

# 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.

Deteção 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
Solução tecnológica para inspeção e segurança de informações institucionais em nuvem						
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 <i>on-premise</i> 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.

1.



## 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://paineldepregcos.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
VALOR TOTAL ANUAL										6.005.892,50

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.

