicação com as fontes geradoras de eventos, e ao armazenar eventos em base de dados, anonimizar o campo que contém a informação de nome de usuário, seja este um CPF, matrícula, e-mail ou uma string (ex: nome.sobrenome);
- 1.38. As informações disponibilizadas no painel de visualização deverão ser orientadas a intervalo de datas, e fornecer estatísticas dos eventos de segurança que são protegidas pela solução, sendo minimamente: Usuários que mais geram eventos de segurança no ambiente protegido; Endereços IPs que mais geram eventos de segurança no ambiente protegido; Incidentes de segurança mais frequentes;
- 1.39. O painel deverá permitir visualizar detalhes de cada evento de segurança coletado;
- 1.40. Permitir filtrar eventos por usuário (credencial);
- 1.41. Permitir filtrar eventos por endereço IP de origem;
- 1.42. Todos os softwares fornecidos deverão ser licenciados pelo período mínimo de 36 (trinta e seis) meses, e contemplar garantia, suporte e atualização dos respectivos fabricantes. A solução deverá ser dimensionada para o volume de usuários indicados no quadro de itens do presente termo de referência, devendo ser considerado o período contratual de 36 (trinta e seis) meses para a licença de uso que integra a solução;
- 1.43. O fabricante ou a solução ofertada de governança de dados, deverá possuir certificação de compliance como ISO 27001 ou similar, garantindo que seus produtos atendam aos rígidos padrões da indústria e sejam auditados e revisados regularmente;
- 1.44. Por se tratar de solução entregue como serviço na nuvem, modelo SAS, o fabricante deve adotar abordagem baseada em risco para seu sistema de gestão de segurança da informação (SGSI), a implantação de um SGSI, reduz o risco de divulgação, modificação ou destruição não autorizada, acidental ou intencional das informações, além de constantemente, realizar testes de penetração de terceiros no

tenant e varredura automatizada para garantir a segurança do software; Por se tratar de software de proteção de dados sensíveis com análise comportamental de usuários para ambientes computacionais o fabricante ou a solução de governança de dados deverá ser certificada ISO/IEC 27017;

- 1.45. A solução deve suportar a utilização de servidores virtualizados para os componentes;
- 1.46. A solução deve possibilitar a configuração de credencial diferente para cada servidor/serviço a ser monitorado;
- 1.47. Por se tratar de software de proteção de dados sensíveis o fabricante ou a solução de governança de dados deverá ser certificada ISO/IEC 27701 que trata do gerenciamento de privacidade da informação dentro da organização;
- 1.48. A solução deverá monitorar múltiplos domínios e servidores de arquivos Windows e NAS (Network Attached Storage) do ambiente, incluindo: Contas, estruturas de diretórios, permissões e eventos;
- 1.49. A solução a ser fornecida deverá possuir compatibilidade comprovada no site dos fabricantes dos storage Netapp e EMC para que tenha compatibilidade com a Infraestrutura do órgão;
- 1.50. Caso a solução necessite da instalação de agente para o monitoramento dos eventos do Active Directory e servidores de arquivos, os agentes não devem gerar nenhuma queda de performance nos servidores;
- 1.51. O gerenciamento da solução deverá ser centralizado para todos os módulos;
- 1.52. A solução deverá monitorar todos os domain controllers instalados em qualquer versão do Windows Server 2003 até 2022;
- 1.53. A solução deverá monitorar todos os servidores de arquivos instalados em Windows Server 2012 até Windows Server 2022;
- 1.54. A solução deverá monitorar no mínimo, os seguintes eventos do Microsoft Active Directory: Conta habilitada e desabilitada; Autenticação de conta (TGT); Renovação

de acesso (TGS); Replicação de AD; Logon de conta no DC; Criação, deleção, renomeação, modificação, remoção e adição de membros no objeto do DS; Requisição de acesso NTLM; Alteração de senha de usuário; Conta de usuário bloqueada; Conta de usuário desbloqueada; Netlogon vulnerável; Criação, deleção e modificação de GPO; Tentativa de reset de senha; Criação, atualização, deleção, habilitação e desabilitação de tarefa agendada dentro do DC; Alteração de política de kerberos;

- 1.55. A solução deverá monitorar no mínimo, os seguintes eventos do servidor de Arquivos Windows: Arquivo criado; Arquivo deletado; Arquivo aberto; Arquivo renomeado; Arquivo modificado; Mudança de proprietário do arquivo; Permissões adicionadas no arquivo; Permissões removidas no arquivo; Proteção adicionado no arquivo; Proteção removida no arquivo; Pasta criada; Pasta deletada; Pasta renomeada; Mudança de proprietário da pasta; Permissões adicionadas na pasta; Permissões removidas na pasta; Proteção adicionada na pasta; Proteção removida na pasta;
- 1.56. Deverá ser possível definir os proprietários das pastas através da console;
- 1.57. A solução deverá exibir uma lista com todas as contas de usuários monitoradas, indicando no mínimo, o tipo de conta (serviço, executiva ou administrativa) e grupos que fazem parte;
- 1.58. A solução deverá exibir o repositório monitorado em formato hierárquico, expandindo as pastas e sub-pastas até o nível do arquivo, permitindo a visualização de quais usuários tem acesso a cada recurso e as permissões concedidas;
- 1.59. A solução deverá possuir uma visão bi-direcional indicando através de uma visualização gráfica e interativa, todas as permissões dos usuários e grupos, e quais as permissões aplicadas nos objetos (arquivos e pastas);
- 1.60. A solução deverá disponibilizar a visibilidade de permissões, sejam elas NTFS ou share;

- 1.61. A solução deverá realizar a classificação do conteúdo do arquivo, fornecendo visibilidade sobre onde residem os dados confidenciais e sensíveis no sistema de arquivos;
- 1.62. A solução deverá utilizar múltiplos fatores para realizar a classificação do conteúdo do arquivo, incluindo: Metadados, padrões, dicionários, palavras-chave e expressão regular;
- 1.63. A solução deverá indicar para qualquer arquivo e pasta no servidor monitorado, uma visualização gráfica contendo o nível de exposição e indicando se o arquivo é sensível ou não a partir da classificação realizada;
- 1.64. A solução deverá fornecer filtros para visualizar apenas determinados objetos de dados em exibição gráfica interativa, incluindo pastas protegidas e pastas únicas;
- 1.65. A solução deverá incluir informações de classificação de dados na tela das permissões, incluindo: nome da regra classificada, e quantidade de instâncias sensíveis encontradas no arquivo;
- 1.66. A solução deverá fornecer para as permissões, tipos de exibição diferentes, incluindo exibições hierárquicas e de lista;
- 1.67. A solução deverá realizar a classificação de imagens através de OCR ou tecnologia similar;
- 1.68. A solução deverá possibilitar a criação de regras customizadas para que os administradores possam definir o que deve ser encontrado dentro do conteúdo do arquivo, de acordo com a necessidade organizacional;
- 1.69. Deve ser possível realizar o agendamento do escaneamento das regras de classificação, podendo especificar: horário, dia e tempo de duração;
- 1.70. Deve ser possível exportar eventos e informações apenas referente aos dados classificados como sensíveis;

- 1.71. Deve ser possível definir o escopo do ambiente que vai ser classificado, podendo definir: repositório, arquivo, pasta, tipo de arquivo, quantidade mínima de hits e outros;
- 1.72. A solução deverá auxiliar na conformidade com a LGPD, identificando aonde os dados pessoais (CPF, RG, CNH e outros) são armazenados, quem tem acesso aos dados e quais são as atividades em cima destes dados;
- 1.73. A solução deverá escanear e classificar no mínimo os seguintes tipos de arquivos: doc, docx, dwg, rtf, ppt, xls, txt, csv, pdf, xml, log, eml, jpg, jpeg, gif, png, rar e zip;
- 1.74. A solução deverá encontrar em arquivos com formato tabular, palavras chaves em cabeçalhos e colunas;
- 1.75. Deve ser possível limitar escopo dentro dos sistemas de arquivos a ser analisado;
- 1.76. Deve ser possível definir partes específicas do arquivo a serem analisadas no escopo como: Colunas específicas de arquivos do tipo Microsoft Excel, cabeçalho, rodapé e marca d'água de arquivos Microsoft Office, links de arquivos Microsoft Office e PDF;
- 1.77. A solução deverá indicar no painel de diretórios: o nome da regra, a quantidade de hits do termo sensível encontrado nos arquivos e pastas e a quantidade de hits incluindo sub-pastas;
- 1.78. A solução deverá ser entregue utilizando a infraestrutura em nuvem disponibilizada pelo fabricante, e poderá ser ofertada e instalada localmente desde que não retenha os logs nativos e não seja baseada em software livre.
- 1.79. A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar acesso a dados que o usuário não costuma acessar;

- 1.80. Nos alertas em tempo real, deve ser possível configurar para que, um usuário, uma pasta, um período ou uma ação específica seja alertada, caso ocorra ação que os envolva;
- 1.81. A solução deverá notificar os administradores através de alertas para qualquer tipo de atividade incomum e comportamentos suspeitos de usuários;
- 1.82. Os alertas da solução deverão ser encaminhados via SMTP e SNMP;
- 1.83. A solução deverá suportar a configuração de respostas automáticas para os alertas gerados, possibilitando a execução automática de scripts ou comandos pré-configurados;
- 1.84. A solução deverá realizar a análise comportamental dos usuários de forma automática, através de machine learning, entendendo o comportamento e rotina de todos os usuários, o que acessam, quando acessam e onde;
- 1.85. A solução deverá contemplar a assinatura de uma base de conhecimentos do fornecedor com mais de 150 modelos de alertas pré-configurados de eventos suspeitos tais como: Ataques de sequestro de dados (ransomware); Detecção de ferramentas nocivas ao ambiente; Ações com acessos negados; Ações de escalasões de privilégios; Excesso de tentativas de autenticação ou contas bloqueadas; Atividades suspeitas em dados parados e/ou inativos; Alterações anormais em GPO; Ataques de golden ticket; Ataques de injeção de códigos maliciosos; Ataques de descoberta de contas com NTLM e Kerberos; Ataques de força bruta;
- 1.86. Os modelos de alertas devem ser atualizados de forma automática;
- 1.87. A solução deverá detectar ameaças em todos os estágios de um ataque cibernético, incluindo dashboard que indica algumas categorias como: Reconhecimento, intrusão, exploração, escalação de privilégio, movimento lateral, negação de serviço e exfiltração de dados;
- 1.88. A solução deverá monitorar a atividade do usuário para construir perfis de comportamento e usar os modelos de ameaça baseados em comportamento para alertar quando uma atividade anormal no Active Directory é detectada;



- 1.89. A solução deverá construir perfis de comportamento comparando as atividades dos usuários e entidades e identificando a relação entre eles;
- 1.90. A solução deverá possuir um período de aprendizado, para que seja feito a coleta de eventos e identificação do comportamento dos usuários para a criação do perfil comportamental;
- 1.91. A solução deverá realizar a descoberta de contas privilegiadas de forma automática, identificando contas executivas, contas de serviço e contas administrativas baseado no seu comportamento e nos grupos de segurança que a conta está inserida;
- 1.92. A solução deverá exibir uma lista com todas as contas de usuários monitoradas, indicando no mínimo, o tipo de conta (serviço, executiva ou administrativa) e grupos que fazem parte;
- 1.93. A solução deverá possuir dashboard de alertas indicando os usuários mais alertados, dispositivos e modelos de alertas gerados;
- 1.94. A solução deverá possuir política de automação para remediação de exposição de dados para toda a organização, removendo as permissões globais das pastas e arquivos;
- 1.95. A solução deverá possuir política de automação para remediar permissões inconsistentes, garantindo que não exista permissão quebrada e aplicando as entradas de permissão corretamente para as sub-pastas e arquivos;
- 1.96. As políticas de automação para remediação devem ser executadas de forma manual e automática;
- 1.97. A solução deverá possuir política de automação para remediar permissões inconsistentes, garantindo que não exista permissão quebrada e aplicando as entradas de permissão corretamente para as sub-pastas e arquivos;

- 1.98. Para análise forense do usuário mais alertado, o dashboard deve possuir página que agregue dados importantes do comportamento daquele usuário. Isso permite que se identifique o cenário do possível ataque;
- 1.99. No dashboard, a partir de um alerta selecionado, a solução deve exibir página que liste todos os eventos ocorridos que motivaram a ferramenta a gerar o alerta. A lista desses eventos deve ser customizável podendo ser filtrada, exibidas ou ocultas colunas e agregada por valores das colunas exibidas;
- 1.100. A solução deverá suportar na busca dos eventos a utilização de operadores relativos, auxiliando na investigação e nos resultados esperados;
- 1.101. Deve ser possível salvar uma pesquisa customizada, agendando para que ela possa ser executada de forma automática e que os administradores recebam as informações necessárias de forma periódica;
- 1.102. A solução deverá suportar a criação e utilização de flags para serem aplicadas as contas de usuários e aos recursos monitorados, essas flags podem ser utilizadas nos filtros e na aba de eventos;
- 1.103. A solução deverá identificar dados que não foram acessados por um período, podendo especificar a quantidade de dias desejado;
- 1.104. A solução deverá disponibilizar dashboard das informações correlacionadas dos dados do Active Directory, com painéis, indicando no mínimo: Usuários com senha que nunca expira, contas de usuários obsoletas, contas executivas, contas desabilitadas e contas habilitadas com a senha expirada;
- 1.105. A solução deverá disponibilizar dashboard com painéis dos dados correlacionados dos servidores de arquivos Windows, indicando no mínimo: Arquivos sensíveis expostos para toda organização, pastas expostas, permissões obsoletas, permissões direta nas pastas, pastas com permissões inconsistentes e pastas com dados obsoletos;

- 1.106. Deve possuir visualização de indicadores de risco para o Active Directory com configurações que podem ser exploradas por usuários maliciosos, como: Admins com SPNs, contas habilitadas, porém sem uso e contas sem senha;
- 1.107. Deve ser possível comparar os gráficos do dashboard através da console, indicando a diferença dos valores atuais com o período anterior;
- 1.108. Os widgets devem ser configuráveis e customizáveis, podendo alterar o modo de visualização, para alguns tipos, como: widgets de métrica única, widgets de porcentagem e widgets com linha do tempo;
- 1.109. Os alertas devem ser apresentados também em dashboard web que apresente: quantidade de alertas e suas severidades em determinado período, usuários mais alertados em determinado período, tipos de comportamentos suspeitos que mais ocorreram, máquinas que foram mais utilizadas para as ações suspeitas, classificação dos alertas dentro de um cenário de ataque cibernético;
- 1.110. A solução deverá possuir Widget de geolocalização com mapa indicando a origem da ação para os alertas gerados;
- 1.111. A solução deverá possuir uma tela de visualização de eventos, podendo realizar pesquisas e filtros à cerca de todas as atividades e dados do ambiente;
- 1.112. Todos os eventos podem ser filtrados e organizados no mínimo por: tipo de evento, ID do evento, operação, status e plataforma;
- 1.113. A solução ofertada deve manter o log das operações de abrir, criar, apagar, modificar, renomear e acesso negado aos arquivos e pastas;
- 1.114. A solução deverá fornecer a visão das permissões efetivas, ou seja, agregando permissões de Share e NTFS;
- 1.115. A solução deve fornecer método para assinalar ou associar um ou mais usuários como "Proprietário(s)" de uma pasta ou grupo;
- 1.116. Deve ser possível definir uma data e horário para busca dos eventos;

- 1.117. A solução deverá possuir filtro para última atividade registrada do usuário, facilitando a busca de contas que estão atualmente inativas;
- 1.118. Os logs apresentados pela solução ofertada devem conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto, caminho (path) dos dados, domínio, arquivo impactado e nome do usuário;
- 1.119. A solução deverá fornecer relatório dos níveis de exposição das permissões, no contexto de dados sensíveis para qualquer pasta e arquivo;
- 1.120. A solução deverá permitir filtragem gráfica, ordenação e agrupamento dos logs;
- 1.121. A solução deverá permitir que os usuários realizem pesquisas baseadas em critérios como: data do evento, servidor ou plataforma em que o evento ocorreu, tipo de evento, arquivos ou diretórios acessados;
- 1.122. Deve ser possível alterar o conjunto de dados (colunas) retornados da consulta aos logs de acordo com a necessidade da informação;
- 1.123. A solução deve ser capaz de identificar qual dado ou arquivo contém informações sensíveis ou confidenciais por meio de busca em seu conteúdo por informações definidas em dicionários fornecidos pelo fabricante ou por informações definidas e customizadas pelo usuário;
- 1.124. A solução deverá fornecer relatório das permissões, incluindo dados da classificação;
- 1.125. A solução deverá fornecer relatório das atividades de acesso dos usuários aos arquivos e pastas;
- 1.126. A solução deverá fornecer relatório dos resultados da classificação dos dados, incluindo o número de hit e regra classificada;
- 1.127. A solução deverá fornecer relatório dos dados que estão com permissões de grupos globais e quem está utilizando estas permissões para acessar as informações;
- 1.128. A solução deve exibir na mesma interface gráfica das informações sobre os permissionamentos e ACL's, a quantidade de informações sensíveis e qual tipo de

informação sensível classificada para facilitar a identificação de potenciais repositórios e pastas superexpostos;

- 1.129. A solução deverá fornecer relatório para SID não resolvido em ACLs;
- 1.130. A solução deverá fornecer relatório sobre grupos de segurança não utilizados ou vazios;
- 1.131. A solução deverá fornecer relatório para usuários desabilitados;
- 1.132. Deve ser possível exportar o relatório em no mínimo 3 tipos de formatos: CSV, Excel e PDF;
- 1.133. Deverá ser possível realizar o agendamento de relatórios;
- 1.134. Deverá ser possível encaminhar o relatório apenas para o proprietário do dado;
- 1.135. A solução deverá coletar informações de ferramentas de perímetro para monitorar atividades na borda da organização de forma e adicionar contexto a segurança dos dados não estruturados e usuários internos;
- 1.136. A solução deverá ser totalmente compatível e integrada ao módulo de análise de comportamento dos usuários e alerta em tempo real;
- 1.137. A solução deverá coletar eventos de auditoria das ferramentas de borda monitoradas através de integração nativa ou syslog;
- 1.138. A solução deverá suportar criptografia para receber os dados de auditoria da borda;
- 1.139. A solução deverá suportar a coleta de eventos de DNS, VPN e Web Proxies;
- 1.140. A solução deverá coletar no mínimo os seguintes eventos e metadados das ferramentas de borda:
  - 1.140.1. DNS: Client DNS query, Upstream DNS query, DNS Zone Transfer e DNS Client Update;
  - 1.140.2. Tipo de evento;

- 1.140.3. Nome da máquina ou objeto para quem a requisição foi feita;
- 1.140.4. Categoria da URL;
- 1.140.5. Reputação da URL
- 1.140.6. DNS record type;
- 1.140.7. Status do evento e motivo do status;
- 1.140.8. VPN: Login e Logout/Disconnect;
- 1.140.9. IP Externo;
- 1.140.10. Tipo de evento;
- 1.140.11. Nome de usuário;
- 1.140.12. Status do evento e Razão do status;
- 1.140.13. Agente
- 1.140.14. Sistema operacional
- 1.140.15. Endereço MAC
- 1.140.16. Tipo de conexão
- 1.140.17. IP de destino
- 1.140.18. Dispositivo de destino
- 1.140.19. Reputação do IP Externo;
- 1.140.20. Web proxies: Proxy access/HTTP Request
- 1.140.21. URL da requisição HTTP;
- 1.140.22. Categorização da URL;
- 1.140.23. Reputação da URL;
- 1.140.24. IP de origem;

- 1.140.25. Nome de usuário;
  - 1.140.26. Tamanho do Upload;
  - 1.140.27. Tamanho do Download
  - 1.140.28. Duração da sessão;
  - 1.140.29. Código do status HTTP;
- 1.141. A solução deverá ter pesquisas pré-definidas de eventos do tipo:
- 1.141.1. Requisições DNS feitas para sites malicioso;
  - 1.141.2. Falhas de requisições web para sites maliciosos;
  - 1.141.3. Falhas de logins de VPN a noite;
  - 1.141.4. Falhas de logins de VPN durante o fim de semana;
  - 1.141.5. Falhas de logins de VPN partindo de fontes suspeitas;
  - 1.141.6. Falhas de logins de VPN feitos por usuários desabilitados ou inativos;
  - 1.141.7. Lista de todas as conexões VPN abertas por mais de um dia esse mês;
  - 1.141.8. Login de VPN a partir de país listado em Blacklist;
  - 1.141.9. Login de VPN a partir de fonte suspeita;
  - 1.141.10. Login de VPN a partir de fonte anonima;
  - 1.141.11. Falhas de requisições web feitas por usuários desabilitados ou inativos;
  - 1.141.12. Maior download de sites de storage na semana;
  - 1.141.13. Maior upload de sites de storage na semana;
  - 1.141.14. Maior download de site web suspeito no dia e na semana;
  - 1.141.15. Maior upload de site web suspeito no dia e na semana;
  - 1.141.16. Requisições a sites web suspeitos;

- 1.141.17. A solução deverá suportar receber eventos syslog de dispositivos que utilizem TLS;
- 1.141.18. A solução deverá identificar e alertar eventos originados em geolocalização suspeita para a organização que serão identificadas a partir do IP externo do usuário, quando coletado;
- 1.142. A solução deverá oferecer proteção e alerta para ataques do tipo:
  - 1.142.1. Mudança entre localização física distante em curto período;
  - 1.142.2. Credentials stuffing;
  - 1.142.3. Força bruta;
  - 1.142.4. Tunelamento por DNS;
  - 1.142.5. Reconhecimento por DNS Zone Transfer;
  - 1.142.6. DNS Cache Snooping;
  - 1.142.7. DNS Cache poisoning

## **2. ITEM 2: SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO**

- 2.1.Os serviços de instalação e configuração deverão compreender, no mínimo:
- 2.2.a implantação completa do projeto, ou seja, deverão contemplar todos os componentes no ambiente tecnológico dessa administração;
- 2.3.responsabilização por todos os instrumentais necessários durante o período de implantação e testes de aceitação;
- 2.4.instalação e configuração de todo ferramental tecnológico fornecido para atender as funcionalidades e requisitos descritos.
- 2.5.providenciar o planejamento de testes, fornecendo um “Plano de Homologação e Testes” contendo todo o processo de homologação dos produtos e detalhamento dos testes que serão executados para validar a solução implementada;



- 2.6. execução de uma série de testes funcionais básicos para verificar o perfeito funcionamento do ambiente, seguindo os procedimentos definidos no “Plano de Homologação e Testes”, sendo tais testes a serem obrigatoriamente executados nos componentes de hardware e software envolvidos no projeto;
- 2.7. elaboração da “Documentação e Finalização do Projeto”, que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e ou gerencial.
- 2.8. Caberá à Contratada a disponibilização de todos os recursos necessários à instalação da solução.

### **3. ITEM 3: SERVIÇO DE TREINAMENTO**

- 3.1. Os treinamentos deverão contemplar a explanação teórica e prática para administradores da solução adquirida.
- 3.2. Os treinamentos poderão ser remotos ou a CONTRATANTE disponibilizará em seu ambiente uma sala para a execução dos treinamentos, com infraestrutura e apoio básicos (mesas, cadeiras, projetor, tela de projeção, computadores); em caso de impossibilidade de realização no ambiente da CONTRATANTE, caberá à Contratada arcar com toda a infraestrutura (salas, instalações e equipamentos, recursos audiovisuais, coffee-break etc.).
- 3.3. O treinamento a ser ofertado não possui obrigatoriedade de ser oficial do Fabricante da solução, contudo deve ser baseado em documentação oficial ou autorizado por ele.
- 3.4. A carga mínima exigida para este treinamento é de 20 horas.
- 3.5. A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 4 (quatro) horas de instrução diária, com a possibilidade de dividir a turma em dois períodos.
- 3.6. Poderão ser demandadas a quantidade de até 2 (duas) turmas, sendo cada uma com no máximo 10 (dez) participantes.

3.7.A CONTRATANTE resguardar-se-á do direito de acompanhar e avaliar o treinamento com instrumento próprio e, caso a mesma não atinja os requisitos mínimos especificados, esta deverá ser reestruturada e aplicada novamente, sem nenhum custo adicional à CONTRATANTE.

3.8.O conteúdo programático do treinamento deverá contemplar, no mínimo, mas não se restringindo, informações necessárias a:

3.9.Procedimentos de instalação física e lógica;

3.10. Procedimentos necessários à configuração técnica e a completa operação do produto;

3.11. Procedimentos de manutenção do produto que devem ser realizados pelos técnicos do Órgão;

3.12. Apresentação geral da solução fornecida;

3.13. Descrição detalhada das partes e componentes de toda a solução, apresentando suas características funcionais;

3.14. Introdução do conceito de classificação, monitoramento e auditoria de dados e comportamento de usuários;

3.15. Visão completa da estrutura do AD, com possibilidades de administrar seu repositório de usuários e grupos de segurança utilizando uma interface única, juntamente com a gestão de seus servidores de arquivos;

3.16. Auditoria eficiente do Active Directory e File Server, fornecendo à equipe de TI visibilidade de todos os eventos ocorridos;

3.17. Gestão e controle de Permissionamento, de Registro de Eventos, de Análise Comportamental e Forense de todas as plataformas monitoradas;

3.18. Criação e/ou emissão de Relatórios, visando facilitar o controle sobre o que acontece em todos os ambientes;

3.19. Alertas de eventos, quando alguma ação for disparada;

- 3.20. Consultas e pesquisas de eventos fora de comportamento normal.
- 3.21. Auditoria de autenticação em aplicações web.
- 3.22. Outros tópicos da solução necessários ao pleno domínio da solução e suas Integrações poderão ser explanados em comum acordo ente as partes na Reunião Inicial de Projeto.
- 3.23. Quando da conclusão do treinamento, a Contratada disponibilizará à CONTRATANTE relatório da execução do evento, contendo no mínimo os seguintes dados:
  - 3.24. Nomes dos participantes e respectivo controle de frequência;
  - 3.25. Conteúdo do treinamento aplicado;
  - 3.26. Data e Hora;
  - 3.27. Carga horaria executada.

#### **4. DA GARANTIA E SUPORTE TÉCNICO**

- 4.1.A contratada deverá prover a garantia, atualização e suporte técnico da solução durante toda a vigência contratual, a partir da data de emissão do Termo de Recebimento Definitivo referente à implantação e operacionalização da solução no ambiente tecnológico do MinC, e deverá contemplar obrigatoriamente no mínimo:
  - 4.2.Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;
  - 4.3.Atualização dos softwares fornecidos se houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos;
  - 4.4.Correções de falhas (bugs) de software durante o período contratual, sendo executadas pela Contratada e/ou pelo Fabricante da solução, sem ônus adicionais;

- 4.5. Entrega, por parte da Contratada, de manuais técnicos e/ou documentação da solução fornecida, já entregues anteriormente, em caso de alterações dos mesmos, sem ônus adicionais para a Contratante;
- 4.6. As novas versões do objeto contratado deverão ser disponibilizadas em até 5 (cinco) dias corridos, a partir do lançamento oficial da versão.
- 4.7. Caso os serviços de manutenção e suporte técnico para todos os componentes da solução não sejam executados diretamente pela Contratada, mas sim pelo próprio Fabricante ou por empresa(s) representante(s) ou credenciada(s) por este, a Contratada deverá comunicar tal fato ao MinC, e assegurar que todos os padrões de atendimento e demais requisitos contratuais serão cumpridos. O aceite por parte dessa administração do atendimento não exime a Contratada da responsabilidade integral pelo atendimento e cumprimento dos prazos acordados.
- 4.8. Somente serão aceitas soluções originais do fabricante dos componentes da solução.
- 4.9. A Contratada deverá disponibilizar acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (website) para todos os produtos que compõem a solução, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, "troubleshootings", com pesquisa efetuada através de ferramentas de busca) e atualizações.
- 4.10. O atendimento deverá ser sob o regime 24x7 (24 horas por dia, 7 dias na semana), com disponibilidade de Central de Atendimento para abertura de chamados via sistema, e-mail, ligação gratuita ("0800") ou por Ordem de Serviço (O.S.).
- 4.11. O acesso para 'downloads' de 'patches', 'fixes', 'drivers' e quaisquer outras atualizações necessárias, devem estar disponíveis 24x7 (vinte e quatro horas por dia, sete dias por semana), durante todo o período de suporte, e podem ser feitos através de http ou ftp, no sítio do fabricante do 'software';
- 4.12. A Contratante deve ter o direito de realizar a atualização do software durante todo o período de suporte técnico, por uma versão mais recente quando disponibilizada, e

sempre que julgar necessário. As novas versões devem estar disponíveis para ‘download’, no sítio do fabricante do ‘software’;

4.13. Caso seja necessária a utilização de senha para ‘download’ de ‘patches’, ‘fixes’, ‘drivers’ e quaisquer outras atualizações no sítio do fabricante do ‘software’, esta deverá ser fornecida diretamente à Contratante, durante todo o período de manutenção;

4.14. Todo e qualquer licenciamento deverá ser feito em nome da Contratante, durante todo o período de manutenção;

4.15. A vigência contratual abrangerá a prestação de suporte, manutenção e atualização da solução pelo período contratual a partir da emissão do Termo de Recebimento Definitivo da solução.

4.16. Durante o período de vigência contratual, o licitante vencedor deverá atender às solicitações da CONTRATANTE, em qualquer horário, respeitando as condições e níveis de serviço especificados.

4.17. Entende-se por “Garantia” ou “Suporte” ou “Manutenção”, doravante denominada unicamente como “Garantia”, toda atividade do tipo “corretiva” não periódica que variavelmente poderá ocorrer, durante todo o período de garantia; esta possui suas causas em falhas e erros no software, e trata da correção dos problemas atuais e não iminentes de desenvolvimento do mesmo. Esta “Garantia” inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, devendo contemplar, sem nenhum ônus, as seguintes atividades incluindo, mas não se limitando a:

4.18. recuperação de desastres, desinstalações, reconfigurações ou reinstalações decorrentes de falhas de software;

4.19. atualização da versão de software – toda e qualquer evolução incluindo correções em bibliotecas, “patches”, “fixes”, “service packs”, “releases”, “versions”, “builds”, vacinas extras específicas, “updates”, “upgrades”, e englobando inclusive versões

não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado;

4.20. qualquer correção decorrente de erros ou falhas cometidas na execução dos serviços contratados e/ou decorrentes de integração e adequação sistêmica, desde que, comprovadamente, não tenham se dado em função de falhas nas especificações feitas pelo MinC.

4.21. Os serviços de manutenção e suporte técnico deverão ser executados com base nos seguintes parâmetros:

Modalidade	Descrição
Atendimento Telefônico (Help Desk)	Chamados abertos através de ligação telefônica, e-mail ou sistema Web, em regime de 24x7: 24 horas por dia, 7 dias por semana.
Atendimento Remoto	Atendimento remoto de chamados técnicos, por meio de acesso remoto via VPN, "TeamViewer", "Cisco Webex" "SysAid" ou outra ferramenta similar, desde que tecnicamente viável e mediante autorização expressa da dessa administração conforme os padrões de segurança do Órgão, objetivando análise e solução remota dos problemas apresentados.
Atendimento Presencial (on-site)	Atendimentos técnicos executados nas dependências da dessa administração, através de visita de profissional especializado, com a finalidade de resolver os chamados.

4.22. Quando couber, no caso de atendimento remoto por meio de ferramenta adequada (via VPN, por exemplo), este deverá ser comunicado previamente à CONTRATANTE, que efetuará o cadastramento do responsável pelo atendimento, e disponibilizará os recursos necessários para a execução da demanda.

4.23. Todo o serviço de suporte técnico/manutenção deve ser solicitado inicialmente via Help Desk, ficando a transferência do atendimento para o Atendimento Remoto condicionado à autorização da dessa administração.

4.24. Todo o serviço de suporte técnico/manutenção solicitado inicialmente via Help Desk, deve ser transferido para o Atendimento Presencial quando o atendimento do Help Desk não for suficiente para solução do problema sem a intervenção presencial de um técnico.

4.25. Definição de prazos:

Prazo	Descrição
Início de Atendimento	Período que compreende o tempo entre o registro de abertura do chamado técnico até o primeiro contato do técnico e/ou comparecimento de um técnico ao local (quando necessário).
Solução de Contorno	Período compreendido entre o “Início de Atendimento” e a apresentação de solução de contorno, sendo definida como uma alternativa que viabilize a operacionalização do ambiente até o tratamento definitivo do incidente.
Solução Definitiva	Período decorrente entre o “Início de Atendimento” até o momento em que a solução for disponibilizada em plena e perfeita condição de funcionamento no local onde está implantada, estando condicionada à aprovação e ateste da equipe técnica da dessa administração, conforme o caso.

4.26. A critério dessa administração o Início do Atendimento, assim como sua execução poderá ser agendado ou adiado e, nestes casos, a contagem de horas para a resolução do chamado fica prorrogada para ser contabilizada a partir da data do novo agendamento.

4.27. A Contratada poderá solicitar a prorrogação de qualquer dos prazos de início e término de atendimento de chamados, desde que o faça antes do seu vencimento e com a devida justificativa.

4.28. Níveis de Severidade:

Severidade	Descrição	Atendimento
CRÍTICA	Incidente que ocasiona a inoperância total da solução ou de algum componente, com a indisponibilidade para qualquer tipo de funcionalidade, comprometendo de forma crítica o ambiente negocial da dessa administração.	Os chamados de Severidade CRÍTICA deverão ser atendidos a qualquer hora do dia ou da noite (cobertura 24 x 7), seja em dia útil, final de semana ou feriado, e não poderão ser interrompidos até a recuperação plena do funcionamento da Solução, mesmo que se estenda para períodos noturnos e dias não úteis como sábados, domingos e feriados.

		O atendimento cuja severidade for classificada como CRÍTICA deverá ser realizado obrigatoriamente ON-SITE.
ALTA	Incidente que ocasiona a inoperância parcial da solução ou de algum componente, com o comprometimento do funcionamento e/ou performance da solução, porém sem interrupção completa.	Os chamados de Severidade ALTA deverão ser atendidos a qualquer hora do dia ou da noite (cobertura 24 x 7), seja em dia útil, final de semana ou feriado e não poderão ter o atendimento interrompido até a recuperação plena do funcionamento da Solução, mesmo que se estenda para períodos noturnos e dias não úteis como sábados, domingos e feriados.  Os chamados de Severidade ALTA poderão ser opcionalmente atendidos on-site a critério da dessa administração.
MÉDIA	Incidente que não ocasiona indisponibilidade do sistema, contudo afeta de modo significativo a performance desta, sendo preliminarmente solucionado temporariamente mediante aplicação de solução de contorno disponível.	Os chamados de Severidade MÉDIA deverão ser atendidos em dias úteis, em horário comercial (das 8:00 às 18:00), e opcionalmente em final de semana ou feriado, conforme agendamento prévio.
BAIXA	Atividades que não impactam na disponibilidade da solução, como diagnósticos, configurações, consultas técnicas, esclarecimentos.	Os chamados de suporte de Severidade BAIXA opcionalmente poderão ser atendidos em dias úteis, em horário comercial (das 8:00 às 18:00).

4.29. A severidade do chamado poderá ser reavaliada quando verificado que esta foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e resolução.

4.30. Para o atendimento das atividades demandadas, a Contratada deverá atender os seguintes prazos constantes no quadro a seguir, conforme o nível de severidade aplicado (Acordo de Níveis de Serviço):



Severidade	Início de Atendimento	Solução de Contorno	Solução Definitiva
CRÍTICA	Até 2 horas.	Até 24 horas.	Até 72 horas.
ALTA	Até 4 horas.	Até 48 horas.	Até 96 horas.
MÉDIA	Até 8 horas.	Até 72 horas.	Até 120 horas.
BAIXA	Até 12 horas.	Até 96 horas.	Até 240 horas.

- 4.31. Casos em que a Contratada não puder executar os serviços de suporte até o limite dos prazos de atendimento, tais chamados não atendidos deverão ser devidamente documentados, contendo a justificativa da Contratada e o aceite do Gestor, observando-se o preceito da razoabilidade e considerando-se os prejuízos à Contratante. Em caso de não aceite da justificativa por parte da Contratante, serão aplicadas as penalidades cabíveis à Contratada.
- 4.32. O não atendimento a um chamado técnico somente poderá ser justificado em casos de motivo de força maior ou por dependência da CONTRATANTE; neste caso, a Contratada deverá formalizar antecipadamente ao Gestor do Contrato ou ao Fiscal Técnico os motivos que impedem a execução do serviço demandado.
- 4.33. Todos os serviços deverão ser prestados em consonância com as melhores práticas e recomendações de mercado e do Fabricante da solução.
- 4.34. Um chamado técnico só poderá ser dado como concluído após verificação e aceite do responsável da CONTRATANTE.
- 4.35. Chamados fechados sem anuência da Contratante ou sem que a(s) demanda(s) tenha(m) sido de fato resolvida(s) deverão ser reabertos e os prazos contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.
- 4.36. A Contratada deverá manter um cadastro das pessoas indicadas pela Contratante, as quais poderão efetuar abertura e autorizar o fechamento de chamados.
- 4.37. Cada pessoa cadastrada no sistema deverá receber identificação e senha que permitam acesso seguro ao sistema de informação da Contratada, de maneira a evitar que pessoas não autorizadas possam acionar o serviço.

- 4.38. A conclusão do atendimento técnico se dará quando ocorrer a “Solução Definitiva” do problema mencionado no chamado (Severidades CRÍTICA, ALTA e MÉDIA), e/ou sanando a dúvida (Severidade BAIXA), estando a conclusão condicionada à aprovação do Fiscal Técnico do Contrato.
- 4.39. É vedado à Contratada interromper o atendimento até que o serviço seja recolocado em pleno estado de funcionamento, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados, não cabendo custos adicionais à Contratante.
- 4.40. Em caso de vício(s) insanável(is) nos componentes da solução que impossibilitem o funcionamento da solução de segurança, o(s) componente(s) defeituoso(s) deverá(ão) ser substituído(s) definitivamente em até 10 (dez) dias úteis após a notificação da Contratante, juntamente com a descrição sucinta e precisa do problema ocorrido.
- 4.41. Sempre que houver quebra de Acordo de Nível de Serviços, a Contratante emitirá notificação à Contratada, que terá prazo máximo de 5 (cinco) dias corridos, contados a partir do recebimento do ofício, para apresentar as justificativas para as falhas verificadas. Caso não haja manifestação dentro desse prazo ou caso a Contratante entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação de penalidades previstas, conforme o nível de serviço transgredido.
- 4.42. Na ocorrência de uma situação emergencial na qual já exista chamado técnico aberto, é esperado que tanto o atendimento quanto o restabelecimento da solução sejam feitos de forma imediata, sem a necessidade de abertura de novo chamado técnico.
- 4.43. Chamados fechados sem anuência da Contratante ou sem que a(s) demanda(s) tenha(m) sido de fato resolvida(s) deverão ser reabertos e os prazos contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.
- 4.44. Os chamados técnicos só poderão ser encerrados após expressa anuência do Gestor do Contrato ou do Fiscal Técnico.

- 4.45. Chamados fechados sem anuência da dessa administração ou sem que a(s) demanda(s) tenha(m) sido de fato resolvida(s) deverão ser reabertos e os prazos contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.
- 4.46. A Contratada deverá manter um cadastro das pessoas indicadas pela dessa administração, as quais poderão efetuar abertura e autorizar o fechamento de chamados.
- 4.47. Cada pessoa cadastrada no sistema deverá receber identificação e senha que permitam acesso seguro ao sistema de informação da Contratada, de maneira a evitar que pessoas não autorizadas possam acionar o serviço.
- 4.48. No fechamento do chamado deverá ser emitido, por parte da Contratada, um "Relatório Técnico de Atendimento", a ser encaminhado à dessa administração, apresentando no mínimo as seguintes informações:
- 4.49. Número de identificação do chamado;
- 4.50. Data e hora do chamado;
- 4.51. Data e hora do início e do término do atendimento;
- 4.52. Total de horas utilizadas para atendimento completo;
- 4.53. Severidade da ocorrência;
- 4.54. Identificação do problema/incidente;
- 4.55. Solução de contorno aplicada (quando couber);
- 4.56. Solução definitiva aplicada.



## **Anexo III - Apendice III - Roteiro POC.pdf**



MINISTÉRIO DA CULTURA  
COORDENAÇÃO DE INFRAESTRUTURA TECNOLÓGICA  
COINT/CGINT/STII/GSE/GM/MinC  
Site: - <http://www.cultura.gov.br>

## **APÊNDICE III**

### **PROVA DE CONCEITO**

<b>REQUISITO A SER AVALIADO</b>	<b>ATENDE OU NÃO ATENDE</b>
<b>ITEM 1</b>	-
A solução deverá monitorar, no mínimo, os seguintes eventos do Microsoft Active Directory: Conta habilitada e desabilitada; Autenticação de conta (TGT); Renovação de acesso (TGS); Replicação de AD; Logon de conta no DC; Criação, deleção, renomeação, modificação, remoção e adição de membros no objeto do DS; Requisição de acesso NTLM; Alteração de senha de usuário; Conta de usuário bloqueada; Conta de usuário desbloqueada; Netlogon vulnerável; Criação, deleção e modificação de GPO; Tentativa de reset de senha; Criação, atualização, deleção, habilitação e desabilitação de tarefa agendada dentro do DC; Alteração de política de kerberos;	
A solução deverá monitorar múltiplos domínios e servidores de arquivos Windows e NAS (Network Attached Storage) do ambiente, incluindo: Contas, estruturas de diretórios, permissões e eventos;	
Deverá ser possível definir os proprietários das pastas através da console;	
A solução deverá exibir uma lista com todas as contas de usuários monitoradas, indicando no mínimo, o tipo de conta (serviço, executiva ou administrativa) e grupos que fazem parte;	
A solução deverá exibir o repositório monitorado em formato hierárquico, expandindo as pastas e sub-pastas até o nível do arquivo, permitindo a visualização de quais usuários tem acesso a cada recurso e as permissões concedidas;	
A solução deverá possuir uma visão bi-direcional indicando através de uma visualização gráfica e interativa, todas as permissões dos usuários e grupos, e quais as permissões aplicadas nos objetos (arquivos e pastas);	
A solução deverá realizar a classificação do conteúdo do arquivo, fornecendo visibilidade sobre onde residem os dados confidenciais e sensíveis no sistema de arquivos;	
A solução deverá utilizar múltiplos fatores para realizar a classificação do conteúdo do arquivo, incluindo: Metadados, padrões, dicionários, palavras-chave e	

expressão regular;	
A solução deverá incluir informações de classificação de dados na tela das permissões, incluindo: nome da regra classificada, e quantidade de instâncias sensíveis encontradas no arquivo;	
A solução deverá possibilitar a criação de regras customizadas para que os administradores possam definir o que deve ser encontrado dentro do conteúdo do arquivo, de acordo com a necessidade organizacional;	
A solução deverá auxiliar na conformidade com a LGPD, identificando aonde os dados pessoais (CPF, RG, CNH e outros) são armazenados, quem tem acesso aos dados e quais são as atividades em cima destes dados;	
Nos alertas em tempo real, deve ser possível configurar para que, um usuário, uma pasta, um período ou uma ação específica seja alertada, caso ocorra ação que os envolva;	
Os alertas da solução deverão ser encaminhados via SMTP e SNMP;	
A solução deverá suportar a configuração de respostas automáticas para os alertas gerados, possibilitando a execução automática de scripts ou comandos pré-configurados;	
A solução deverá contemplar a assinatura de uma base de conhecimentos do fornecedor com mais de 150 modelos de alertas pré-configurados de eventos suspeitos tais como: Ataques de sequestro de dados (ransomware); Detecção de ferramentas nocivas ao ambiente; Ações com acessos negados; Ações de escalasções de privilégios; Excesso de tentativas de autenticação ou contas bloqueadas; Atividades suspeitas em dados parados e/ou inativos; Alterações anormais em GPO; Ataques de golden ticket; Ataques de injeção de códigos maliciosos; Ataques de descoberta de contas com NTLM e Kerberos; Ataques de força bruta;	
A solução deverá detectar ameaças em todos os estágios de um ataque cibernético, incluindo dashboard que indica algumas categorias como: Reconhecimento, intrusão, exploração, escalação de privilégio, movimento lateral, negação de serviço e exfiltração de dados;	
A solução deverá realizar a descoberta de contas privilegiadas de forma automática, identificando contas executivas, contas de serviço e contas administrativas baseado no seu comportamento e nos grupos de segurança que a conta está inserida;	
A solução deverá possuir dashboard de alertas indicando os usuários mais alertados, dispositivos e modelos de alertas gerados;	
A solução deverá possuir política de automação para remediação de exposição de dados para toda a organização, removendo as permissões globais das pastas e arquivos;	
Para análise forense do usuário mais alertado, o dashboard deve possuir página que agregue dados importantes do comportamento daquele usuário. Isso permite que se identifique o cenário do possível ataque;	
No dashboard, a partir de um alerta selecionado, a solução deve exibir página que liste todos os eventos ocorridos que motivaram a ferramenta a gerar o alerta. A lista desses eventos deve ser customizável podendo ser filtrada, exibidas ou ocultadas colunas e agregada por valores das colunas exibidas;	

Deve ser possível salvar uma pesquisa customizada, agendando para que ela possa ser executada de forma automática e que os administradores recebam as informações necessárias de forma periódica;	
A solução deverá disponibilizar dashboard das informações correlacionadas dos dados do Active Directory, com painéis, indicando no mínimo: Usuários com senha que nunca expira, contas de usuários obsoletas, contas executivas, contas desabilitadas e contas habilitadas com a senha expirada;	
A solução deverá disponibilizar dashboard com painéis dos dados correlacionados dos servidores de arquivos Windows, indicando no mínimo: Arquivos sensíveis expostos para toda organização, pastas expostas, permissões obsoletas, permissões direta nas pastas, pastas com permissões inconsistentes e pastas com dados obsoletos;	
Deve ser possível comparar os gráficos do dashboard através da console, indicando a diferença dos valores atuais com o período anterior;	
A solução deverá possuir uma tela de visualização de eventos, podendo realizar pesquisas e filtros à cerca de todas as atividades e dados do ambiente;	
A solução deverá fornecer relatório das atividades de acesso dos usuários aos arquivos e pastas;	
A solução deverá coletar no mínimo os seguintes eventos e metadados das ferramentas de borda:	
DNS: Client DNS query, Upstream DNS query, DNS Zone Transfer e DNS Client Update;	
Reputação da URL	
Tipo de conexão	
Tamanho do Upload;	
Login de VPN a partir de país listado em Blacklist;	
Login de VPN a partir de fonte suspeita;	
A solução deverá ter pesquisas pré-definidas de eventos do tipo:	
Requisições DNS feitas para sites malicioso;	
Maior download de sites de storage na semana;	
A solução deverá oferecer proteção e alerta para ataques do tipo:	
Tunelamento por DNS;	
Força bruta;	
A solução deverá ser capaz de analisar em tempo real e prevenir comportamentos suspeitos em aplicações web, mesmo que estas não estejam integradas ao Active Directory, atendendo minimamente os seguintes critérios:	
Comunicar-se através de API HTTP REST ou UDP com a aplicação web protegida, calculando e fornecendo em tempo real um score de risco e o nível de risco que este score representa, para cada evento de autenticação que ocorre em uma dada	



aplicação.	
Possibilitar a criação e configuração de políticas de risco, possuindo no mínimo 4 níveis de risco parametrizáveis a serem definidos em cada política.	
Fornecer para cada autenticação analisada o score de risco processado acompanhado da ação (permitir, notificar, desafiar ou bloquear) indicada para o nível de risco do evento em questão, de acordo com a política definida.	
Possibilitar o agrupamento de credencias, de modo que uma credencial possa estar associada a mais de uma aplicação web protegida.	
Ser capaz de processar e fornecer o score de risco tanto para autenticações com a credencial e senha corretos como para autenticações com credencial e/ou senha incorretos.	
Possuir uma base de inteligência de segurança para ser utilizada na mensuração do risco dos acessos, construída com informações próprias e públicas (OSINT), de modo a identificar IPs de má reputação e/ou utilizados para serviço de proxy.	
Realizar a mensuração de risco no processo de autenticação sem armazenar e sem ter acesso a senha da credencial em questão, em nenhuma hipótese.	
Construir padrão de comportamento de uma credencial com base no histórico de seu uso, composto minimamente por navegador, dispositivo, localização geográfica (cidade e país), sistema operacional, identificador do provedor de internet.	
Realizar a mensuração de risco de todos os acessos levando em consideração o padrão de comportamento da credencial e a base de inteligência de segurança.	
Todos os eventos processados e armazenados pela solução deverão ser georreferenciados de acordo com o endereço IP de origem, contendo minimamente país, cidade, latitude e longitude.	
Ser capaz de bloquear o processo de autenticação de usuários com base no score de risco do evento, mesmo quando a credencial e a senha forem corretamente imputadas no ato da autenticação.	
Identificar ataques do tipo “força bruta”, elevando de forma automática e proporcional o score de risco do IP de origem do acesso com base no número de tentativas de autenticações fracassadas em um curto intervalo de tempo.	
A reputação das origens detectadas como geradores de ataques de força bruta deverá decair após determinado tempo, e o tempo de decaimento da reputação deverá aumentar em função da recorrência de tentativas de ataques de força bruta.	
Elevar o score de risco de uma credencial ao detectar mudança geográfica de longa distância.	
Segmentar os eventos processados por credencial, possibilitando navegar por todos os eventos de uma dada credencial, informando no mínimo os seguintes detalhes de cada evento: Cidade, coordenadas geográficas, nome do navegador utilizado, nome do dispositivo utilizado no acesso, endereço ip de origem, score de risco e resultado da ação com base na política definida, código identificador do ISP (internet service provider) e descritivo com análise do evento.	
Possuir gráfico que represente os eventos de uma credencial específica em um	

intervalo de tempo escolhido, distinguindo-os pelos níveis de risco definidos em política.	
Possuir dashboard para visualização de eventos no formato de representação de mapa geográfico que possibilite distinguir diferentes níveis de risco, detalhando informações como cidade, usuário, score de risco do evento, data e hora do evento.	
Possuir dashboard para visualização do risco organizacional em um intervalo de tempo escolhido, segmentado por aplicação protegida ou não, distinguindo o volume de eventos que representam o risco mitigado, o risco em mitigação (pendente) e o risco assumido.	
Ser capaz de processar eventos originados em IPv4 e IPv6.	
Possuir identificador único para todos os eventos processados pela solução.	
Possuir mecanismo de processamento e armazenamento de eventos baseado em tecnologias escaláveis.	
Possuir mecanismo de dissuasão de ataques de força-bruta baseado em desafio criptográfico a ser decifrado pelo navegador cliente, sem necessidade de interação dos usuários da aplicação protegida.	
O nível de dificuldade do desafio criptográfico deverá ser parametrizável.	