

Estudo Técnico Preliminar 73/2023

1. Informações Básicas

Número do processo: 01400.013362/2023-15

2. Descrição da necessidade

Estudo de **solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP)** com fornecimento de licenças e ferramenta de descoberta e classificação de dados, controle de acesso, monitoramento de atividade, auditoria e proteção através de bloqueio, criptografia e quarentena, para aplicações e ambientes de armazenamento em nuvem, **Cloud Access Security Broker (CASB)**, incluindo implantação da solução, treinamento e suporte técnico pelo período de 36 (trinta e seis) meses.

2.1. Motivação/Justificativa

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

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

I - política nacional de cultura e política nacional das artes;

II - proteção do patrimônio histórico, artístico e cultural;

III - regulação dos direitos autorais;

IV - assistência ao Ministério do Desenvolvimento Agrário e Agricultura Familiar e ao Instituto Nacional de Colonização e Reforma Agrária nas ações de regularização fundiária, para garantir a preservação da identidade cultural dos remanescentes das comunidades dos quilombos;

V - proteção e promoção da diversidade cultural;

VI - desenvolvimento econômico da cultura e a política de economia criativa;

VII - desenvolvimento e a implementação de políticas e ações de acessibilidade cultural; e

VIII - formulação e implementação de políticas, de programas e de ações para o desenvolvimento do setor museal.

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

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

2.1.4. Assim, as ações de aquisições de equipamentos, de contratações de serviços e soluções de tecnologia da informação para atender as demandas do Ministério da Cultura precisam ser realizadas de forma gradativa e concatenada com aquelas realizadas no âmbito do Ministério do Turismo de modo a que seja possível realizar a adaptação da infraestrutura de tecnologia da informação do Edifício Sede do Ministério da Cultura (localizado no bloco B da

Esplanada dos Ministérios) e dos demais anexos e unidades vinculadas à pasta, sem colocar em risco a continuidade das atividades laborais dos servidores e colaboradores do Ministério da Cultura que ainda fazem uso de equipamentos e serviços de tecnologia da informação providos pelo Ministério do Turismo.

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

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

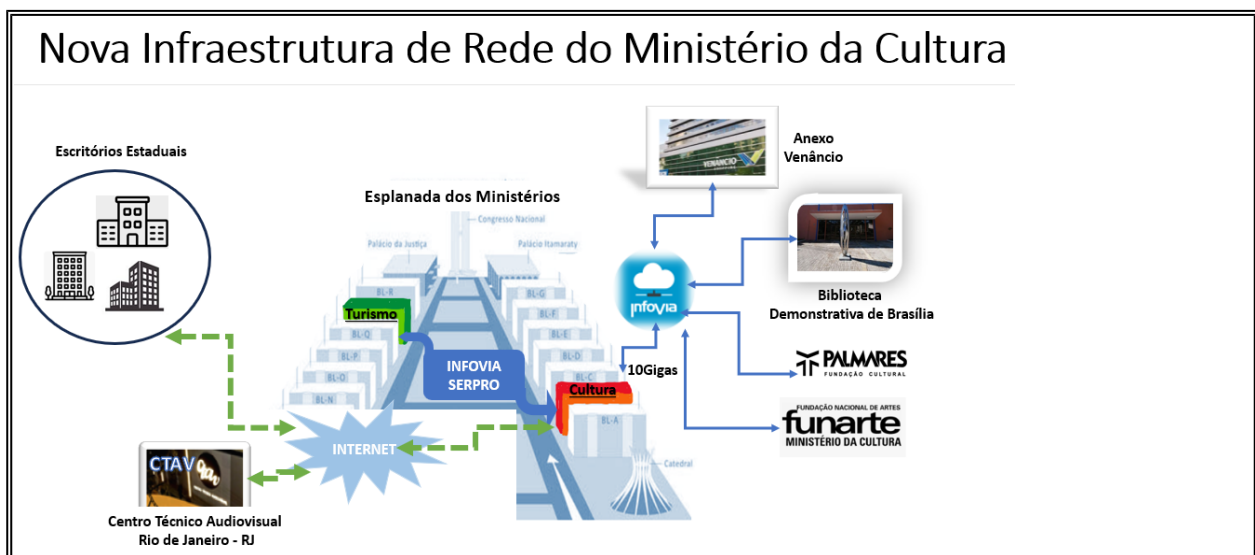
2.1.7 Características da Rede de computadores e do Datacenter do Ministério da Cultura

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

2.1.7.2 Para a composição desta nova topologia, a conectividade entre as unidades do Ministério da Cultura é garantida por meio do uso da **INFOVIA** nos locais em que este recurso está disponível, sendo eles: "**Anexo Edifício Venâncio Shopping**" e na "**Biblioteca Demonstrativa**", localizados na Asa sul; "**Fundação Cultural Palmares**" localizada na asa norte; e **Funarte** localizada no eixo monumental, ambos em Brasília - DF.

2.1.7.3 Além das localidades supracitadas que contam com a possibilidade da conectividade via INFOVIA, há ainda as unidades que terão suas conexões à sede realizadas por meio de links de acesso à internet e uso de tecnologia SDWAN combinada com VPN do tipo SITE-TO-SITE, sendo eles: Todos os Escritórios Estaduais, o Centro Técnico Audiovisual.

2.1.7.4 A topologia, em implantação consta ilustrada na figura a seguir:



2.1.7.5 Diante da topologia de rede supracitadas observa-se que o Datacenter localizado no edifício sede do Ministério da Cultura deverá manter conexão com várias localidades, seja por meio de acesso via internet ou por meio de conexão à INFOVIA, e que portanto, as soluções de armazenamento e processamento, como todas as demais soluções implementadas no Datacenter, precisam ser dimensionadas com capacidade e performance adequadas ao cenário previsto que terá o Datacenter do Edifício sede do Ministério da Cultura como principal provedor dos serviços de Tecnologia da Informação da Pasta.

Necessidade de proteção da informação

2.1.8 O Ministério da Cultura enfrenta desafios significativos devido à natureza diversificada e complexa de suas atribuições, uma vez que a promoção de expressões culturais abrange uma ampla variedade de setores, incluindo artes, patrimônio, indústrias criativas, direitos autorais, diversidade cultural e muito mais. desta forma o gerenciamento eficiente dos recursos de incentivo a cultura, é crucial para assegurar que programas e projetos culturais sejam bem-sucedidos e atinjam seus objetivos.

2.1.9 Considerando que a Pasta passou os últimos anos por várias transformações chegando a ser vinculada a outros órgãos como uma Secretaria Especial, e em que pese o fato de que atualmente o órgão voltou a ser um Ministério estratégico para o Governo Federal, verifica-se que os anos de pouca visibilidade de nenhuma prioridade, impactaram na perda de profissionais e de conhecimento tanto pela evasão de servidores e colaboradores quanto pela descontinuidade de projetos de extrema importância Institucional.

2.1.10 O cenário de pouca priorização pelo qual a Pasta passou, resultou em um legado de sistemas e informações desarrumados e que necessitam urgentemente de ações de retomada do controle das informações, gestão do conhecimento, mapeamento dos sistemas e gestores de informações, promovendo desse modo, uma jornada de governança de dados, possibilitando a aceleração da reconstrução do Ministério da Cultura por meio da disponibilização de novos serviços digitais que alcancem o cidadão e que ao mesmo tempo fortaleçam internamente as equipes para a boa gestão das políticas públicas de incentivo a cultura.

2.1.11 Assim junção dos fatores: ausência de investimentos em tecnologia da informação; falta de priorização orçamentária para as ações relacionadas a cultura; evasão de servidores e colaboradores; e a descontinuidade de programas e projetos estruturantes no âmbito do Ministério da Cultura, proporcionaram a construção do cenário atual onde existem diversos sistemas e repositórios de dados com informações que foram construídas ao longo dos anos e que: tratam-se da história da gestão pública de incentivo a cultura; ou tratam-se de registros de projetos executados com dinheiro público e que precisam prestar contas; ou tratam-se do registro de ações recentes e antigas já executadas pelos gestores públicos e que podem ser auditadas a qualquer tempo.

2.1.12 Desta forma considerando que o Datacenter do Ministério da Cultura, por suas características de provedor de ambiente de sistemas e bancos de dados para os sistemas da Pasta e de suas vinculadas, conforme topologia já citada neste, é possível afirmar que atualmente existem informações de grande valor para o Governo Federal e para a os cidadãos, valores estes cujas definições constam elencados a seguir:

- a) **Valor Estratégico** : Informações relacionadas às estratégias do Ministério, seus objetivos de longo prazo e planos de crescimento, registros de estratégias implementadas e seus resultados.
- b) **Valor Financeiro** : Informações que têm impacto direto nas finanças do Ministério, como dados financeiros, orçamentos, gestão dos recursos de incentivo a cultura, documentação sobre os programas de governo e a execução dos projetos financiados com dinheiro público.
- c) **Valor Operacional** : Informações que sustentam as operações diárias do Ministério, incluindo dados sobre processos, fluxos de trabalho e recursos humanos, agendas políticas e estratégicas.
- d) **Valor Legal e Regulatório** : Informações que estão em conformidade com leis e regulamentos, bem como aquelas que são usadas em processos legais, contratos e conformidade regulatória.
- e) **Valor de Conhecimento** : Informações que são importantes para o aprendizado, inovação e tomada de decisões informadas, incluindo pesquisas, dados de mercado e insights.
- f) **Valor de Reputação e Imagem** : Informações que envolvem a conservação da imagem do Ministério e do Governo Brasileiro perante o público, e outros países.
- g) **Valor de Segurança** : Informações críticas que precisam ser protegidas contra ameaças de revelações de segurança, como dados pessoais processos administrativos internos.
- h) **Valor de Continuidade de Negócios** : Informações que são essenciais para garantir a continuidade das operações em situações de emergência ou desastres.
- i) **Valor de Histórico e Arquivamento** : Informações históricas e arquivadas que podem ser úteis para referência futura, conformidade regulatória ou análise de tendências e prestação de contas.
- j) **Valor Social e Ambiental** : Informações relacionadas ao impacto social e ambiental das atividades do Ministério, incluindo responsabilidade social corporativa e sustentabilidade.

Vulnerabilidades das informações

2.1.13 Ao longo dos últimos anos houve um considerável crescimento do número de ataques e riscos associados a dados sensíveis, isso se deve principalmente pelo crescimento do uso de serviços digitais e pela simplificação de acesso a informação que deve ser ofertada em atendimento as Leis de acesso a informação e a LGPD.

2.1.14 Considerando que o cidadão está cada vez mais familiarizado com os serviços digitais, e que por isso faz uso dos serviços com maior frequência, o meio digital passou a ser alvo de pessoas mal intencionadas que procuram vulnerabilidades em sistemas e equipamentos pessoais ou de governo para explorar e ganhar dinheiro com tais informações ou permissões de acesso, desta forma a informação atualmente acabou se tornando um ativo extremamente valioso para as organizações, no mundo todo, os casos relacionados à violação de dados já atingiram grandes varejistas, instituições financeiras, provedores de aplicações e órgãos do governo.

2.1.15 Em 14 de agosto de 2018 foi sancionada a Lei nº 13.709, Lei Geral de Proteção de Dados (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direitos público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade. Essa Lei cria uma regulamentação para o uso, proteção e transferência de dados pessoais no Brasil, nos âmbitos privado e público

2.1.16 Segundo o artigo 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. Isso inclui protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

2.1.17 Ocorre que as informações de propriedade e responsabilidade do Ministério da Cultura encontra-se espalhadas em diversos sistemas e serviços, cujos repositórios estão em aplicações em produção no datacenter do Ministério da cultura como é o caso das informações constantes da base de dados do SALIC - Sistema de Apoio às Leis de Incentivo a Cultura e de diversos outros sistemas o SEI - Sistema Eletrônico de Informações, *Mapas.cultura.gov.br* e etc.

2.1.18 Existem ainda informações de propriedade e responsabilidade do Ministério da Cultura que encontra-se espalhadas nos órgãos por onde o Ministério da Cultura foi vinculado em gestões passadas, como é o caso do Ministério da Cidadania e do Ministério do Turismo.

2.1.19 Neste cenário em que existem diversos repositórios de informações de responsabilidade do Ministério da Cultura, e que o acesso a estes repositórios de informações não possui um controle refinado, ou seja, há processos no SEI e em outros sistemas que guardam dados financeiros, dados pessoais e registros históricos com níveis básicos de controle de acesso, verifica-se vulneráveis tais repositórios, seja pela ausência de controles ou seja pela ausência de classificação das informações e orientações aos usuários.

2.1.20 Como agravante da situação de vulnerabilidade, existe o fato de não haver ainda no âmbito do ministério, soluções implementadas que venham a fazer o controle de acesso de forma monitorada ou mesmo que bloqueie ou alerte o envio não autorizado de informações.

2.1.21 Neste sentido é importante que esta Pasta venha a adquirir, ainda que de forma gradual, a capacidade de prevenir, detectar e reduzir as vulnerabilidades relacionadas aos seus repositórios de informações, sejam por meio de campanhas de conscientização seja por meio da implementação de soluções automatizadas de controle e monitoramento.

2.1.22 Considerando os fatores já citados, assim como já realizado por outros órgãos do governo federal, verifica-se razoável o estudo da implementação de recursos voltados a prevenção à perda de dados, de forma a possibilitar a atuação desta Pasta de maneira preventiva - ao monitorar as mensagens e arquivos transitados, aplicando regras definidas por meio de políticas de segurança de modo a evitar que, seja de forma intencional ou por um equívoco de algum servidor ou colaborador, ocorra perda de dados ou o envio de dados sensíveis ou a revelação de informações que possam comprometer a imagem institucional.

2.1.23 Por meio da implementação deste tipo de ferramenta de segurança da informação, caso seja identificado algum conteúdo que não deve ser transitado, a ferramenta pode alertar o usuário que este conteúdo é sensível ou mesmo bloquear o trâmite, baseado em filtros de conteúdo que demandam uma configuração detalhada, tais ações podem ser implementadas por meio de ferramentas DLP e CASB, onde:

- a) o CASB é uma solução de segurança cibernética que atua como intermediária entre uma organização e seus serviços de nuvem, como SaaS (Software as a Service), PaaS (Platform as a Service) e IaaS (Infrastructure as a Service), no caso do Ministério da Cultura há o uso de repositórios em nuvem pelos servidores e colaboradores, quando da realização de reuniões virtuais, armazenamento de dados na plataforma Teams, OnDrive, Onnote, e no

sharepoint, neste sentido o CASB trata-se de um serviço projetado para proteger os dados e aplicar políticas de segurança em ambientes de nuvem, oferecendo visibilidade, controle e segurança sobre o acesso aos recursos na nuvem.

a.1) Como o Minc utiliza armazenamento em nuvem para compartilhar documentos reuniões virtuais gravadas e etc. com o uso de um CASB poderá ser implementado o monitoramento e o controle ao acesso a esses documentos, podendo detectar atividades suspeitas, como tentativa de compartilhamento não autorizado ou download massivo de dados. Além disso, o CASB pode aplicar políticas de criptografia, autenticação multifatorial e restrições de acesso para garantir a segurança dos dados na nuvem.

a) o DLP é uma estratégia e conjunto de tecnologias projetadas para proteger os dados voluntários de uma organização, evitando sua divulgação não autorizada ou perda acidental. Isso é feito monitorando, identificando e controlando o movimento de dados dentro e fora da organização, aplicando políticas de segurança para prevenir vazamentos de dados.

a.1) Considerando que o Ministério lida com informações sensíveis dos usuários, servidores, colaboradores, e de cidadãos, tais como: números de contato e dados pessoais, com a implementação de uma solução DLP, o DLP poderá monitorar o tráfego de saída da rede em busca de informações temporárias e bloquear qualquer tentativa de envio desses dados por e-mail não autorizado ou transferência para dispositivos de armazenamento externos. Ele também pode impedir o uso não autorizado de dispositivos USB na rede corporativa para evitar vazamentos de dados. E assim, se alguém tentar enviar informações acidentalmente ou intencionalmente, o DLP aplicará políticas de bloqueio ou notificação, protegendo os dados pessoais ou institucionais que estiverem sendo acessados.

2.1.24 Portanto, ambas as soluções, CASB e DLP, podem desempenhar papéis cruciais na proteção dos dados do Minc, mas em contextos diferentes. O CASB concentra-se na segurança em ambientes de nuvem, enquanto o DLP se concentra em proteger os dados, independentemente de onde estão armazenados ou como são usados. Em muitos casos, as organizações implementaram ambas as soluções para obter uma abordagem abrangente de segurança de dados.

2.1.25 A implementação conjunta do CASB e do DLP é recomendada quando a organização deseja garantir a segurança de dados de forma abrangente, especialmente em ambientes de nuvem, e quando precisa cumprir regulamentações de proteção de dados ou proteger informações altamente provisórias. Essas soluções funcionam em conjunto para proteger dados em toda a organização, independentemente de sua localização ou forma de uso.

2.1.26 Neste contexto considerando que o Ministério da Cultura está sujeito a regulamentações específicas que tratam de proteção de dados, como a Lei de Proteção de Dados Pessoais (LGPD) no Brasil, a implementação conjunta do CASB e do DLP ajuda a cumprir os requisitos de conformidade, a integração do CASB com o DLP permite ainda, em atendimento as recomendações dos órgãos de controle, o monitoramento contínuo de atividades em nuvem e a capacidade de responder rapidamente a incidentes de segurança, como tentativa de vazamento de dados.

2.1.27 Destaque-se, ainda, o Decreto nº 10.222, de 5 de fevereiro de 2020, do Governo Federal, que aprova a Estratégia Nacional de Segurança Cibernética. Entre requisitos e controles definidos no documento, a seção 1.3, “Proteção Estratégica”, define uma proteção para infraestruturas críticas, no qual o Ministério da Cultura se insere, o que envolve institucionalizar processos, procedimentos e soluções de prevenção a vazamentos de informações pessoais ou institucionais.

2.1.28 O mesmo Decreto nº 10.222 cita o Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação e dispõe sobre princípios, objetivos, instrumentos, atribuições e competências de segurança da informação para os órgãos e entidades da Administração Pública Federal, sob o prisma da governança. Nessa temática, destaca-se que o Decreto nº 9.637 pontua a relevância da segurança de informações sigilosas e a proteção contra vazamento de dados.

2.1.29 Desta forma, este estudo visa a proteção do ambiente do Ministério da Cultura, por meio de ferramenta de DLP e CASB de modo a possibilitar, dentre outros recursos, proteção e autenticidade dos dados, maximizando a proteção contra ameaças da web. Ainda, a solução é parte de um conjunto essencial de funcionalidades necessárias para a gestão efetiva dos ativos de negócios deste Ministério.

2.1.30 Considerando os apontamentos supracitados, verifica-se que a aquisição da solução de DLP e CASB é necessária para que o Ministério da Cultura possa cumprir a sua missão, atendendo com qualidade e segurança às expectativas dos usuários dos seus serviços, além de se tratar de providência relevante em atendimento a implantação de processos e recursos de segurança da informação no âmbito desta pasta, conforme recomendação dos órgãos de controle.

2.1.31 O uso de tais ferramenta é justificável ainda no âmbito do apoio ao Programa de Privacidade e Segurança da Informação, com a possibilidade de auditar, monitorar e implantar controles automatizados. Ou seja, uma ferramenta para apoiar o programa, conforme preconiza a norma internacional ISO/IEC 16167:2013 que dispõe sobre as diretrizes para classificação, rotulação e tratamento da informação.

2.1.32 Por fim, esta iniciativa visa atender a diretriz contida na Política de Segurança da Informação e Cibernética no que diz respeito ao gerenciamento e resposta a incidentes de segurança. A referidas diretrizes definem que o Ministério da Cultura deverá adotar solução tecnológica para prevenção de vazamento de informações, visando garantir a rastreabilidade das informações e evitar que elas sejam perdidas, acessadas por pessoas não autorizadas, roubadas, mal utilizadas ou vazadas por usuários mal-intencionados.

3. Área requisitante

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

4. Necessidades de Negócio

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

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

4.2. Prevenir a perda de dados por meio de adoção de uma estratégia de monitoramento e observância às diretivas constantes na Lei Geral de Proteção de Dados, LGPD, de 21 de Agosto de 2020, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

4.3. A iniciativa em questão está em conformidade e encontra-se alinhada ao Plano Diretor de Tecnologia da Informação – PDTIC do Ministério da Cultura, bem como ao Planejamento Institucional 2021 – 2023.

4.3.1. A presente aquisição também guarda alinhamento à Estratégia de Governo Digital (EGD) para o período de 2020 a 2022, instituída pelo Decreto nº 10.332, de 28 de abril de 2020, prorrogada até 2023 pelo Decreto nº 11.260, de 22 de novembro de 2022, no tocante ao Objetivo Estratégico OE 16 "Otimização das infraestruturas de tecnologia da informação". Para alcance desse objetivo estratégico, a EGD enuncia como iniciativa (Iniciativa nº 16.1) a realização de, no mínimo, seis compras centralizadas de bens e serviços comuns de TIC.

5. Necessidades Tecnológicas

1. 5.1 A fim de manter a segurança do ambiente computacional do Ministério da Cultura, é imprescindível que tenhamos uma solução de prevenção de perda de dados. A lista abaixo possui um resumo das necessidades tecnológicas que o Ministério pretende adquirir:

- a) Fornecer informações de onde os dados estão armazenados na nuvem, em dispositivos móveis e em ambientes locais do Ministério;
- b) Monitorar como os dados estão sendo usados quando os funcionários estiverem conectados ou não à rede;
- c) Proteger os dados contra vazamento ou roubo, independentemente de onde estiverem armazenados ou como estiverem sendo usados;
- d) Fazer a integração na proteção de correio eletrônico, DLP e criptografia;
- e) Promover a proteção necessária ao uso de uma nuvem privativa ou de terceiros. ex. armazenamento externo ao domínio do Ministério da Cultura;
- f) Controle via endpoint: através de um agente instalado, se torna possível monitorar todos os possíveis canais de fuga de informação de uma estação de trabalho ou servidor, abrangendo desde um upload para qualquer destino http, https ou ftp até uma simples impressão de documento ou cópia para dispositivo usb;
- g) Implementação de monitoramento de rede: através deste canal de monitoramento se torna possível, através da escuta de tráfego, a detecção de fuga da informação em praticamente qualquer protocolo de rede;
- h) Implementação de proteção web: este canal de monitoramento se integra com dispositivos de filtragem de internet (proxies e alguns firewalls) visando monitorar toda a saída de internet da organização (sem agente), na ótica de vazamento de dados sensíveis, impedindo que estes dados sejam trafegados para destinos não permitidos;
- i) Monitoramento de e-mail: este canal de monitoramento deve se integrar diretamente com serviços de mensageria do outlook. através desta integração se torna possível o monitoramento de toda saída de dados via e-mail, sem agente instalado, sempre tentando impedir o vazamento de dados;
- j) Apoio a descoberta de rede: este canal de monitoramento está diretamente ligado a descoberta de onde os dados sensíveis residem. seja em servidores de arquivos, OneDrive, SharePoint, box ou até mesmo nas estações dos próprios usuários. através desta ótica, torna se possível manter informações sensíveis armazenadas sempre da melhor forma possível
- k) Monitoramento em nuvem, este canal de monitoramento deve se integrar com serviços de nuvem como casb – cloud access security broker e Microsoft 365 para monitoramento de todo tráfego de e-mail que passa por este canal
- l) Implementar um módulo casb – cloud access security broker, permitindo que todos os controles de DLP existentes atualmente sejam ampliados para aplicações de nuvem.

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

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

- a) A solução deverá ser compatível com as demandas previstas no PCA do MinC com vistas a facilitar e viabilizar a execução no Sistema PGC para o exercício de 2023;
- b) Observar aspectos de compatibilidade com o datacenter do Minc;

6.2. Requisitos de Garantia e Assistência Técnica

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.3. Requisitos da Capacitação

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

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

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

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

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

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

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

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

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

6.4. Requisitos Legais

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

- a. 1. Lei 14.133, de 01 de abril de 2021.
- b. 2. Lei nº 10.520, de 17 de julho de 2002, que institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências;
- c. 3. Decreto nº 10.024, de 20 de setembro de 2019, que regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências;
- d. 4. Lei Complementar nº 123, de 14 de dezembro de 2006, que institui o Estatuto Nacional da microempresa e da Empresa de Pequeno Porte.
- e. 5. Instrução Normativa nº 05 do MPOG, de 26 de maio de 2017, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.
- f. 6. Instrução Normativa SGD/ME nº 94, DE 23 DE DEZEMBRO DE 2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.
- g. 7. Instrução Normativa SEGES /ME nº 73, de 30 de setembro de 2022, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

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

6.5. Requisitos de Manutenção e Garantia

6.5.1. A garantia de funcionamento das licenças adquiridas, bem como o suporte técnico serão pelo período de 36 (trinta e seis) meses.

6.5.2. O serviço de assistência técnica em GARANTIA deverá cobrir todos os procedimentos técnicos destinados ao reparo de eventuais falhas apresentadas nos equipamentos, de modo a restabelecer seu normal estado de uso e dentre os quais se incluem a substituição de peças, ajustes e reparos técnicos em conformidade com manuais e normas técnicas especificadas pelo fabricante.

6.5.3. Para efeitos de certificar a garantia, a CONTRATADA deve possuir recurso disponibilizado via web, site do próprio fabricante, que permita verificar a garantia do equipamento através da inserção do seu número de série.

6.5.4. Durante o prazo de garantia será substituída sem ônus para o CONTRATANTE, a parte ou peça defeituosa, após a conclusão do respectivo analista de atendimento de que há a necessidade de substituir uma peça ou recolocá-la no sistema.

6.5.5. A substituição de componentes ou peças decorrentes da garantia não gera quaisquer ônus para o CONTRATANTE. Toda e qualquer peça ou componente consertado ou substituído, fica automaticamente garantido até o final do prazo de garantia técnica do contrato.

6.5.6. As peças substitutas deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento e devem integrar a garantia da solução.

6.5.7. Os serviços de suporte técnico abrangem:

- I. 1. Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;
- II. 2. Elaboração de relatórios, estudos e diagnósticos sobre o ambiente;
- III. 3. Transferência de conhecimento aos técnicos da CONTRATANTE referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes; e
- IV. 4. Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante.

6.5.8. O suporte técnico contempla o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software ou para correção de problemas, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução.

6.5.9. O suporte técnico deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TIC (sistemas operacionais, servidores de banco de dados, servidores de aplicação, etc.) necessários ao funcionamento da solução.

6.5.10. Deve contemplar também a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período. A cada nova liberação de versão e release, será disponibilizada em formato digital manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas. Em caso de lançamento de *patch* de correção, a CONTRATADA deverá comunicar o fato ao CONTRATANTE e indicar a forma de obtenção e os defeitos que serão corrigidos pelo *patch*. Em ambos os casos, a comunicação deve ser feita no prazo de até 30 (trinta) dias, a contar do lançamento de nova versão ou solução de correção.

6.5.11. A CONTRATADA será responsável pelos serviços de implantação das novas versões e releases dos produtos por ela fornecidos como partes do objeto, bem como pela aplicação dos patches de correção e pacotes de serviço (service packs) relativos a esses produtos. Para a implantação das novas versões/releases, bem como para a aplicação dos patches, deverá ser aberto chamado de suporte técnico com nível de severidade adequado e a prestação dos serviços deve ser agendada com os responsáveis pela solução na CONTRATANTE.

6.5.12. Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela CONTRATADA e/ou pelo fabricante; e também através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução CONTRATADA.

6.5.13. A CONTRATADA auxiliará o CONTRATANTE na reinstalação das ferramentas, caso seja necessário, ao longo do tempo de garantia da ferramenta.

6.5.14. A CONTRATADA deverá disponibilizar os seguintes canais de acesso ao suporte técnico:

- I. 1. Portal Web, E-mail, Central 0800 e/ou telefone fixo;
- II. 2. O atendimento deve ser 24x7x365, ou seja, 24 (vinte e quatro) horas por dia em 7 (sete) dias da semana por 365 (trezentos e sessenta e cinco) dias por ano, em língua portuguesa.
- III. 3. O recebimento dos equipamentos/serviços será efetivado pela equipe designada pelo CONTRATANTE, e dar-se-á da forma provisória e definitiva. A forma provisória será no ato da entrega dos equipamentos/serviços e a forma definitiva será após a instalação, configuração e teste da solução.

6.6. Requisitos Temporais

6.6.1. O prazo de início de atendimento para os chamados de suporte técnico e manutenção pela garantia deverá estar de acordo com o especificado no acordo de nível de serviço do Termo de Referência.

6.6.2. O prazo de entrega e instalação deverá estar de acordo com o especificado no Termo de Referência, caso não seja especificado um prazo diferente na ordem de serviço.

6.6.3. Os equipamentos e as licenças de softwares devem ser entregues em Brasília, no endereço descrito na tabela abaixo:

UF	ENDEREÇO
----	----------

DF	Esplanada dos Ministérios Bloco B - Zona Cívico-Administrativa, Brasília - DF, 70068-900
-----------	--

6.6.4. A entrega dos equipamentos deverá acontecer no horário compreendido entre as 09:00 as 17:00 e poderá ser agendada em data e hora previamente com a CONTRATANTE;

6.6.5. Caberá ao CONTRATANTE rejeitar no total ou em parte, os materiais entregues em desacordo com o objeto do Termo de Referência.

6.6.6. O recebimento dos equipamentos será efetivado pela equipe designada pelo CONTRATANTE, e dar-se-á da forma provisória e definitiva. A forma provisória será no ato da entrega dos equipamentos e a forma definitiva será após a instalação, configuração e teste da solução.

6.7. Requisitos de Segurança

6.7.1. A empresa CONTRATADA para prestação dos serviços deverá observar os seguintes requisitos quanto à Segurança da Informação e Comunicações:

6.7.2. Deverão ser observados os regulamentos, normas e instruções de segurança da informação e comunicações adotadas pelo Ministério da Cultura, incluindo, mas não se limitando, ao definido na Política de Segurança da Informação e suas Normas Complementares, durante a execução dos serviços nas instalações do Ministério;

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

6.7.4. Toda informação confidencial gerada e/ou manipulada em razão desta contratação, seja ela armazenada em meio físico, magnético ou eletrônico, deverá ser devolvida nas seguintes hipóteses, mediante formalização entre as partes:

- a. 1. Término ou rompimento do Contrato; ou
- b. 2. Solicitação do Ministério da Cultura.

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

6.7.6. Quando solicitado formalmente pelo Ministério da Cultura, deverão ser realizadas, prioritária e concomitantemente, alterações para sanar possíveis problemas de segurança ou de vulnerabilidade nos referidos sistemas ou softwares utilizados para execução do serviço contratado;

6.7.7. A CONTRATADA deverá informar ao Ministério da Cultura, formalmente e tempestivamente, sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados;

6.7.8. Prestar os esclarecimentos necessários ao Ministério da Cultura, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução;

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

6.7.10. A empresa CONTRATADA não poderá divulgar, mesmo que em caráter estatístico, quaisquer informações originadas no Ministério da Cultura, sem prévia autorização;

6.7.11. O acesso às instalações da CONTRATADA onde serão realizados os serviços deverá ser controlado e permitido somente às pessoas autorizadas;

6.7.12. A CONTRATADA deverá manter os seus profissionais identificados por crachás, quando em trabalho, devendo substituir imediatamente aquele que seja considerado inconveniente à boa ordem ou que venha a transgredir as normas disciplinares do Ministério;

6.7.13. A CONTRATADA deverá manter os seus profissionais informados quanto às normas disciplinares do Ministério, exigindo sua fiel observância, especialmente quanto à utilização e segurança das instalações;

6.7.14. Deverá ser celebrado TERMO DE COMPROMISSO entre a CONTRATADA e o Ministério da Cultura para garantir a segurança das informações do Ministério, assim como, celebrado o TERMO DE CIÊNCIA a todos envolvidos na prestação dos serviços;

6.7.15. Não transferir a terceiros os serviços contratados;

6.7.16. Manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados, documentos elaborados e informações obtidas dentro do Ministério da Cultura.

6.8. Requisitos Sociais, Ambientais e Culturais

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

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

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

6.9. Requisitos de Pagamento

6.9.1. As Ordens de Serviço somente serão validadas e liberadas para pagamento quando as condições a seguir forem satisfeitas:

1. As licenças forem entregues e instaladas pela CONTRATADA atendendo às especificações contidas no Termo de Referência;
2. O fornecedor emitir certificado de garantia de 36 (trinta e seis) meses para as licenças entregues;
3. A qualidade do serviço tiver sido avaliada e aceita pela CONTRATANTE.

6.9.2. O pagamento deverá ser efetuado mediante a apresentação de Nota Fiscal ou Fatura pela CONTRATADA, que deverá conter as informações necessárias à conferência do objeto fornecido, incluindo o prazo de validade, a data da emissão, os dados do contrato e do órgão contratante, o período de prestação dos serviços, o valor a pagar e eventual destaque do valor de retenções tributárias cabíveis.

6.9.3. O objeto será recebido provisoriamente, pelo responsável pelo seu acompanhamento e fiscalização para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência, no prazo de até 05 (cinco) dias úteis.

6.9.4. Em até 15 (quinze) dias corridos após a emissão do Termo de Recebimento Provisório, salvo a inexistência de pendências a serem sanadas, sendo confirmada sua operação e desempenho a contento, nos termos do Termo de Referência, a CONTRATANTE emitirá o Termo de Recebimento Definitivo;

6.9.5. Antes do pagamento, a CONTRATANTE verificará a regularidade fiscal da CONTRATADA através de consulta “on-line” ao Sistema de Cadastramento Unificado de Fornecedores - SICAF, ou na impossibilidade de acesso ao referido sistema, mediante consulta aos sítios oficiais.

6.9.6. À CONTRATANTE fica reservado o direito de retenção ou glosa no pagamento, sem prejuízo das sanções cabíveis quando a CONTRATADA:

1. Não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou
2. Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade inferior à demandada.

6.10. Requisitos de Aceitação do Objeto

6.10.1. A aceitação do objeto ocorrerá apenas se a empresa vencedora apresentar todos os critérios de habilitação;

6.10.2. A descrição do objeto na Nota Fiscal deverá ser idêntica à descrição do edital e da Nota de Empenho, caso contrário o serviço executado deverá ser recusado para correção da documentação por parte da contratada.

6.11. Requisitos de Instalação

6.11.1. A CONTRATADA deverá instalar a solução ofertada nas instalações da CONTRATANTE;

6.11.2. A empresa que realizar a implantação deverá ter técnicos treinados em toda a solução ofertada;

6.11.3. Os serviços que eventualmente acarretem risco para os sistemas em produção ou requeiram parada de servidores, equipamentos e rede elétrica, somente poderão ser executados fora de expediente, em horários previamente acordados com a área de TI do local de instalação.

6.12. Requisitos de Experiência Profissional

6.12.1. A licitante deverá apresentar declaração, datada e assinada por seu representante legal, de que, caso se sagre vencedora do certame, no momento da assinatura do contrato, disporá de profissionais com nível superior e com as seguintes certificações ou equivalentes:

No mínimo 02 (dois) profissionais capacitados e certificados pela fabricante envolvendo os produtos de hardware e software da solução.

6.12.1. A comprovação de que os profissionais compõem o quadro permanente da licitante se fará mediante a apresentação de cópia da Carteira de Trabalho (CTPS) ou do contrato social da licitante, no caso de sócio, ou contrato de prestação de serviços pelo prazo de vigência do contrato.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. O quantitativo estimado para a aquisição desta solução de prevenção contra vazamento de dados para usuários está baseado no número de usuários e seguiu a seguinte métrica:

- 784 usuários ativos
- 267 novos postos de trabalho a serem contratados (conforme Termo de Referência DOC SEI nº 1425900)
- 50 novos postos para concurso já autorizado
- Margem adicional de 10% para eventuais novas necessidades

7.2. Este número foi obtido por meio da ferramenta Microsoft System Center, que é uma ferramenta utilizada para gerenciar computadores. Os itens que compõem a solução estão baseados em estudos realizados com base na solução mais completa disponível, conforme tabela abaixo:

LOTE	ITEM	DESCRIÇÃO	MÉTRICA	QUANTIDADE
1	1	Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention - DLP.	Unidade	1.200
	2	Repasse de Conhecimento	Turma	1
	3	Configuração e Instalação	Unidade	1
2	4	Aquisição de licenças de software de solução de descoberta e classificação de dados, controle de acesso, monitoramento de atividade, auditoria e proteção através de bloqueio, criptografia e quarentena, para aplicações e ambientes de armazenamento em nuvem - CASB - Cloud Access Security Broker.	Unidade	1.200

5	Repasse de Conhecimento	Turma	1
6	Configuração e Instalação	Unidade	1

8. Levantamento de soluções

8.1 Identificação das Soluções

8.1.1 Os estudos elaborados pela Equipe de Planejamento da Contratação visam identificar, analisar e elencar as alternativas de atendimento à demanda considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

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

- **Solução 1:** Adoção da Solução baseada em Software Livre.
- **Solução 2:** Aquisição de solução de prevenção de perda de dados (*Data Loss Prevention - DLP*).
- **Solução 3:** Aquisição de solução de descoberta e classificação de dados, controle de acesso, monitoramento de atividade, auditoria e proteção através de bloqueio, criptografia e quarentena, para aplicações e ambientes de armazenamento em nuvem conhecida no mercado como CASB (*Cloud Access Security Broker*).
- **Solução 4:** Aquisição combinada de DLP e CASB.

9. Análise comparativa de soluções

9.1. A análise comparativa de soluções consiste na identificação e comparação dos diferentes aspectos qualitativos inerentes a vantajosidade de cada solução considerando os seguintes conceitos: "mais vantajosa", "alguma vantagem" e "menos vantajosa".

Aspecto da Solução	Solução 1 Software Livre	Solução 2 DLP	Solução 3 CASB	Solução 4 DLP e CASB
Complexidade da Gestão da Solução	Alta: Soluções Open Source são complexas pelo fato de não haver nenhum suporte técnico e dificuldade em gerenciar uma única solução com produtos de fabricantes diferentes	Média: A adaptabilidade da solução aos sistemas legados do MinC e dificuldade em gerenciar uma única solução com produtos de fabricantes diferentes	Média: A adaptabilidade da solução aos sistemas legados do MinC e dificuldade em gerenciar uma única solução com produtos de fabricantes diferentes	Média: A adaptabilidade da solução aos sistemas legados do MinC e dificuldade em gerenciar uma única solução com produtos de fabricantes diferentes
Valor da Contratação	Baixo: Soluções OpenSource não tem custos de contratação	Médio: Abertura de concorrência em soluções pode oferecer valor menor ou igual ao valor atual	Médio: Abertura de concorrência em soluções pode oferecer valor menor ou igual ao valor atual	Médio: Abertura de concorrência em soluções pode oferecer valor menor ou igual ao valor atual
	Alta: Maior necessidade de customização devido a natureza do software ser	Baixa: Sem a necessidade de customização devido a	Baixa: Sem a necessidade de customização devido a	Baixa: Sem a necessidade de customização devido a

Necessidade de Customização	de uso geral. Sem contar a necessidade de adaptar soluções na busca de alcançar aderência	produtos de fabricantes diferentes e compatibilidade com sistemas legados	produtos de fabricantes diferentes e compatibilidade com sistemas legados	produtos de fabricantes diferentes e compatibilidade com sistemas legados
Integrabilidade	Baixa: Devido a ausência de soluções que subsidiem o alcance dos objetivos	Alta: As soluções pesquisadas nesse ETP possuem integração total ou parcial entre os produtos exigidos nos requisitos técnicos.	Alta: As soluções pesquisadas nesse ETP possuem integração total ou parcial entre os produtos exigidos nos requisitos técnicos.	Alta: As soluções pesquisadas nesse ETP possuem integração total ou parcial entre os produtos exigidos nos requisitos técnicos.
Grau de Dependência Tecnológica	Baixa: Soluções Open Source são fáceis de serem substituídas tanto por Open Source quanto Softwares proprietário, muitas delas são construídas baseadas em outras soluções de mercado.	Média: A Solução pode oferecer dependência de outras soluções para funcionar de forma integrada	Média: A Solução pode oferecer dependência de outras soluções para funcionar de forma integrada.	Média: A Solução pode oferecer dependência de outras soluções para funcionar de forma integrada.
Necessidade de Revisão dos processos de trabalho para utilização mais eficientes da solução	Alta: A falta de Integrabilidade das soluções Open Source influencia na necessidade de revisão dos processos de trabalho. Esta solução precisa que ferramentas sejam inseridas em processos para os quais não foram inicialmente concebidas.	Baixo: O nível de Integrabilidade das novas soluções influencia na necessidade de revisão dos processos de trabalho	Baixo: O nível de Integrabilidade das novas soluções influencia na necessidade de revisão dos processos de trabalho	
Maturidade do mercado no fornecimento da solução	Desconhecido: O modelo de utilização de Open Source tem crescido em ambientes governamentais. Contudo para DLP e CASB não cobre os objetivos esperados.	Consolidada: As soluções são estáveis e tem amplo fornecimento no mercado	Consolidada: As soluções são estáveis e tem amplo fornecimento no mercado	Consolidada: As soluções são estáveis e tem amplo fornecimento no mercado. Sem contar que a combinação amplia o espectro de atuação.
Necessidade de Capacitação	Alta: Existe uma grande necessidade de capacitação principalmente se houver necessidade de customização do código.	Baixo: É necessário capacitar equipes, entretanto alguns produtos oferecem suporte a capacitação	Baixo: É necessário capacitar equipes, entretanto alguns produtos oferecem suporte a capacitação	

9.2 SOLUÇÃO 1 - Implantar Software Livre

9.2.1 A primeira solução a ser avaliada consiste na adoção de software livre. Por “software livre” devemos entender aquele software que respeita a liberdade e senso de comunidade dos usuários, à grosso modo, isso significa que os usuários possuem a liberdade de executar, copiar, distribuir, estudar, mudar e melhorar o software.

9.2.2 Ao mesmo tempo que tal fato pode ser encarado de forma positiva, há que se levar em consideração que este cenário pode resultar numa grande fragilidade de segurança, se não for aplicado padrões de projeto de software as customizações são feitas sem levar em consideração aspectos importantes de padronização, segurança, escalabilidade e consistência.

9.2.3 Outro ponto muito importante na adoção de software livre é que estes não possuem suporte ou garantia. Não há empresa ou entidade que responda comercial, civil ou juridicamente pela solução.

9.2.4 O software livre pode ser uma opção econômica e flexível, mas pode não atender a todas as necessidades de segurança avançada ou oferecer o mesmo nível de suporte disponível em soluções comerciais.

9.2.5 Embora essas ferramentas de código aberto possam ser úteis em um contexto de segurança em nuvem, elas não oferecem todas as funcionalidades abrangentes de um CASB comercial

9.2.6 Da existência de Software Público Brasileiro

9.2.7 De acordo com a busca realizada no dia 22/06/2023, com as palavras chaves "data loss prevention", o portal: softwarepublico.gov.br, retornou que não havia encontrado nenhum software correspondente.

CATÁLOGO DE SOFTWARE PÚBLICO

Resultado da pesquisa

PESQUISAR CATÁLOGO DE SOFTWARE

☐ Todos ☒ Software Público

Data Loss Prevention

FILTRO

MAIS OPÇÕES

0 Software(s)

Exibir: 15

Ordenar por: Avaliação

PESQUISAR CATÁLOGO DE SOFTWARE

☐ Todos ☒ Software Público

casb

FILTRO

MAIS OPÇÕES

0 Software(s)

Exibir: 15

Ordenar por: Avaliação

9.2.8 De mesmo modo, foi consultado no portal da Administração Pública, onde o órgão central do SISP estabeleceu o Catálogos de Soluções de TIC com Condições Padronizadas, disponíveis em: <https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic>

Catálogos de Soluções de TIC

Os Catálogos de Soluções de TIC com Condições Padronizadas são instrumentos previstos nos processos de contratação de Soluções de TIC.

Publicado em 02/12/2019 08h48

Atualizado em 07/07/2023 14h39

Compartilhe: f t

9.2.9 Pelas razões supracitadas, a equipe de planejamento da contratação não encontrou elementos objetivos que justifiquem a utilização desse cenário/solução.

9.3 SOLUÇÃO 2 - Implementação de solução de Prevenção de Perda de Dados (DLP).

9.3.1 Soluções do tipo DLP, tratam-se de um conjunto de tecnologias que visa proteger dados sensíveis contra vazamentos não autorizados ou divulgações inadvertidas, sendo projetada para identificar, monitorar e controlar o tráfego de dados, dentro da rede interna, com o objetivo de prevenir a perda de informações críticas.

9.3.2 A implementação de uma solução de Prevenção contra Vazamento de Dados (DLP) no Ministério da Cultura pode representar um salto em relação aos mecanismos de segurança da informação, um vez que contribuirá com a proteção de dados sensíveis e agregaria conformidade com regulamentações tais como a LGPD.

9.3.1 A implementação de solução de DLP traz os seguintes benefícios:

- a) **Identificação de Dados Sensíveis** - capacidade de identificar dados sensíveis com base em políticas predefinidas, como números de cartões de crédito, informações de identificação pessoal (PII), informações financeiras, propriedade intelectual, entre outros.
- b) **Monitoramento de Atividades** - capacidade de monitorar continuamente as atividades relacionadas aos dados sensíveis, incluindo transferências de arquivos, comunicações por e-mail, uploads para a nuvem e outras interações com os dados.
- c) **Controles de acesso** - Implementação de controles de acesso granulares para garantir que apenas usuários autorizados tenham permissão para acessar, modificar ou transferir dados confidenciais.
- d) **Prevenção contra Vazamentos** - Prevenção contra vazamentos de dados por meio de ações como bloqueio de transferências de arquivos, criptografia ou alertas em tempo real quando atividades suspeitas são bloqueadas.
- e) **Integração com Políticas de Segurança** - Utilizando-se das regras definidas na política de segurança do ministério será possível aplicar medidas de prevenção contra vazamentos de forma alinhada com os requisitos internos e regulamentações externas vinculadas a POSIC do MINC.
- f) **Relatórios e Auditoria** - fornecimento de recursos de geração de relatórios e auditorias para documentar atividades relacionadas à prevenção contra vazamento de dados, facilitando a análise e o cumprimento de requisitos regulatórios.

9.3.2 Uma solução de DLP é eficaz para proteger dados internos, porém não oferece a mesma proteção e controle abrangentes sobre dados e atividades em serviços de nuvem.

9.4 SOLUÇÃO 3 - Contratação de solução Cloud Access Security Broker (CASB).

9.4.1 Projetada para monitorar e controlar o acesso a dados e aplicativos na nuvem, esse tipo de solução oferece uma camada de segurança entre os usuários e os serviços de nuvem, possibilitando ao Ministério da Cultura a capacidade de proteger os dados armazenados em repositórios disponibilizados em nuvem, garantindo assim a conformidade com as políticas de segurança definidas pela Pasta.

9.4.2 Desta forma por meio da implementação de uma solução CASB será possível aos gestores do do Minc a visibilidade e controle sobre as atividades dos usuários na nuvem, independentemente de onde esses usuários estão localizados ou de qual dispositivo estão utilizando. Algumas das características típicas de uma solução CASB incluem:

- a) **Monitoramento de Atividades na Nuvem** - A capacidade de monitorar e registrar atividades de usuários em serviços de nuvem, identificando comportamentos suspeitos ou não autorizados;
- b) **Controle de Acesso** - Implementação de políticas de acesso que definem quem pode acessar quais dados e aplicativos na nuvem. Isso ajuda a garantir que apenas usuários autorizados tenham acesso a informações adicionais;
- c) **Proteção de Dados** - Mecanismos para proteger dados protegidos contra vazamentos, seja por meio de criptografia, prevenção contra perda de dados (DLP) ou outras tecnologias de proteção.

d) Identificação e Autenticação - Verificação da identidade dos usuários que acessam serviços na nuvem, com autenticação multifatorial e outros métodos de segurança.

e) Detecção de Ameaças - Identificação de atividades suspeitas ou ameaças na nuvem, permitindo uma resposta rápida a possíveis incidentes de segurança.

f) Integração com Serviços na Nuvem - Integração com os principais serviços em nuvem utilizados pela organização, como plataformas de armazenamento, colaboração e aplicativos empresariais.

9.4.3 Ao implementar uma solução CASB, haverá ganhos para o ministério com a ampliação da postura de segurança para a nuvem, mitigando riscos associados ao uso cada vez maior de serviços baseados em nuvem e garantindo que as políticas de segurança se estendam de forma consistente, independentemente da localização dos dados e usuários.

9.4.4 Uma solução de CASB é eficaz para proteger dados na nuvem, porém não oferece a mesma proteção e controle abrangentes sobre dados e atividades em serviços *on premise*.

9.5 SOLUÇÃO 4 - Implementação da combinação de soluções DLP e CASB

9.5.1 A solução 4 consiste na contratação de solução de mercado compreendendo a contratação de empresa especializada no fornecimento de licenças de software de solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP) e CASB (Cloud Access Security Broker), incluindo implantação da solução, treinamento, manutenção especializada e suporte técnico pelo período de 36 (trinta e seis) meses.

9.5.2 A implementação conjunta de uma solução DLP (Prevenção contra Vazamento de Dados) e uma solução CASB (Cloud Access Security Broker) possibilita uma abordagem holística para a segurança da informação, considerando que o Ministério da Cultura, embora possua datacenter próprio, a Pasta vem fazendo o uso extensivo de serviços em nuvem, com o office 365, sharepoint, On Drive entre outros recursos presentes em ambientes em nuvem.

9.5.3 Desta forma, enquanto a solução DLP oferece proteção contra vazamento de dados em diferentes canais, como e-mail, transferências de arquivos e dispositivos removíveis. Por outro lado, o CASB se concentra na segurança dos dados em ambientes de nuvem. Juntas, essas soluções poderão realizar uma cobertura abrangente, protegendo dados em diferentes contextos e canais de comunicação.

9.5.4 Considerando o ambiente híbrido da infraestrutura de TI do Ministério, que combina infraestrutura local e serviços em nuvem. A implementação conjunta permite uma abordagem coesa para prevenção de vazamento de dados em toda a infraestrutura, garantindo que os dados sensíveis estejam protegidos, independentemente de sua localização.

9.5.5 Ao integrar as soluções DLP e CASB, será possível obter visibilidade total sobre as atividades de dados, desde a criação e transferência até o armazenamento em serviços em nuvem. Isso facilita a identificação de padrões suspeitos e a resposta rápida a incidentes de segurança.

9.5.6 A implementação conjunta permitirá também a gestão centralizada de políticas de segurança do Ministério da Cultura, simplificando a administração e garantindo consistência nas abordagens de segurança em todos os ambientes.

9.5.7 A combinação de DLP e CASB no âmbito do Ministério também serve para reforçar as defesas contra ameaças tanto internas quanto externas, abordando tanto vazamentos acidentais quanto ataques maliciosos.

9.5.8 Neste sentido, considerando que o universo de usuários, colaboradores e servidores, desta Pasta está distribuído em várias localidades, tais como: Escritórios Estaduais, CTAV -RJ e Biblioteca Demonstrativa de Brasília, e ainda considerando o crescente uso de serviços em nuvem, resta identificada a vulnerabilidade dos repositórios de dados pessoais tanto em ambientes da rede interna quanto em ambientes em nuvem,.

9.5.9 Assim, seja em sistemas ou repositórios de caixas de e-mail corporativas ou pastas de arquivos em nuvem podem ser utilizadas pelos diversos usuários desta Pasta, para o armazenamento de dados pessoais e sensíveis sem um controle efetivo do tratamento de tais informações, o que coloca em risco o controle do acesso e distribuições de tais dados, por não haver uma ferramenta do tipo DLP combinada com uma solução CASB.

9.6 Portanto, considerando os aspectos técnicos mencionados, a solução 4 se apresentou como um cenário viável mas compatível com as necessidades do Ministério da Cultura, uma vez que a implementação conjunta de soluções DLP e CASB oferece uma abordagem integrada e abrangente para a segurança da informação no âmbito da rede do Ministério da Cultura, proporcionando controle, visibilidade e proteção consistentes em ambientes locais e em nuvem.

9.7 Neste sentido a estratégia é especialmente valiosa em um cenário em constante evolução, onde os dados corporativos estão distribuídos em diversas plataformas e serviços como é o caso do Ministério da Cultura, conforme já relatado no levantamento das necessidades.

9.8 Considerando a análise realizada pela equipe de planejamento da contratação constante neste ETP verifica-se viáveis as soluções 02, 03 e 04 .

9.10 Dentre as soluções viáveis verifica-se que a solução 04 que trata-se da combinação da solução 02 e 03 é a que apresenta maior abrangência quanto a implementação de controles e quanto ao atendimento das necessidades do Ministério da Cultura, e portanto será abordada como a solução a ser estudada de forma a compor a solução de tecnologia a ser implementada no âmbito do Ministério.

9.2. A equipe também realizou a avaliação dos cenários quanto à disponibilidade de soluções na APF e quanto aos padrões de governo para TIC, conforme o disposto nas alíneas a, c e d, inciso II do artigo 11 da IN SGD/ME nº 1/2019, a saber:

Requisito	ID do cenário	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	SOLUÇÃO 01		X	
	SOLUÇÃO 02	X		
	SOLUÇÃO 03	X		
	SOLUÇÃO 04	X		
A Solução está disponível no Portal do Software Público Brasileiro?	SOLUÇÃO 01		X	
	SOLUÇÃO 02		X	
	SOLUÇÃO 03		X	
	SOLUÇÃO 04		X	
A Solução é um software livre ou software público?	SOLUÇÃO 01	X		
	SOLUÇÃO 02		X	
	SOLUÇÃO 03		X	
	SOLUÇÃO 04		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	SOLUÇÃO 01	X		
	SOLUÇÃO 02	X		
	SOLUÇÃO 03	X		
	SOLUÇÃO 04	X		
A Solução é aderente às regulamentações da ICPBrasil? (quando houver necessidade de certificação digital)	SOLUÇÃO 01			X
	SOLUÇÃO 02			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 03			X
	SOLUÇÃO 04			X
	SOLUÇÃO 01			X
	SOLUÇÃO 02			X
	SOLUÇÃO 03			X
	SOLUÇÃO 04			X

10. Registro de soluções consideradas inviáveis

10.1. A Solução 1 compreende o uso de solução baseada em software livre se mostra inviável. Devido à falta de expertise interna; suporte técnico especializado; complexidade e integração limitada; ausência de garantias; Necessidade de Conformidade com Regulamentos; Complexidade das Atividades em Nuvem e necessidade de composição com vários produtos para entrega aproximada da necessidade, fica evidente que esta solução não atenderia as necessidades do Ministério da Cultura.

Os desafios e riscos associados à implementação de soluções de DLP e CASB com software livre no MinC não se justifica diante das vantagens ofertadas por soluções comerciais que oferecem maior suporte, conformidade, confiabilidade e eficácia em ambientes complexos de segurança cibernética.

10.2. Soluções 2 e 3: Como informado no item 9, a aquisição em separado das soluções de CASB e DLP, não atenderia por completo às necessidades do MinC.

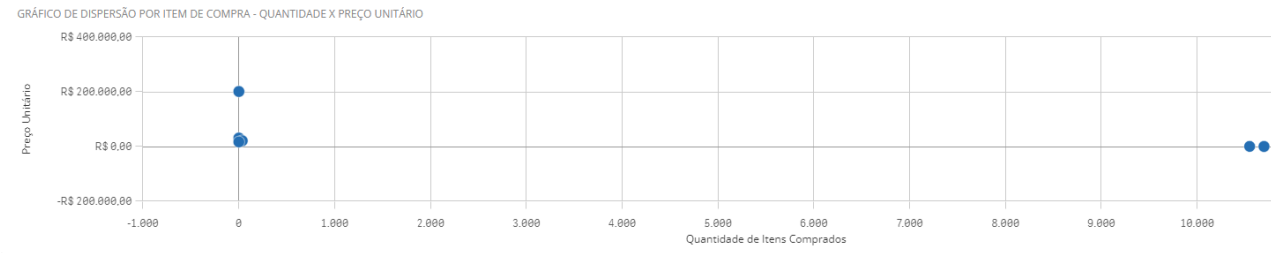
10.3. Adesão à Ata de Registro de Preços. Ao realizar pesquisa por Atas de Registros de preço disponíveis para adesão, não foi encontrada ata que dispusesse de solução que atenda aos objetivos buscados com as soluções elencadas neste documento.

11. Análise comparativa de custos (TCO)

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

11.1.1. Pregão Eletrônico 67/2022 - 179007 Banco da Amazônia S/A

Este pregão é o que apresenta itens mais similares à abordagem escolhida neste projeto.



Código do CATSER	Descrição do Item	Unidade de Fornecimento	Quantidade ofertada	Valor unitário	Fornecedor	Órgão	UASG
27022	OUTROS SERVICOS DE GERENCIAMENTO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMACAO E COMUNICACAO (TIC)	UND SERVIÇO TÉCNICO	10,698	R\$ 271,10	ISH TECNOLOGIA S/A	MINISTERIO DA FAZENDA	1790(AMAZ
27022	OUTROS SERVICOS DE GERENCIAMENTO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMACAO E COMUNICACAO (TIC)	UND SERVIÇO TÉCNICO	10,548	R\$ 594,22	ISH TECNOLOGIA S/A	MINISTERIO DA FAZENDA	1790(AMAZ
27022	OUTROS SERVICOS DE GERENCIAMENTO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMACAO E COMUNICACAO (TIC)	UND SERVIÇO TÉCNICO	1	R\$ 17,043,32	ISH TECNOLOGIA S/A	MINISTERIO DA FAZENDA	1790(AMAZ
27022	OUTROS SERVICOS DE GERENCIAMENTO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMACAO E COMUNICACAO (TIC)	UND SERVIÇO TÉCNICO	36	R\$ 21,133,33	ISH TECNOLOGIA S/A	MINISTERIO DA FAZENDA	1790(AMAZ
27022	OUTROS SERVICOS DE GERENCIAMENTO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMACAO E COMUNICACAO (TIC)	UND SERVIÇO TÉCNICO	1	R\$ 31,021,66	ISH TECNOLOGIA S/A	MINISTERIO DA FAZENDA	1790(AMAZ
27022	OUTROS SERVICOS DE GERENCIAMENTO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMACAO E COMUNICACAO (TIC)	UND SERVIÇO TÉCNICO	1	R\$ 201,199,95	ISH TECNOLOGIA S/A	MINISTERIO DA FAZENDA	1790(AMAZ

A diferença significativa ao pretendido neste projeto é que decidimos não adquirir o suporte separado da licença por entendermos que são itens indissociáveis. Neste pregão o **item 4** consiste em "**Serviço de Suporte e Operação das Soluções**" se referindo ao DLP e CASB que trata o pregão. Sendo assim, o fato de uma cobrança separada pode comprometer o uso do valor da licença para cálculo da média.

Objeto da Compra

Pregão Eletrônico - Contratação de empresa especializada para o fornecimento de Solução de Prevenção a Perdas de Dados\, composta pelas ferramentas DATA LOSS PREVENTION - DLP e CLOUD ACCESS SECURITY BROKES - CASB\, para atendimento das necessidades de segurança da informação do Banco da Amazônia S/A\, contemplando serviços técnicos de implantação\, suporte\, operação da solução e treinamento\, Pregão Eletrônico - O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de empresa especializada no fornecimento de licenças de software de solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP)\, contemplando suporte\, instalação\, configuração\, treinamento\, garantia e atualização irrestrita para a última versão existente do fabricante por 36 (trinta e seis) meses.

Modalidade da Compra

Pregão

Resultado 1

DADOS DA COMPRA

Identificação da Compra:	00067/2022
Número do Item:	00001
Objeto da Compra:	Pregão Eletrônico - Contratação de empresa especializada para o fornecimento de Solução de Prevenção a Perdas de Dados, composta pelas ferramentas DATA LOSS PREVENTION - DLP e CLOUD ACCESS SECURITY BROKES - CASB, para atendimento das necessidades de segurança da informação do Banco da Amazônia S/A, contemplando serviços técnicos de implantação, suporte, operação da solução e treinamento.
Quantidade Ofertada:	10.698
Valor Proposto Unitário:	R\$ 936
Valor Unitário do Item:	R\$ 271,1
Código do CATSERV:	27022
Descrição do Item:	OUTROS SERVICOS DE GERENCIAMENTO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMACAO E COMUNICACAO (TIC)
Descrição Complementar:	undefined
Unidade de Fornecimento:	UND SERVIÇO TÉCNICO
Modalidade da Compra:	Pregão
Forma de Compra:	SISRP
Data do Resultado:	16/03/2023

DADOS DO FORNECEDOR

Nome do Fornecedor:	ISH TECNOLOGIA S/A
CNPJ/CPF:	01707536000104
Porte do Fornecedor:	Outros

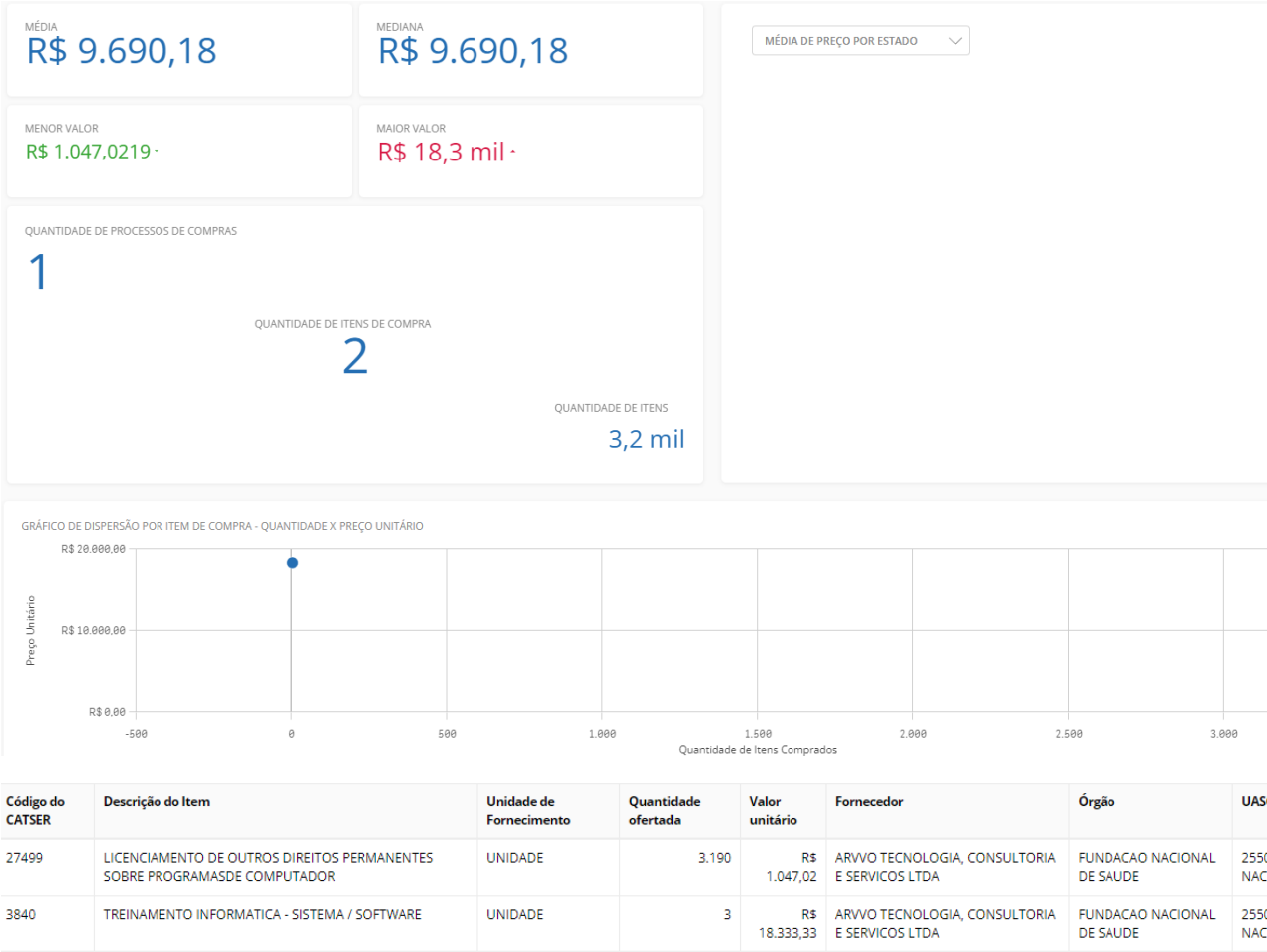
DADOS DO ÓRGÃO

Número da UASG:	179007 - BANCO DA AMAZONIA S/A
Órgão:	MINISTERIO DA FAZENDA
Órgão Superior:	PRESIDENCIA DA REPUBLICA - PRES

Os valores encontrados são referentes a pagamentos anuais quando referentes as licenças.

11.1.2. Pregão Eletrônico 10/2022 - 255000 MS- Fundação Nacional de Saúde/DF

Este pregão apresenta apenas dois (2) itens pretendidos por este projeto. Sendo eles a aquisição e solução DLP e o respectivo Treinamento.



Objeto da Compra

Pregão Eletrônico - Contratação de empresa especializada para o fornecimento de Solução de Prevenção a Perdas de Dados\, composta pelas ferramentas DATA LOSS PREVENTION - DLP e CLOUD ACCESS SECURITY BROKES - CASB\, para atendimento das necessidades de segurança da informação do Banco da Amazônia S/A\, contemplando serviços técnicos de implantação\, suporte\, operação da solução e treinamento., Pregão Eletrônico - O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de empresa especializada no fornecimento de licenças de software de solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP)\, contemplando suporte\, instalação\, configuração\, treinamento\, garantia e atualização irrestrita para a última versão existente do fabricante por 36 (trinta e seis) meses.

Modalidade da Compra

Pregão

Resultado 3

DADOS DA COMPRA

Identificação da Compra:	00010/2022
Número do Item:	00001
Objeto da Compra:	Pregão Eletrônico - O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de empresa especializada no fornecimento de licenças de software de solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP), contemplando suporte, instalação, configuração, treinamento, garantia e atualização irrestrita para a última versão existente do fabricante por 36 (trinta e seis) meses.
Quantidade Ofertada:	3.190
Valor Unitário do Item:	R\$ 1047,0219
Código do CATSERV:	27499
Descrição do Item:	LICENCIAMENTO DE OUTROS DIREITOS PERMANENTES SOBRE PROGRAMAS DE COMPUTADOR
Descrição Complementar:	undefined
Unidade de Fornecimento:	UNIDADE
Modalidade da Compra:	Pregão
Forma de Compra:	SISPP
Data do Resultado:	02/12/2022

DADOS DO FORNECEDOR

Nome do Fornecedor:	ARVVO TECNOLOGIA, CONSULTORIA E SERVICOS LTDA
CNPJ/CPF:	25359140000181
Porte do Fornecedor:	Outros

DADOS DO ÓRGÃO

Número da UASG:	255000 - MS-FUNDACAO NACIONAL DE SAUDE/DF
Órgão:	FUNDACAO NACIONAL DE SAUDE
Órgão Superior:	-

DADOS DA COMPRA

Identificação da Compra:	00010/2022
Número do Item:	00002
Objeto da Compra:	Pregão Eletrônico - O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de empresa especializada no fornecimento de licenças de software de solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP), contemplando suporte, instalação, configuração, treinamento, garantia e atualização irrestrita para a última versão existente do fabricante por 36 (trinta e seis) meses.
Quantidade Ofertada:	3
Valor Unitário do Item:	R\$ 18333,3333
Código do CATSERV:	3840
Descrição do Item:	TREINAMENTO INFORMATICA - SISTEMA / SOFTWARE
Descrição Complementar:	undefined
Unidade de Fornecimento:	UNIDADE
Modalidade da Compra:	Pregão
Forma de Compra:	SISPP
Data do Resultado:	02/12/2022

DADOS DO FORNECEDOR

Nome do Fornecedor:	ARVVO TECNOLOGIA, CONSULTORIA E SERVICOS LTDA
CNPJ/CPF:	25359140000181
Porte do Fornecedor:	Outros

DADOS DO ÓRGÃO

Número da UASG:	255000 - MS-FUNDAÇÃO NACIONAL DE SAÚDE/DF
Órgão:	FUNDAÇÃO NACIONAL DE SAÚDE
Órgão Superior:	-

Fonte: www.comprasgovernamentais.gov.br

Os valores encontrados são referentes ao pagamento de três (3) anos quando referentes as licenças.

11.1.3. Pregão Eletrônico 17/2022 - 253002 Agência Nacional de Vigilância Sanitária - DF

Neste pregão, dos quatro (4) itens adquiridos, apenas o item 4 foi utilizado como referência neste estudo.

MÉDIA
R\$ 406,00

MEDIANA
R\$ 400,15

MENOR VALOR
R\$ 201,35

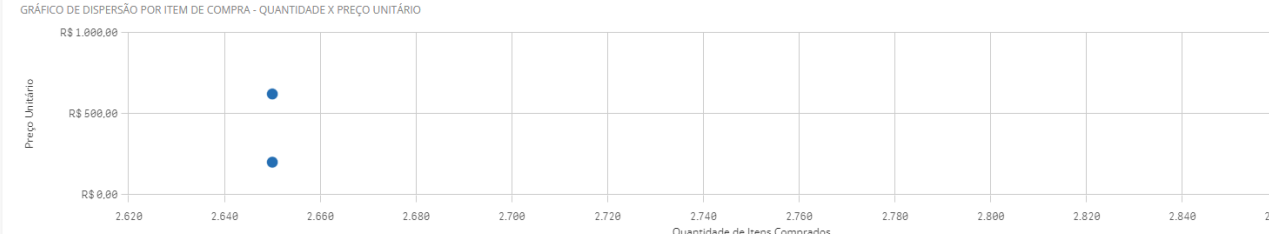
MAIOR VALOR
R\$ 622,40

QUANTIDADE DE PROCESSOS DE COMPRAS
1

QUANTIDADE DE ITENS DE COMPRA
4

QUANTIDADE DE ITENS
11,0 mil

MÉDIA DE PREÇO POR ESTADO



Código do CATSER	Descrição do Item	Unidade de Fornecimento	Quantidade ofertada	Valor unitário	Fornecedor	Órgão	UASG - Unidade
27464	LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWAREPARA SERVIDOR	UNIDADE	2.650	R\$ 201,35	BLUE EYE SOLUCOES EM TECNOLOGIA LTDA	AGENCIA NACIONAL DE VIGILANCIA SANITARIA	253002 - AGE VIGILANCIA S
27464	LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWAREPARA SERVIDOR	UNIDADE	2.861	R\$ 336,50	BLUE EYE SOLUCOES EM TECNOLOGIA LTDA	AGENCIA NACIONAL DE VIGILANCIA SANITARIA	253002 - AGE VIGILANCIA S
27464	LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWAREPARA SERVIDOR	UNIDADE	2.861	R\$ 463,80	BLUE EYE SOLUCOES EM TECNOLOGIA LTDA	AGENCIA NACIONAL DE VIGILANCIA SANITARIA	253002 - AGE VIGILANCIA S
27464	LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWAREPARA SERVIDOR	UNIDADE	2.650	R\$ 622,35	BLUE EYE SOLUCOES EM TECNOLOGIA LTDA	AGENCIA NACIONAL DE VIGILANCIA SANITARIA	253002 - AGE VIGILANCIA S

Resultado 6

DADOS DA COMPRA

Identificação da Compra:	00017/2022
Número do Item:	00004
Objeto da Compra:	Pregão Eletrônico - Solução de segurança composta por: antivírus com EDR com correção automatizada, antispam e mensagem gateway, gerenciamento de ativos e portal de software e prevenção de perda de dados (DLP) com garantia de funcionamento pelo período de 36 (trinta e seis) meses, incluídos todos os softwares e suas licenças de uso, serviços de implantação, garantia de atualização contínua, suporte técnico on-site e remoto e repasse de conhecimento de todas as soluções.
Quantidade Ofertada:	2.650
Valor Unitário do Item:	R\$ 622,35
Código do CATSERV:	27464
Descrição do Item:	LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWARE PARA SERVIDOR
Descrição Complementar:	undefined
Unidade de Fornecimento:	UNIDADE
Modalidade da Compra:	Pregão
Forma de Compra:	SISPP
Data do Resultado:	04/10/2022

DADOS DO FORNECEDOR

Nome do Fornecedor:	BLUE EYE SOLUCOES EM TECNOLOGIA LTDA
CNPJ/CPF:	26025401000190
Porte do Fornecedor:	Outros

DADOS DO ÓRGÃO

Número da UASG:	253002 - AGENCIA NACIONAL DE VIGILANCIA SANITARIA - DF
Órgão:	AGENCIA NACIONAL DE VIGILANCIA SANITARIA
Órgão Superior:	-

Fonte: www.comprasgovernamentais.gov.br

Os valores encontrados são referentes ao pagamento de três (3) anos quando referentes as licenças.

11.1.4. Comparando os Pregões encontrados

05/07/2023, 04:28

Compras.gov.br



Texto/Termos pesquisados: DATA LOSS PREVENTION

Pesquisando em: Objeto, Descrição Sumária, Descrição Completa

Objeto		Contexto / [Item]
Pregão: 67/2022 UASG: 179007 Decreto Nº 10.024/2019	Objeto: Objeto: Pregão Eletrônico - Contratação de empresa especializada para o fornecimento de Solução de Prevenção a Perdas de Dados, composta pelas ferramentas DATA LOSS PREVENTION - DLP e CLOUD ACCESS SECURITY BROKES - CASB , para atendimento das necessidades de segurança da informação do Banco da Amazônia S/A, contemplando serviços técnicos de implantação, suporte, operação da solução e treinamento.	Nenhum registro foi encontrado com este critério

Histórico de eventos publicados

Itens e Download

	Objeto	Contexto / [Item]
Pregão: 10/2022 UASG: 255000 Decreto Nº 10.024/2019	Objeto: Objeto: Pregão Eletrônico - O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de empresa especializada no fornecimento de licenças de software de solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP), contemplando suporte, instalação, configuração, treinamento, garantia e atualização irrestrita para a última versão existente do fabricante por 36 (trinta e seis) meses.	...e de solução de prevenção contra vazamento de dados - Data Loss Prevention - DL [1]

[Historico de eventos publicados...](#)

Itens e Download

(Licitações 1-2 de 2)

Voltar

Objeto	
Pregão: 67/2022 UASG: 179007 Decreto Nº 10.024/2019	Objeto: Objeto: Pregão Eletrônico - Contratação de empresa especializada para o fornecimento de Solução de Prevenção a Perdas de Dados, composta pelas ferramentas DATA LOSS PREVENTION - DLP e CLOUD ACCESS SECURITY BROKES - CASB, para atendimento das necessidades de segurança da informação do Banco da Amazônia S/A, contemplando serviços técnicos de implantação, suporte, operação da solução e treinamento.
Histórico de eventos publicados...	
Itens e Download Editais	
Objeto	
Pregão: 10/2022 UASG: 255000 Decreto Nº 10.024/2019	Objeto: Objeto: Pregão Eletrônico - O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de empresa especializada no fornecimento de licenças de software de solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP), contemplando suporte, instalação, configuração, treinamento, garantia e atualização irrestrita para a última versão existente do fabricante por 36 (trinta e seis) meses.
Histórico de eventos publicados...	
Itens e Download Editais	
Objeto	
Pregão: 17/2022 UASG: 253002 Decreto Nº 10.024/2019	Objeto: Objeto: Pregão Eletrônico - Solução de segurança composta por: antivírus com EDR com correção automatizada, antispam e messenger gateway, gerenciamento de ativos e portal de software e prevenção de perda de dados (DLP) com garantia de funcionamento pelo período de 36 (trinta e seis) meses, incluídos todos os softwares e suas licenças de uso, serviços de implantação, garantia de atualização contínua, suporte técnico on-site e remoto e repasse de conhecimento de todas as soluções.
Histórico de eventos publicados...	
Itens e Download Editais	

A partir das análise realizada sobre os Pregões encontrados, não foi possível fazer uma comparação efetiva dada a variação de itens em cada contratação. A seguir comparação possível, considerando valores **anuais**.

medida	descrição	Pregão 67/2022	Pregão 17/2022	Pregão 10/2022	Média
usuário	Serviço de subscrição anual da solução de DLP	R\$ 271,10	R\$ 207,45	R\$ 349,01	R\$ 275,85
un.	Serviço de implantação da solução de DLP	R\$ 201.199,95	n/a	n/a	n/a
turma	Serviço de capacitação na solução de DLP	R\$ 31.021,66	n/a	R\$ 18.333,33	R\$ 24.677,50
usuário	Serviço de subscrição anual da solução de CASB	R\$ 594,22	n/a	n/a	n/a
mês	Serviço de suporte e operação das soluções	R\$ 21.133,33	n/a	n/a	n/a
turma	Serviço de capacitação na solução de CASB	R\$ 17.043,32	n/a	n/a	n/a

11.1.5. Pesquisa de Preços com Fornecedores de Solução

Dada a escassez de dados atuais para uma efetiva comparação de preços a partir de compras já efetuadas, optou-se por ampliar a pesquisa, realizando cotação junto a Fornecedores de soluções.

A seguir a média encontrada a partir de Proposta Comercial fornecida por três(3) fornecedores.

ITEM	OBJETO	QUANT	FORNECEDOR 1	FORNECEDOR 2	FORNECEDOR 3	MÉDIA UNITÁRIA
1	Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention - DLP.	1200	4.260,00	4.860,00	4.452,00	4.524,00
2	Configuração e Instalação	1	150.000,00	138.800,00	112.033,00	133.611,00
3	Repasse de Conhecimento	1	120.000,00	118.800,00	115.685,00	118.161,67
4	Aquisição de licenças de software de solução de descoberta e classificação de dados, controle de acesso, monitoramento de atividade, auditoria e proteção através de bloqueio, criptografia e quarentena, para aplicações e ambientes de armazenamento em nuvem	1200	3.390,00	4.860,00	3.441,00	3.897,00
5	Configuração e Instalação	1	170.000,00	138.800,00	139.100,00	149.300,00
6	Repasse de Conhecimento	1	114.000,00	118.800,00	122.080,00	118.293,33

*Contemplando suporte, garantia e atualização irrestrita para a última versão existente do fabricante por **36 (trinta e seis) meses**.

11.1.6. Pesquisa de Preços utilizando Catálogo de Soluções de TIC com Condições Padronizadas,

O Catálogo em questão (Anexo III deste Estudo Técnico) foi elaborado pela Secretaria de Governo Digital do Ministério da Economia (SGD), fundamentado na Instrução Normativa SGD/ME nº1, de 4 de abril de 2019 e publicado em 02/07/2020, conforme Processo SEI nº19974.100166/2020-06.

Embora seja referência oficial, o referido catálogo data de julho de 2020, sendo necessária sua atualização. Para tanto utilizamos o Índice de Custo de Tecnologia da Informação (ICTI) acumulado de julho de 2020 até junho de 2023 (último data divulgada pelo IPEA).

Fonte: <https://www.ipea.gov.br/cartadeconjuntura/index.php/2023/08/indice-de-custo-da-tecnologia-da-informacao-icti-junho-de-2023/>

Seguinte esta lógica, o valor encontrado foi o seguinte:

Valor DLP Catálogo	Valor para 3 anos	ICTI acumulado Jun/20 a Jul/23	Valor DLP Corrigido 3 anos
674,63	2.023,89	17,54%	2.378,88

Registre-se que no catálogo não foi encontrado preço para solução CASB, apenas para DLP.

11.2. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

Dada a disparidade encontrada no valor das licenças e a impossibilidade de encontrar ao menos três preços públicos para os itens de Configuração/Instalação e Repasse de Conhecimento, optou-se pela combinação de todos os valores encontrados.

Após a combinação dos preços encontrados, foram utilizadas 3 metodologias de análise, a saber: Média Simples, Média + Desvio Padrão, e Mediana.

A média simples gerou um valor total de R\$ 7.726.595,07 para a contratação.

A Média combinada com desvio padrão, metodologia que desconsidera valores inexequíveis e os excessivamente elevados, gerou um valor de R\$ 8.522.013,00.

Já a mediana gerou um valor total de R\$ 7.798.397,00 para a contratação.

Por fim, utilizando os valores de DLP do catálogo SGD combinado com os menores valores encontrados para os demais itens, chegou-se ao valor de R\$ 7.353.852,83, valor este adotado como referência para a presente contratação por ser o menor dentre todos os pesquisados.

Todos os cálculos aqui relatados encontram-se pormenorizados no Anexo II deste Estudo Técnico.

11.2. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

A presente seção descreve de forma comparativa e sintética os custos anuais projetados ao longo de 3 anos com vistas a apresentar uma melhor visualização do impacto da adoção de forma centralizada cada um dos produtos apresentados nas soluções estudadas nas seções anteriores.

Dessa Forma, a tabela a seguir representa a estimativa de custos anuais com base nos cálculos realizados no levantamento de preços das soluções:

GRUPO	ITEM	DESCRIÇÃO	QUANT.	ANO 1	ANO 2	ANO 3	TOTAL
1	1	Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention (DLP), contemplando suporte, garantia e atualização irrestrita para a última versão existente do fabricante por 36 (trinta e seis) meses.	1.200	2.854.656,00	0,00	0,00	2.854.656,00
	2	Configuração e Instalação DLP	1	144.400,00	0,00	0,00	144.400,00
	3	Repasse de Conhecimento /Treinamento DLP	1	80.768,00	0,00	0,00	80.768,00
2	4	Aquisição de licenças de software de solução de descoberta e classificação de dados, controle de acesso, monitoramento de atividade, auditoria e proteção através de bloqueio, criptografia e quarentena, para aplicações e ambientes de armazenamento em nuvem - CASB - Cloud Access Security Broker. contemplando suporte, garantia e atualização irrestrita para a última versão existente do fabricante por 36 (trinta e seis) meses.	1.200	4.042.098,00	0,00	0,00	4.042.098,00
	5	Configuração e Instalação	1	138.950,00	0,00	0,00	138.950,00
	6	Repasse de Conhecimento /Treinamento CASB	1	92.980,83	0,00	0,00	92.980,83

	TOTAL	7.353.852,83
--	--------------	---------------------

12. Descrição da solução de TIC a ser contratada

12.1. Solução - A Combinação de Prevenção de Perda de Dados (DLP) e Cloud Access Security Broken (CASB).

12.1.1. A solução de DLP e CASB oferece o nível de proteção necessário para evitar violações de dados e proteger a reputação da empresa. Com essa tecnologia ao Ministério da Cultura obtém recursos abrangentes de descoberta, monitoramento e proteção que fornecem total visibilidade e controle sobre os dados confidenciais.

12.1.2. Descoberta de onde os dados residem em todos os canais: nuvem, e-mail, web, endpoints e armazenamento local (Storage).

12.1.3. Monitoramento de como os dados estão sendo usados dentro e fora da rede corporativa. Proteção dos dados de serem expostos ou roubados em tempo real.

12.1.4. Proteção contra ameaças baseadas em nuvem, como malware e ransomware. com visibilidade total de todos os serviços em nuvem, mesmo aqueles que usam conexões criptografadas por SSL.

12.1.5. Detecção de anomalias e fontes de inteligência de ameaças, como quais de seus usuários comprometeram contas, incluindo detecções antimalware estáticas e dinâmicas, além de aprendizado de máquina para detectar ransomware.

12.1.6. Protege e evita a perda de dados confidenciais em todos os serviços de nuvem em seu ambiente, não apenas naqueles que você sanciona. Aproveite o DLP corporativo avançado para descobrir e proteger dados confidenciais em serviços de nuvem sancionados e a caminho de ou para qualquer serviço de nuvem, sancionado ou não, sejam os usuários locais ou remotos, em um dispositivo móvel ou acessando de um navegador da web, ou entrando de um aplicativo móvel ou cliente de sincronização, além de Combater a perda de dados com criptografia, tokenização ou prevenção de upload.

12.1.7. Essas soluções caracterizam-se como “serviço comum” conforme Art. 9º, §2º do Decreto 7.174/2010. A fundamentação pauta-se na premissa que a contratação de serviços se baseia em padrões de desempenho e qualidade que claramente podem ser definidos no Termo de Referência, havendo diversos fornecedores capazes de prestá-los.

12.1.8. O detalhamento técnico da solução encontra-se pormenorizado do Anexo I (Especificação Técnica) deste Estudo Técnico Preliminar.

13. Estimativa de custo total da contratação

Valor (R\$): 7.353.852,83

13.1. Assim, considerando o resultado das pesquisas realizada, temos os seguintes valores (médios) estimados para a presente contratação:

LOTE	ITEM	DESCRIÇÃO	MÉTRICA	QUANT	VALOR UNIT	VALOR TOTAL
1	1	Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention - DLP.	Unidade	1.200	2.378,88	2.854.656,00
	2	Configuração e Instalação	Unidade	1	144.400,00	144.400,00
	3	Repasse de Conhecimento	Turma	1	80.768,00	80.768,00
	4	Aquisição de licenças de software de solução de descoberta e classificação de dados, controle de acesso, monitoramento de atividade, auditoria e proteção através de bloqueio, criptografia e	Unidade	1.200	3.368,42	4.042.098,00

2		quarentena, para aplicações e ambientes de armazenamento em nuvem - CASB - Cloud Access Security Broker.				
	5	Configuração e Instalação	Unidade	1	138.950,00	138.950,00
	6	Repasse de Conhecimento	Turma	1	92.980,83	92.980,83
VALOR TOTAL						7.353.852,83

14. Justificativa técnica da escolha da solução

14.1 Do ponto de vista técnico, a implantação conjunta de soluções de DLP (Data Loss Prevention) e CASB (Cloud Access Security Broker) para o caso do Ministério da Cultura, envolve uma série de benefícios relacionados, principalmente a segurança da informação, considerando a integração dessas ferramentas:

14.1.1 Proteção de Dados Sensíveis

DLP: Ajuda a identificar, monitorar e proteger dados sensíveis contra vazamentos acidentais ou intencionais, garantindo conformidade com regulamentações de privacidade, recurso extremamente importante diante da complexidade da rede de computadores do Ministério da Cultura, conforme já citado em outros capítulos.

CASB: Reforça políticas de segurança ao controlar o acesso a dados protegidos em serviços de nuvem, como e-mails, documentos e colaboração online, recursos amplamente utilizados no âmbito do Ministério da Cultura.

14.1.2 Conformidade com a LGPD.

DLP: Auxilia na conformidade com regulamentações governamentais e setoriais, como a LGPD no Brasil ou o GDPR na União Europeia e com a política de segurança da informação do Minc.

CASB: Oferece visibilidade e controle sobre o uso de serviços na nuvem, garantindo que as práticas estejam em conformidade com as regulamentações aplicáveis e com a política de segurança da informação do Minc.

14.1.3 Prevenção contra Ameaças Internas:

DLP: Identifica atividades suspeitas dentro da rede do Minc, prevenindo ameaças externas e vazamentos não autorizados.

CASB: Monitora atividades na nuvem para identificar comportamentos anômalos que possam indicar uma ameaça interna.

14.1.4 Controle de Acesso à Nuvem: - considerando o crescente uso de serviços em nuvem no âmbito do Ministério da Cultura e a ampliação da rede de computadores desta Pasta, toram se relevantes os aspectos de :

DLP: Controle o acesso a dados protegidos armazenados localmente.

CASB: Gerencia o acesso a serviços na nuvem, aplicando políticas de segurança e autenticação para usuários e dispositivos.

14.1.5 Gestão Unificada de Eventos e Incidentes:

DLP e CASB: Facilitam a centralização da gestão de eventos de segurança e incidentes, simplificando a resposta a ameaças, uma vez que os alertas deverão encaminhados para uma única equipe, será possível centralizar as informações facilitando o aperfeiçoamento contínuo da política de segurança e da implementação dos ajustes necessários.

14.1.6 Adaptação à Evolução Tecnológica:

DLP e CASB: Proporcionam flexibilidade para adaptar as políticas de segurança à medida que a tecnologia e as ameaças evoluem, essas características são essenciais para o acompanhamento da maturidade das equipes de servidores e colaboradores, além de possibilitar os níveis de restrições e bloqueios de forma gradativa, possibilitando uma melhor adaptação dos usuários e gestores.

14.1.7 A integração de DLP e CASB se mostra vantajosa, pois melhora a segurança de dados em ambientes de nuvem, simplifica a gestão de políticas de segurança e fornece visibilidade e controle abrangentes sobre como os dados são

usados e protegidos em toda a organização. Isso é especialmente importante no cenário atual do Ministério da Cultura onde as equipes dependem cada vez mais de serviços em nuvem para armazenamento e colaboração de dados, sem abrir mão dos recursos locais de rede e datacenter, características marcantes do ambiente híbrido utilizado nesta Pasta.

14.2. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS

14.2.1 Considerando os apontamentos relacionados ao levantamento de quantitativos e demais informações que comprovaram o estudo de quantidades necessárias para atender a demanda do Ministério da Cultura, restou verificado que o número de usuários da rede é muito dinâmico.

14.2.2 Tal situação se justifica diante da situação de que o Ministério da Cultura foi recriado e encontra-se em um momento de reestruturação, com criação de Escritórios Estaduais, contratação de colaboradores e servidores, neste sentido verifica-se tecnicamente necessário que a contratação possibilite a implementação de licenças de forma gradativa.

14.2.2 Portanto, recomenda-se que o instrumento contratual permita a aquisição inicial de um volume necessário para a realização da primeira implantação e posteriormente seja possível a realização de acréscimos de usuários a medida que for ampliado o quantitativo de usuários, uma vez que estão previstas ações tais como: contratação de mão de obra terceirizada além da realização de concurso público para o próximo exercício.

14.2.3 Neste sentido se houvesse a contratação do total estimado poderiam existir licenças pagas sem uso, e ser for executada uma contratação com quantitativos muito inferiores, seria necessário realizar uma contratação complementar para alcançar o número adequado de licenças para atender a demanda do Ministério da Cultura após a sua reestruturação total.

15. Justificativa econômica da escolha da solução

15.1 QUANTO A ECONOMICIDADE.

15.1.1 Considerando que a contratação pretendida visa a aquisição de duas soluções em grupos diferentes, verifica-se a possibilidade de que ocorra a implementação gradativa das soluções, podendo ser realizada a implantação de uma das duas primeiro e depois a implementação da segunda, tendo em vista a possível limitação de recursos orçamentários.

15.1.2 Neste sentido verifica-se ainda a escolha da contratação por meio de um registro de preços acertada, tendo em vista o fato de que há a necessidade da implantação de forma gradativa, e portanto ao se efetuar o registro de preços é possível garantir que não haverá alteração dos preços das licenças durante o processo de amadurecimento das políticas e da ampliação do quantitativo de usuários da rede de computadores do Ministério da Cultura.

15.1.3 Assim o Registro de Preços do volume máximo de licenças para as duas soluções visa ainda possibilitar a economia em escala, uma vez que, conforme constam nos estudos de estimativa de preços é perceptível que o fornecimento destes tipos de soluções tende a ser reduzido quanto ocorre uma contratação com maior número de licenças.

15.1.4 Desta forma, 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.

15.1.5 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.

15.1.6 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.

15.1.7 Vigência do Registro de Preços - 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.

1.

15.1.8 Da Adesão à Ata de Registro de Preços 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, consequentemente, não participes do certame licitatório.

15.2. O PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS.

15.2.1 A divisão da solução em dois grupos visa o alcance de maior competitividade, possibilitando assim com que empresas especializadas na venda de cada um tipo das soluções possam entregar os produtos com preços mais competitivos.

15.2.2 Além disso, como já relatado no item anterior, o registro de preços visa o ganho em escala e a garantia de manutenção do preço unitário durante a vigência da ata de modo a auxiliar no planejamento orçamentário para a implantação gradativa da solução.

17. Benefícios a serem alcançados com a contratação

17.1. Com a presente contratação, além dos benefícios já citados na seção 8.2.4, são esperados os seguintes benefícios:

1. Proteção dos Ativos de Informação e, por consequência, dos dados de negócio do Ministério da Cultura;
2. Identificação eficaz de violações de políticas e atividades suspeitas em tempo real, através dos servidores físicos e virtuais.
3. Redução da probabilidade de ocorrência de incidentes de segurança;
4. Controle da saída de dados sensíveis, seja via transferência de arquivos ou publicação em páginas da internet; e
5. Redução dos danos/perdas causados por incidentes de segurança.

18. Providências a serem Adotadas

1. **18.1** Levando-se em conta as justificativas para escolha da solução, não haverá nenhuma providência a ser adotada para sua implementação, a não ser as atividades normais para a implantação das soluções em produção.

19. Declaração de Viabilidade

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

19.1. Justificativa da Viabilidade

1.

1.1.

Pelo fato de a solução analisada elevar a segurança da rede do Ministério da Cultura, conforme os benefícios já apontados no item 16, a equipe de planejamento conclui esse estudo com a Declaração da Viabilidade, apresentando os resultados esperados em termos de economicidade, eficiência, efetividade e eficácia, de forma alinhada ao disposto no Normativa SGD/ME nº 94, de 23 de dezembro de 2022:

1. Economia no valor da aquisição devido a abertura do pregão para qualquer solução, seja com produtos integrados ou não, de um único fabricante ou de fabricantes diferentes.

2. Eficiência na detecção e resposta às ameaças avançadas.
3. Eficácia nas implementações de políticas de segurança e gerenciamento de dados externos e internos.

Além disso, a presente contratação atende adequadamente as demandas de negócio formuladas, os benefícios a serem alcançados são adequados, os custos previstos são compatíveis e caracterizam economicidade, os riscos envolvidos são administráveis.

A equipe de planejamento desta contratação seguiu as orientações do "Guia de Boas Práticas e Orientações para a Contratação de TIC e atendeu as recomendações da IN 01/2019 ME/SG.

20. Responsáveis

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

Despacho: Integrante Técnico

RAMON LEONN VICTOR MEDEIROS

Membro da comissão de contratação



Assinou eletronicamente em 27/12/2023 às 16:41:19.

Despacho: Integrante Requisitante

FELIPE FINGER SANTIAGO

Membro da comissão de contratação



Assinou eletronicamente em 27/12/2023 às 16:42:26.

Despacho: Integrante Administrativo

FREDERICO GUIMARAES CARDOSO

Membro da comissão de contratação



Assinou eletronicamente em 27/12/2023 às 17:14:19.

JAIME HELENO CORREA DE LISBOA

Autoridade competente



Assinou eletronicamente em 27/12/2023 às 16:44:03.

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_Especificações_Técnica-SEI_MinC_1562329.pdf (527.35 KB)
- Anexo II - Mapa Estimativo - DLP_CASB.xlsx (21.24 KB)

**Anexo I - Caderno_de_Especificações_Técnica-
SEI_MinC_1562329.pdf**



MINISTÉRIO DA CULTURA
SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO
 Esplanada dos Ministérios, Bloco B, - Bairro Zona Cívica Administrativa, Brasília/DF, CEP 70068-900
 Telefone: - <http://www.cultura.gov.br>

CADERNO DE ESPECIFICAÇÕES TÉCNICAS

ANEXO I

PROCESSO: 01400.013362/2023-15

**DOCUMENTOS
RELACIONADOS**

OBJETO - Solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP) com fornecimento de licenças e ferramenta de descoberta e classificação de dados, controle de acesso, monitoramento de atividade, auditoria e proteção através de bloqueio, criptografia e quarentena, para aplicações e ambientes de armazenamento em nuvem, Cloud Access Security Broker (CASB), incluindo implantação da solução, treinamento e suporte técnico pelo período de 36 (trinta e seis) meses

ESTUDO TÉCNICO PRELIMINAR 73/2023

TERMO DE REFERÊNCIA 84/2023

CONTRATAÇÃO: 420001/90065/2023

QUADRO DE COMPOSIÇÃO - GRUPO/LOTE E ITENS.

LOTE	ITEM	DESCRIÇÃO
01	1	Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention - DLP
	2	Configuração e Instalação
	3	Repasse de Conhecimento
02	4	Aquisição de licenças de software de solução de descoberta e classificação de dados, controle de acesso, monitoramento de atividade, auditoria e proteção através de bloqueio, criptografia e quarentena, para aplicações e ambientes de armazenamento em nuvem - CASB - Cloud Access Security Broker
	5	Configuração e Instalação
	6	Repasse de Conhecimento

1. ITEM 01 - AQUISIÇÃO DE LICENÇAS DE SOFTWARE DE SOLUÇÃO DE PREVENÇÃO CONTRA VAZAMENTO DE DADOS - DATA LOSS PREVENTION - DLP

Obs.: caso haja divergências entre este documento e os demais que fazem parte do edital, deverá prevalecer o constante neste documento.

1.1. Gerenciamento da solução de Prevenção de Perda de Dados

1.1.1. A solução deve fornecer uma estrutura de política única em todos os canais de exfiltração de dados (por exemplo, e-mail, Web, aplicativos SaaS, Impressão, aplicações, Mídia Removível, Compartilhamento de Arquivos);

1.1.2. Todas as funções de gerenciamento, incluindo alterações de configuração e upgrades, devem ser conduzidas a partir de um console central;

1.1.3. O sistema deve apoiar o acesso baseado em funções e a administração delegada com funções pré-definidas e personalizáveis:

- Auditor
- Gerente de Incidentes
- Gerente de Políticas
- Super Administrador

- Administrador

1.1.4. A solução proposta deve oferecer suporte à integração com Active Directory ou File Directory (CSV);

1.1.5. A solução deve oferecer suporte à criação/exceção de política com base no diretório de usuário/grupo, máquina, rede, domínio;

1.1.6. A solução deve ter a capacidade de auditar alterações (por exemplo, logon/off, alterações de regras, logs do sistema, logs de tráfego);

1.1.7. Capacidade de o sistema notificar quando está tendo problemas de conexão;

1.1.8. Capacidade de integração (via syslog ou extração de banco de dados) com ferramentas de SIEM para fins de registro e alerta;

1.1.9. A solução deve fornecer escalabilidade futura para todos os componentes integrantes da arquitetura que compõe o sistema de DLP;

1.1.10. A solução deve oferecer suporte a ambientes de infraestrutura virtualizados, como Azure ou AWS para o portal de gerenciamento, banco de dados e outros componentes.

1.1.11. A solução deve ter integração nativa com Classificações de Dados (Boldon James, Microsoft AIP, Seclore, Titus).

1.1.12. A solução proposta deve ser capaz de implantar o agente usando métodos comuns de implantação de software, como GPO, SCCM, JAMF etc.

1.1.13. A solução deve fornecer a capacidade de verificar o status do agente e relatar quaisquer agentes que não estejam funcionando corretamente;

1.1.14. As comunicações com os módulos da solução e sistemas integrados devem ser criptografadas, via https (entrada/saída);

1.1.15. A solução deve oferecer suporte ao Microsoft RMS;

1.1.16. A solução deve usar um banco de dados relacional corporativo, como SQL;

1.1.17. O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade para instalação, no mínimo, nos sistemas operacionais:

- Windows Server 2008 R2 SP1;
- Windows Server 2012;
- Windows Server 2012 R2;
- Windows Server 2016;

1.1.18. A arquitetura da solução deve oferecer suporte a sites remotos e usuários de rede distribuídos em muitos locais diferentes.

1.1.19. A solução deve descrever em meios de implantação típicos e onde cada componente reside.

1.1.20. A solução deve oferecer suporte à autenticação de dois fatores para acesso do administrador ao console de gerenciamento

1.1.21. A solução deve suportar os seguintes algoritmos de criptografia:

- AES (128)
- AES (256)
- Triple DES

1.1.22. A solução deve ter uma API RESTful disponível para incidentes de obtenção e atualização

1.1.23. Solução deve ser capaz de ser implantada em Máquinas Virtuais AWS EC2 e Azure

1.1.24.

1.1.25.

1.2. **Configuração de políticas de segurança de dados e detecção de conteúdo confidencial**

1.2.1. A solução deve ter políticas específicas de conformidade "prontas para uso" com base na região e no tipo de setor.

1.2.2. A solução deve ter políticas pré-definidas (1500+) baseadas em RegEX, Dicionários ou Scripts e deve ser capaz de selecionar políticas com base na correlação do país e das indústrias.

1.2.3. A solução deve fornecer políticas predefinidas para identificar possíveis expressões que sejam indicativas de cyberbullying, padrões autodestrutivos ou descontentamento dos funcionários

1.2.4. A solução deve ter políticas de Indicadores de Risco de Roubo de Dados (por exemplo, dados enviados em horários incomuns, e-mail para concorrentes, comunicação suspeita de malware,

currículos etc.)

- 1.2.5. A solução deve ter a capacidade de usar uma única política para varrer os dados onde quer que sejam armazenados, transmitidos ou usados, tanto na rede quanto no terminal.
- 1.2.6. A solução deve permitir modificar os canais de destino podem para quaisquer políticas. (Ex: incluir em uma política utilizando o protocolo SMTP , poder incluir os protocolos HTTP e HTTPS.
- 1.2.7. Deve configurar exceções baseadas em regras de forma simples evitando geração de falsos positivos
- 1.2.8. A solução deve permitir uma sintaxe flexível para vincular dados a aplicativos específicos, servidores de arquivos, compartilhamentos de rede, impressoras e padrões de conteúdo exclusivos
- 1.2.9. A solução deve oferecer suporte a tipos de arquivo verdadeiros predefinidos
- 1.2.10. A solução deve oferecer suporte a condições de políticas com base na lógica booleana (AND, OR, NOT)
- 1.2.11. A solução deve suportar dados confidenciais em diferentes idiomas, incluindo mas não limitando o suporte para Português do Brasil e Inglês.
- 1.2.12. A solução deve extrair e inspecionar o conteúdo baseado em texto de arquivos e anexos;
- 1.2.13. A solução deve analisar os metadados do arquivo
- 1.2.14. A solução deve oferecer suporte a impressão digital de arquivo parcial e de hash completo para todos os canais de exfiltração de dados
- 1.2.15. A solução deve distinguir entre diferentes tipos de PII ou PHI. Ex: Distinguir entre os nove dígitos sociais de um cliente (CPF) e número de segurança de um número de telefone de nove dígitos sem a presença de uma palavra-chave
- 1.2.16. A solução deve suportar a inspeção de tipos de arquivos de arquivos (ZIP, TAR) para detectar o conteúdo com impressão digital.
- 1.2.17. A solução deve suportar a análise de arquivos e anexos grandes (20 MB e maiores) durante o processo de impressão digital do conteúdo.
- 1.2.18. A solução deve fornecer um método para dados de impressão digital, como registros de clientes (dados estruturados)
- 1.2.19. A solução deve proteger pelo menos 10 milhões de linhas de conteúdo específico de um banco de dados de informações confidenciais sem depender de palavras-chave ou padrões
- 1.2.20. A solução deve oferecer suporte a um método de detecção de aprendizado de máquina para códigos-fonte, formulários.
- 1.2.21. A solução deve suportar regras totalmente personalizáveis com expressões regulares, palavras-chave, frases-chave e dicionários
- 1.2.22. A solução deve oferecer suporte ao conteúdo da lista de permissões para remover com segurança a detecção de conteúdo textual
- 1.2.23. A solução deve oferecer suporte à detecção de várias palavras-chave com base em um peso especificado
- 1.2.24. A solução deve suportar pelo menos 5.000 listas de palavras-chave exclusivas
- 1.2.25. A solução deve suportar correspondência de padrões combinada com validação. Por exemplo, detectar padrões comuns de números de cartão de crédito como bem como fazer a validação da soma de verificação para garantir um número de cartão de crédito válido;
- 1.2.26. A solução deve detectar formatos de arquivo criptografados conhecidos e desconhecidos;
- 1.2.27. A solução deve identificar tags de rótulos de metadados de Boldon James, Proteção de Informações do Azure ou outras soluções de classificação de dados;

1.3. **Configuração de proteção para estações de trabalho**

- 1.3.1. O agente da solução deve ser compatível com MacOS e WindowOS
- 1.3.2. O agente da solução deve ser compatível com VMWare Horizon e Citrix XenApp
- 1.3.3. O agente da solução deve fornecer proteção contínua de dados confidenciais, independentemente de o usuário estar dentro ou fora da rede. A última política aplicada deverá ser sempre a política padrão
- 1.3.4. A solução deve detectar tentativas do usuário de enviar dados confidenciais por e-mail e Web (HTTP/S)
- 1.3.5. A solução deve impedir que os usuários enviem dados confidenciais por qualquer aplicativo no computador endpoint sem precisar abrir uma solicitação de recurso para oferecer suporte a novos

aplicativos.

- 1.3.6. A solução deve impedir a exfiltração de dados por meio de mídia removível (por exemplo, unidades USB)
- 1.3.7. A solução deve ser capaz de aplicar políticas diferentes mesmo quando os usuários estão usando o mesmo endpoint
- 1.3.8. As tarefas de descoberta de dados de endpoint devem ter uma opção de agendamento:
- uma vez;
 - diariamente;
 - semanalmente;
 - continuamente
- 1.3.9. A tarefa de descoberta de dados de endpoint deve ter configurações flexíveis para verificar apenas quando o computador estiver ocioso ou pausar a verificação enquanto o computador estiver funcionando com baterias
- 1.3.10. A tarefa de descoberta de dados deve oferecer suporte à inclusão e exclusão por tipo de arquivo, pastas, idade ou tamanho
- 1.3.11. A tarefa de descoberta de dados deve oferecer suporte a opções de varredura completas e diferenciais
- 1.3.12. A descoberta de dados deve ter uma opção para preservar o tempo de acesso original
- 1.3.13. O agente da solução deve aproveitar as tags de rótulos de metadados MIP ou Boldon James para impor a classificação ou reclassificar quando um arquivo violar uma política de dados em repouso
- 1.3.14. O agente precisa ser auto-regenerativo e resistente a adulterações.
- 1.3.15. Deve monitorar a área de transferência do sistema operacional e tomar medidas com base nos dados copiados e/ou protegidos.
- 1.3.16. A solução precisa oferecer suporte a opções de implantação de sistemas operacionais virtualizados.
- 1.3.17. O agente precisa oferecer uma mensagem pop-up que possa conter informações customizadas quando o usuário violar uma política
- 1.3.18. A mensagem pop-up deve fornecer uma oportunidade para fornecer justificativa comercial quando a política permitir esta ação.
- 1.3.19. A justificativa do usuário deve ser registrada/armazenada em um método que possa ser lido por outros sistemas"
- 1.3.20. Os arquivos copiados para dispositivos removíveis devem ser criptografados e o conteúdo deve ser legível apenas em ativos de propriedade da empresa
- 1.3.21. O agente deve oferecer suporte à visibilidade de dados copiados para dispositivos de mídia removível específicos
- 1.3.22. O agente da solução deve oferecer suporte à criptografia de nível de administrador e senha de auto criptografia para o usuário quando os arquivos são copiados para mídia removível
- 1.3.23. O agente de endpoint precisa ter o mínimo ou nenhum impacto no desempenho da máquina.
- 1.3.24. O agente da solução deve oferecer suporte a políticas hierárquicas de usuário/grupo com correção/resposta configuráveis.
- 1.3.25. O agente da solução deve ser compatível com os navegadores Edge Chromium, Firefox, Safari (Apple) e Chrome
- 1.3.26. O agente da solução deve oferecer suporte ao monitoramento e bloqueio de dados confidenciais carregados para aplicativos em nuvem não autorizados e armazenamento em nuvem
- 1.3.27. O agente da solução deve oferecer suporte a um processo para desabilitar o agente do endpoint com autorização
- 1.3.28. O agente da solução deve oferecer suporte à capacidade de confiar no aplicativo, configurando-o para não ser monitorado.
- 1.3.29. O agente da solução deve oferecer suporte às seguintes operações em dados confidenciais que podem ser executadas nas estações de trabalho:
- 1.3.30. Copiar e colar controles (ou seja, atividades da área de transferência)
- 1.3.31. Controle de impressão em impressoras locais ou de rede
- 1.3.32. Salvar conteúdo em diferentes locais, incluindo salvar em:

- Pastas locais
- Compartilhamentos de arquivos remotos
- Unidades removíveis conectadas a um sistema de endpoint, como unidades USB
- Salvar em locais de armazenamento em nuvem

1.4. **Configuração de proteção para rede - Email**

- 1.4.1. A solução deve ser integrada ao Enterprise SMTP Gateway ou pode ser colocada entre um gateway SMTP corporativo para realizar a análise DLP
- 1.4.2. A solução deve dar suporte ao Exchange Online (no local, híbrido ou O365)
- 1.4.3. A solução deve ter capacidade de implantar gateways SMTP no Azure para se integrar facilmente ao O365
- 1.4.4. A solução deve oferecer suporte à quarentena de e-mail para e-mails que violaram as políticas de DLP
- 1.4.5. A solução deve ter criptografia nativa ou pelo menos integrar-se a ferramentas de criptografia de terceiros via X-Headers
- 1.4.6. A solução deve oferecer suporte a anexos de arquivo maiores que 25 MB para análise de DLP
- 1.4.7. A solução deve suportar quarentena, criptografar, descartar anexos e permitir ações de correção de e-mail
- 1.4.8. A solução deve oferecer suporte à análise de reconhecimento óptico de caracteres (OCR) com base nas políticas de DLP criadas

1.5. **Configuração de proteção para rede – Web**

- 1.5.1. A solução fornece a capacidade de evitar vazamento de dados pelo canal SSL ao integrar com seu próprio gateway sem a necessidade de solução de terceiros ou dependência do protocolo ICAP
- 1.5.2. A solução deve monitorar vários tipos de tráfego na web: webmail, postagem na web e outros protocolos usando HTTP/S
- 1.5.3. A solução deve monitorar o tráfego FTP ativo e passivo
- 1.5.4. A solução deve bloquear e permitir ações de correção da Web
- 1.5.5. A solução deve oferecer suporte a by-pass quando ocorrer um erro inesperado
- 1.5.6. A solução deve suportar páginas de bloqueio personalizáveis
- 1.5.7. A solução deve ter a capacidade de monitorar portas/protocolos adicionais além de HTTP/HTTPS
- 1.5.8. A solução deve ter o Secure ICAP nativo para integração com Proxy, NGFW ou CASB
- 1.5.9. A solução deve suportar integração com outros proxies via ICAP ou encadeamento de proxy
- 1.5.10. A solução precisa dar suporte à implantação do Azure
- 1.5.11. A solução deve oferecer suporte à análise de reconhecimento óptico de caracteres (OCR) com base nas políticas de DLP criadas

1.6. **Configuração de proteção para rede - Monitoramento**

- 1.6.1. A solução deve suportar o modo de conexão SPAN/Mirror Port
- 1.6.2. A solução deve oferecer suporte a VLAN
- 1.6.3. A solução deve suportar a inclusão de redes específicas
- 1.6.4. A solução deve suportar a inclusão de serviços específicos (HTTP,Email,FTP) e portas
- 1.6.5. A solução deve oferecer suporte à análise de OCR com base nas políticas de DLP criadas

1.7. **Prevenção de Perda de Dados para Nuvem**

- 1.7.1. A solução deve aproveitar a mesma estrutura de política de outros canais DLP para canais DLP Cloud API e DLP Cloud Proxy (in-line)
- 1.7.2. A solução deve ter integração de API com os principais aplicativos em nuvem: Office365, G-Suite, Box, Dropbox, Salesforce e ServiceNow
- 1.7.3. A solução deve ter controle DLP granular para M365 Teams, OneDrive e SharePoint
- 1.7.4. A solução deve oferecer suporte à análise para atividades de upload, download e compartilhamento de aplicativos na nuvem para identificar possíveis violações de DLP
- 1.7.5. A solução deve oferecer suporte às seguintes ações de correção para análise de atividades de API: quarentena com nota personalizável, quarentena sem nota, cancelamento de compartilhamento

externo, cancelamento de compartilhamento interno, cancelamento de compartilhamento de tudo e somente auditoria

1.7.6. A solução deve ser capaz de monitorar/controlar atividades de upload/download de aplicativos em nuvem que violem as políticas de DLP de dispositivos não gerenciados e gerenciados

1.7.7. A solução deve ter granularidade para aplicar políticas apenas para aplicativos de nuvem específicos com base na operação do usuário (por exemplo, upload/anexação/download de arquivos)

1.7.8. A solução deve oferecer suporte à varredura de dados em repouso por meio de conexão de API para Office365, G-Suite, Box, Dropbox, Salesforce e ServiceNow

1.7.9. A solução deve oferecer suporte a ações de correção para varredura de dados em repouso quando os arquivos violam políticas de DLP

1.7.10. A solução deve oferecer suporte às seguintes ações de correção para varredura de dados em repouso: quarentena com nota personalizável, quarentena sem nota, cancelar compartilhamento externo, descompartilhar interno, cancelar compartilhamento de tudo e auditar apenas

1.7.11. Capacidade de aplicar políticas granulares com base na atividade do usuário do aplicativo na nuvem (API offline): upload de arquivos, download de arquivos, compartilhamento de arquivos externos, compartilhamento de arquivos não reconhecidos)

1.7.12. Capacidade de aplicar políticas granulares com base na atividade do usuário do aplicativo na nuvem (Real-time-Inline): upload de arquivos, anexação de arquivos, download de arquivos

1.7.13. A solução deve ser capaz de aplicar políticas de dlp por aplicativos de nuvem

1.7.14. A solução deve ter capacidade de criar políticas de DLP com base em predicados diferentes, como localização, funcionalidade de aplicativos em nuvem, registro de dispositivo (gerenciado versus não gerenciado),

1.7.15. A solução deve ter a capacidade de aplicar políticas com base na pontuação de impacto nos negócios que consiste em uma regra básica de detecção com uma pontuação numérica, e essas pontuações são divididas em quatro níveis diferentes: Crítico, Alto, Médio e Baixo.

1.7.16. A solução deve oferecer suporte a aplicativos de nuvem personalizados em linha (HTTPS) sem a necessidade de abrir uma solicitação de recurso e também deve oferecer suporte à proteção DLP para upload/download

1.7.17. Capacidade de suportar qualquer aplicativo em nuvem inline (HTTPS) sem a necessidade de abrir uma solicitação de recurso com o fornecedor, e também deve suportar proteção DLP para upload/download

1.7.18. A solução deve ter diferentes tipos de modo de implantação: API, integração SSO via SAML 2.0 ou instalação do agente

1.7.19. A solução deve ter suporte para adicionar proxy reverso ao fazer a integração SSO via SAML 2.0

1.7.20. Capacidade de oferecer suporte à proteção sem agente ao acessar a partir de dispositivos não gerenciados

1.7.21. A solução deve fornecer análise de comportamento de risco do usuário com base nas atividades do usuário de aplicativos em nuvem

1.7.22. Capacidade de suportar regras de detecção de anomalias para aplicativos em nuvem: Força Bruta, tomada de conta, insider malicioso, comprometido e atividade suspeita por um usuário privilegiado.

1.8. **Configuração de proteção para Dados em Repouso**

1.8.1. A solução deve oferecer suporte à verificação de dados em repouso para Exchange, Outlook PST, bancos de dados, Sharepoint e sistemas de arquivos

1.8.2. A solução deve dar suporte ao OAuth 2.0 para verificação de dados em repouso do Exchange Online

1.8.3. A solução deve suportar SMB, NFS e CIFS para compartilhamentos de arquivos baseados em Windows e não Windows

1.8.4. A solução deve oferecer suporte aos métodos de verificação TCP ou ICMP ao pesquisar compartilhamentos de rede

1.8.5. As tarefas de descoberta de dados devem ter uma opção de agendamento: uma vez, diariamente, semanalmente ou continuamente

1.8.6. A tarefa de descoberta de dados deve oferecer suporte à inclusão e exclusão por tipo de arquivo, pastas, idade ou tamanho

1.8.7. A tarefa de descoberta de dados deve oferecer suporte a opções de varredura diferencial e completa

- 1.8.8. A descoberta de dados deve ter uma opção para preservar o tempo de acesso original
- 1.8.9. A descoberta de dados deve oferecer suporte à alocação de largura de banda para verificação do processo de descoberta
- 1.8.10. A descoberta de dados deve oferecer suporte aos recursos de reconhecimento óptico de caracteres (OCR)

1.9. **Gerenciamento de incidentes**

- 1.9.1. A solução deve fornecer a capacidade de escalar incidentes críticos para gerentes ou proprietários de dados
- 1.9.2. A solução deve fornecer controles de segurança e acesso em torno do caso/incidente (usuário e grupo)
- 1.9.3. A solução deve atribuir incidentes/casos a usuários de diferentes Unidades de Negócios
- 1.9.4. A solução deve permitir a definição e o estabelecimento de fluxos de trabalho específicos (ou seja, adicionar todos os três tipos de eventos aos casos), atribuir casos a usuários/proprietários individuais, permitir que os usuários adicionem notas etc.
- 1.9.5. A solução deve oferecer suporte ao monitoramento e gerenciamento de aspectos críticos e fases de cada incidente/caso e fases de cada incidente/caso até a resolução, envolvendo administradores autorizados especificados e usuários específicos da função, conforme necessário durante todo o processo
- 1.9.6. A solução deve fornecer a capacidade de mostrar apenas determinados incidentes de um departamento específico ao ponto focal atribuído desse departamento
- 1.9.7. A solução deve fornecer a capacidade de liberar automaticamente um e-mail em quarentena, postar a aprovação do gerente sem qualquer intervenção manual no console DLP
- 1.9.8. A solução deve oferecer suporte a scripts de correção para planos de ação de DLP (por exemplo, quando um arquivo viola as políticas de DLP, as soluções deixam um arquivo de exclusão com uma notificação)
- 1.9.9. A solução deve oferecer suporte ao Fluxo de Incidentes (Workflow) via API para liberar e-mails de quarentena

1.10. **Dados em repouso**

- 1.10.1. A solução deve oferecer suporte à varredura de dados em repouso para Exchange, Outlook PST, bancos de dados, Sharepoint e sistemas de arquivos
- 1.10.2. A solução deve oferecer suporte ao OAuth 2.0 para dados do Exchange Online na varredura em repouso
- 1.10.3. A solução deve oferecer suporte a SMB, NFS e CIFS para compartilhamentos de arquivos baseados em Windows e não Windows
- 1.10.4. A solução deve oferecer suporte a métodos de verificação TCP ou ICMP ao pesquisar compartilhamentos de rede
- 1.10.5. As tarefas de descoberta de dados devem ter uma opção de agendamento por: uma vez, diariamente, semanalmente ou continuamente
- 1.10.6. A tarefa de descoberta de dados deve oferecer suporte à inclusão e exclusão por tipo de arquivo, pastas, idade ou tamanho
- 1.10.7. A tarefa de descoberta de dados deve oferecer suporte a opções de varredura diferencial e completa
- 1.10.8. A descoberta de dados deve ter uma opção para preservar o tempo de acesso original
- 1.10.9. A descoberta de dados deve oferecer suporte à alocação de largura de banda para a varredura do processo de descoberta
- 1.10.10. A descoberta de dados deve oferecer suporte a recursos de Reconhecimento Óptico de Caracteres (OCR)

1.11. **Relatórios e Alertas**

- 1.11.1. A solução deve permitir a investigação de incidentes envolvendo dados em repouso, dados em uso e dados em movimento a partir de um console de gerenciamento centralizado.
- 1.11.2. A solução deve fornecer resumo e agrupamento de relatórios personalizados em diferentes variáveis e atributos.
- 1.11.3. A solução deve suportar exportações de relatórios de incidentes via planilha, XML, PDF ou HTML.
- 1.11.4. A solução deve ter relatórios pré-definidos para auxiliar nas investigações.

- 1.11.5. A solução deve suportar a capacidade de salvar relatórios personalizados e filtros de incidentes.
- 1.11.6. A solução deve suportar a capacidade de definir permissões de relatórios por departamentos.
- 1.11.7. A solução deve usar análise de dados avançada para fornecer à sua equipe de operações de segurança um relatório de classificação de pilha sobre os principais riscos de segurança de dados em sua organização
- 1.11.8. A solução deve ser capaz de gerar relatórios programados
- 1.11.9. A solução deve fornecer relatórios flexíveis de incidentes (diário, semanal, mensal, trimestral etc.)
- 1.11.10. A solução deve ser capaz de relatar o número de alertas gerados por destino
- 1.11.11. A solução deve permitir que os usuários criem mensagens de alerta personalizáveis para administradores, usuários e gerentes de usuários
- 1.11.12. A solução deve fornecer um catálogo de relatórios abrangente que forneça um "drill-down" para facilitar a investigação dos incidentes de maior risco
- 1.11.13. A solução deve ser capaz de fornecer dados forenses dentro do mesmo registro de incidente.
- 1.11.14. A solução deve priorizar instantaneamente casos de níveis de risco alto a baixo com limites de pontuação de risco personalizáveis fornecidos em uma pilha de relatórios de classificação de risco de incidente
- 1.11.15. A solução deve capturar dados de eventos com metadados apropriados (data/hora, usuário, protocolo)
- 1.11.16. A solução deve suportar um protocolo de cadeia de custódia
- 1.11.17. A solução deve reter os logs por pelo menos um ano, se não for possível, a solução deve oferecer suporte ao arquivamento de incidentes
- 1.11.18. A solução deve ter a capacidade de alterar a gravidade:
 - Alta;
 - Média;
 - Baixa
- 1.11.19. A solução deve ter a capacidade de alterar seu o status:
 - Novo;
 - Em Processo;
 - Fechado;
 - Falso Positivo;
 - Escalado;

1.12. **Módulo de Classificação de Informação**

- 1.12.1. A solução deverá possuir engine de classificação baseado em Inteligencia Artificial.
- 1.12.2. O produto deve ter seu autoaprendizado alimentado por um sistema de machine learning.
- 1.12.3. A solução deverá integrar-se de forma automatica com soluções de DLP.
- 1.12.4. O software deverá suportar de forma automatica as principais normas (ECC-2018, GDPR, PII, ISSO 27001, PCI, CMMC, SAMA, NCA etc.
- 1.12.5. Para funcionamento da solução, caso seja necessário uso de banco de dados, todo licenciamento da solução deve ser de responsabilidade da contratada.
- 1.12.6. Deverá recomendar níveis de conformidade e classificação ao usuário usando Inteligência Artificial, Machine Learning e tentativas de log para expor ou desclassificar a informação.
- 1.12.7. A solução deverá funcionar tanto on premises quanto em nuvem.
- 1.12.8. O produto deverá gerar e agendar automaticamente os relatórios.

i. Aplicação de Classificação

- Deverá ter a capacidade de escolher mais de um valor de classificação (múltiplas seleções).
- Deve permitir funcionalidade de exibir aos usuários a solicitação de classificar documentos por uma caixa de diálogo pop-up.
- A solução deve permitir a rotulagem assistida, orientando o usuário através de escolhas de classificação para garantir seleções válidas.

- Deve possuir opções de classificação marcadas dinamicamente para esquemas avançados (como ITAR, CUI, SAMA, PII etc.).
- Deve possuir a capacidade de ter uma classificação padrão ou classificação sugerida pela solução.
- A solução deverá solicitar ao usuário para classificar documentos ao salvar, imprimir ou enviar um e-mail.
- A solução deverá aplicar tag em imagens e suporte a vídeo por meio do clique com o botão direito do mouse no Windows Explorer.
- O produto deverá aplicar tag em arquivos CAD por meio do clique com o botão direito do mouse no Windows Explorer.
- A solução deverá aplicar tag (etiquetas) em MS Visio e o Project por meio do clique com o botão direito do mouse no Windows Explorer.
- Deve ter a capacidade de criar expressões regulares (Regexes) para sugestões de classificação no painel do produto.
- A solução deve possuir regras de rotulagem padrão (automáticas) para o Agente. Como por exemplo, permitir que todos os arquivos e e-mails novos ou modificados serão classificados por padrão, ou seja, Internos ou Confidenciais.
- Capacidade de configurar regras de rotulagem padrão (automáticas) e individualmente por plug-in compatível no mínimo com Microsoft Word, Microsoft Excel, Microsoft Power Point e Microsoft Outlook.
- O agente deve se atualizar automaticamente.
- A solução deve possuir autenticação com LDAP para os agentes instalados nas estações de trabalho dos usuários.
- Deve possibilitar a classificação em massa de arquivos com um clique com o botão direito do mouse pelo Windows Explorer.

ii. Funcionalidade do Agente para MacOS

- Deve possuir etiquetas exclusivas e não exclusivas para utilização de no mínimo:
 - i. Tags de classificação;
 - ii. Tags de conformidade;
 - iii. Tags de atributos e quaisquer outras etiquetas personalizadas.
- Possuir capacidade de adicionar vários cabeçalhos flutuantes ao mesmo documento (ou seja, um cabeçalho para interno e um cabeçalho para conformidade de PCI).
- A solução deve ter a capacidade de configurar a aparência visual para cabeçalho e rodapé individualmente nos documentos classificados.

iii. Requisitos Gerais de Políticas

- A solução deve oferecer suporte a classificação automatizada, sugerida e orientada pelo usuário.
- A solução deve avaliar o conteúdo, contexto, identidade e outros atributos de dados não estruturados para tomar decisões de classificação e política.
- A solução deve ter um mecanismo de política simples e flexível para apoiar a criação de regras. Por exemplo, possuir granularidade que permita o bloqueio de envio de e-mails confidenciais, mas permitir criar exceções por endereço de e-mail ou domínio de destino.
- A solução deve acionar ações de política e classificação com base em diferentes eventos, como Abrir, Salvar, Imprimir, Encaminhar, Fechar, Enviar ou Alteração de Classificação.
- A solução deve permitir que os administradores definam políticas com ou sem classificação como parte da política.
- A solução deve permitir que os administradores combinem políticas para fornecer um controle mais refinado.
- A solução deve suportar aninhamento/hierarquia de políticas para controlar o fluxo de execução de políticas, facilitando a manutenção de casos de uso mais avançados para classificação e aplicação de políticas.
- A solução deve fornecer ajuda contextual em toda a interface do usuário para oferecer suporte ao treinamento de segurança e ajudar os usuários a selecionarem as opções corretas de classificação e correção de política.

1.12.9. **Requisitos de classificação e identificação dos dados.**

- i. A solução deve suportar a classificação de mensagens e tarefas no Microsoft Outlook 2013/2016/2019 (ou versão superior) e no Exchange online.
- ii. A solução deve permitir a classificação de documentos do Microsoft Word, Microsoft Excel e Microsoft PowerPoint de todas as versões do Microsoft Office, desde o Office 2013 ao Office 365.
- iii. Deve fornecer um esquema de classificação consistente entre os aplicativos.

- iv. A solução deve suportar a capacidade de impor a classificação de e-mail (Microsoft Outlook, OWA e Office 365) e documentos, independentemente das extensões e tipos de arquivo.
- v. Deve suportar a capacidade de classificar em Enviar, Salvar/Salvar como, Imprimir, Novo e-mail, Fechar/Abriu documento e outros eventos de e-mail e documento.
- vi. O produto deve oferecer suporte a retenção de dados e tags, incluindo campos de dados para períodos de retenção
- vii. Deve exibir com destaque os valores de classificação (facilmente visíveis) no Microsoft Office, Microsoft Outlook e Office 365.
- viii. A solução deve reconhecer a classificação dos emails recebidos e exibir a classificação no Outlook.
- ix. A solução deve suportar diferentes valores de classificação para várias aplicações. Isso pode ser combinado com o direcionamento do usuário para apresentar opções de classificação detalhadas com base no aplicativo e na identidade do usuário.
- x. Permitir que os usuários atribuam valores de classificação por meio de uma interface de usuário de classificação de um clique.
- xi. A solução deve permitir que os usuários atribuam valores de classificação ao usar o recurso de resposta em linha do Microsoft Outlook 2013, 2016 e 2019 (ou superior).
- xii. O produto deve permitir que os usuários atribuam valores de classificação a qualquer tipo de arquivo clicando com o botão direito do mouse no Explorador de Arquivos e selecionando um ou mais arquivos.
- xiii. A solução deve dar suporte à população dinâmica de campos de classificação de fontes diferentes do esquema de classificação pré-configurado, inserindo vários atributos de metadados. Por exemplo, os valores de metadados podem vir de atributos de documentos (por exemplo, autor), variáveis ambientais e Active Directory (por exemplo, grupo, departamento).
- xiv. A solução deve oferecer suporte à solicitação de usuários para confirmar um valor de classificação automatizado (também chamado de "classificação sugerida").
- xv. Deve oferecer suporte à capacidade de solicitar que os usuários alterem a(s) classificação(ões) padrão se o padrão for inadequado para o conteúdo, contexto ou outros atributos do email ou documento.
- xvi. A solução deve oferecer suporte à capacidade de solicitar que os usuários classifiquem em alguns casos e usem a classificação automatizada em outros. Por exemplo, uma classificação padrão pode ser usada para email interno, mas os usuários são solicitados a classificar para email externo. Ou os usuários podem ser solicitados a classificar o email somente quando houver um anexo.
- xvii. Deve suportar a capacidade de verificar determinadas palavras-chave e expressões regulares e definir a classificação de acordo.
- xviii. Deve gerar metadados para todos os tipos de arquivos, incluindo metadados persistentes e incorporados para muitos arquivos que não são do escritório, ou seja, outras extensões/formatos, incluindo PDF, Visio, Project, imagens e arquivos de vídeo
- xix. Oferecer suporte à criação de metadados personalizados ilimitados para interoperabilidade (Departamento, tipo de PII, categoria de documento, contagem de PII etc.), incluindo custom X-headers.
- xx. A solução deve oferecer suporte a marcações visuais personalizáveis em e-mails e documentos (por exemplo, fonte(nome/tamanho/recursos), tamanho, cor e conteúdo).
- xxi. Deve suportar marcações visuais personalizáveis em Microsoft Outlook.
- xxii. A solução deve suportar a adição de marcações visuais na parte superior e inferior de um email.
- xxiii. A solução deve oferecer suporte à capacidade de adicionar marcas d'água em aplicativos suportados do Microsoft Office.
- xxiv. Deve oferecer suporte ao uso de variáveis em marcações visuais, tornando mais fácil para os administradores oferecer suporte a vários casos de uso em uma política.
- xxv. A solução deve suportar diferentes marcações visuais para a mesma classificação, dependendo do contexto. Por exemplo, um documento "Confidencial" com uma palavra-chave específica pode ter marcações diferentes de um documento "Confidencial" com PII.

1.12.10. **Requisitos de Relatórios e Auditoria**

- i. A solução deve registrar a atividade do usuário enquanto os usuários manipulam e-mails, documentos e arquivos.
- ii. Deve fornecer relatórios integrados.
- iii. A solução deve fornecer um conjunto inicial pré-construído de relatórios para o banco de dados de relatórios (em valores separados por tabulação/formato Excel ou Banco de dados).
- iv. Os valores de classificação no e-mail devem ser consistentes, independentemente do usuário acessar os e-mails das plataformas desktop, laptop
- v. Deve ter a capacidade de reter as classificações existentes nos encadeamentos de e-mails.

1.12.11. **Requisitos de configuração e gerenciamento**

- i. A solução deve fornecer um Console de Administração centralizado e baseado na Web para configuração de classificação e gerenciamento de políticas.
- ii. Deve oferecer suporte à configuração de implantação de um servidor central.

- iii. A console centralizada deve funcionar com base em um único agente no cliente das estações de trabalho.
- iv. A solução deve permitir que os clientes recuperem sua configuração de um servidor de gerenciamento central por meio de uma conexão segura (SSL/TLS).
- v. Deve permitir que os administradores enviem as configurações do cliente para os desktops dos usuários por meio do Servidor Central
- vi. A solução deve armazenar em cache as configurações localmente para uso offline.
- vii. Deve permitir que os agentes recebam as atualizações de política sem reiniciar os aplicativos do Microsoft Outlook e do Office.
- viii. A solução deve fornecer a capacidade de implantação em modo silencioso para que o software possa ser implantado e habilitado em diferentes fases.
- ix. Deve permitir que os administradores personalizem todas as cadeias de texto da interface do usuário para oferecer suporte a diferentes idiomas e terminologia. Isso inclui campos e valores de classificação e mensagens de aviso de política.
- x. A solução deve ser capaz de identificar informações como identidade, números de passaporte e informações de cartão de crédito para classificação automatizada por meio de recursos embutidos ou deve ter a capacidade de definir expressões regulares.
- xi. Ser compatível com Microsoft Office 2013 (32 bits e 64 bits), 2016, 2019 ou posterior.
- xii. Ser compatível com Windows 7, 8, 1 e 10 ou superior.

1.12.12. **Requisitos de integração e interoperabilidade**

- i. A solução deve suportar
 - Soluções DRM
 - Soluções DLP
- i. A solução deve fornecer a capacidade de anexar metadados a objetos de informação, alavancados por soluções de e-discovery.
- ii. Deve fornecer a capacidade de anexar metadados a objetos de informação, que podem ser aproveitados por soluções de prevenção de perda de dados (DLP) de terceiros e devem funcionar mesmo quando e-mails e documentos estiverem protegidos.
- iii. A solução deve fornecer a capacidade de gravar tags que a solução DLP possa ler.
- iv. Ter a capacidade de acionar a criptografia com base em metadados.
 - v. A impressão deve ser controlada com base na classificação e no contexto
- vi. Permitir que o usuário aplique a classificação em massa em vários arquivos selecionados nas exibições do explorador de arquivos do Windows

1.12.13. **Aplicação de marcações de classificação em Arquivos**

- i. Deve permitir as seguintes possibilidades de marcações:
- ii. Aplicar uma marcação ao cabeçalho de um arquivo
- iii. Aplicar uma marcação ao rodapé de um arquivo
- iv. Aplicar uma marca d'água a um arquivo
 - v. Aplicar uma marcação de código de campo a um arquivo
- vi. Aplicar metadados persistentes a um arquivo
- vii. As marcações visíveis podem ser personalizadas, para que não afetem os modelos, o conteúdo existente, a estrutura ou a marca.

1.12.14. **Classificação para Email**

- i. A classificação deve ser aplicada em Microsoft Outlook
- ii. Quando um e-mail é classificado, os destinatários e o remetente deverão ser verificados automaticamente no envio, para garantir que sejam apropriados - por exemplo, para evitar que um e-mail marcado como 'interno' vá para um domínio externo.
- iii. O nível de classificação de um email é atualizado automaticamente para corresponder ao nível de qualquer anexo (ou corresponder ao nível mais alto de classificação se houver mais de um anexo).
- iv. Os anexos podem ser verificados para garantir que estão classificados e a classificação não tenha expirado.
 - v. A classificação pode verificar quantos destinatários estão no email
- vi. A classificação deve permanecer em um email mesmo na resposta de um destinatário externo
- vii. Deve aplicar marcações na primeira linha do texto
- viii. Deve aplicar marcações na última linha de texto
- ix. Deve aplicar marcações no assunto de um e-mail como prefixo ou anexado
 - x. Deve aplicar marcações no cabeçalho de um email
- xi. Deve aplicar Gerenciamento de Direitos (por exemplo, Azure RMS, Seclore, Sealpath)
- xii. Deverá manter a classificação automática de e-mail externo para e-mail de entrada com base na última classificação de e-mail enviada pelo usuário interno.

1.12.15. Ações inteligentes de classificação.

- i. Não permitir o usuário salvar ou imprimir sem classificar o documento.
- ii. Deve interromper a disseminação acidental de e-mail para usuários sem um nível de autorização apropriado.
- iii. Deve sugerir ou exigir uma classificação padrão com base na posição da empresa, departamento, localização, conteúdo do arquivo.
- iv. Possuir classificação obrigatória de um arquivo criado externamente ao ser aberto, compartilhado ou impresso.
- v. Deve detectar arquivos aninhados em um arquivo ou o corpo de um e-mail.
- vi. Deve detectar conteúdo em arquivos e sugerir ou exigir classificação.
- vii. Deve detectar conteúdo em arquivos aninhados e sugerir ou exigir classificação.

1.12.16. Proteção de modificação de Metadados

- i. Todos os metadados devem ser persistentes, ou seja, os metadados removidos são reaplicados quando o arquivo é salvo, impresso ou enviado por e-mail.
- ii. Os usuários devem ser impedidos de alterar a classificação.
- iii. Os detalhes do usuário que classificou o arquivo devem ser registrados.
- iv. Se um usuário tiver permissão para alterar a classificação, essa alteração deverá ser registrada.

1.12.17. Gerenciamento de Políticas

- i. Possuir uma ferramenta de gerenciamento simples, onde as políticas podem ser criadas e modificadas
- ii. As regras de políticas devem ser criadas e editadas com um assistente simples.
- iii. As políticas podem ser personalizadas com uma ampla variedade de atributos - por exemplo, atributos do Active Directory.
- iv. Não deve possuir limite para o número de políticas que podem ser criadas.
- v. Deve possuir níveis de classificação ilimitados para permitir que uma política evolua.
- vi. A classificação pode ser alterada ao longo do tempo, à medida que as necessidades de negócios se desenvolvem.
- vii. As políticas devem se alinhar com as políticas internas de marcação e aplicação de uma empresa.
- viii. Deve permitir que uma variedade de elementos de classificação pode ser aplicada - por exemplo, seletores únicos, seletores múltiplos
- ix. Deve permitir que as políticas sejam facilmente testadas (modo de teste) antes da implantação .
- x. Deve permitir que a classificação seja obrigatória para o usuário.
- xi. As políticas devem permitir serem adaptadas para diferentes departamentos ou hierarquia - por exemplo, somente gerentes podem fazer downgrade de uma classificação.
- xii. As regras devem permitir serem adaptadas para diferentes departamentos ou hierarquia - por exemplo, as marcações visíveis não aparecem em um arquivo quando ele é impresso se o usuário estiver no Marketing.
- xiii. Deve permitir que os menus de classificação possam ser adaptados para diferentes departamentos ou hierarquia.
- xiv. Os botões de classificação devem ser agrupados (empilhados) em colunas (para que não ocupem muito espaço na faixa de opções).
- xv. Deve possuir suporte ao idioma Português Brasileiro.
- xvi. O suporte a idiomas deve ser automatizado com base na localização do usuário.

1.12.18. Auditoria

- i. Todas as ações de classificação deverão ser registradas.
- ii. Deve possuir relatórios automatizados.

2. ITEM 04 - AQUISIÇÃO DE LICENÇAS DE SOFTWARE DE SOLUÇÃO DE DESCOBERTA E CLASSIFICAÇÃO DE DADOS, CONTROLE DE ACESSO, MONITORAMENTO DE ATIVIDADE, AUDITORIA E PROTEÇÃO ATRAVÉS DE BLOQUEIO, CRIPTOGRAFIA E QUARENTENA, PARA APLICAÇÕES E AMBIENTES DE ARMAZENAMENTO EM NUVEM - CASB - CLOUD ACCESS SECURITY BROKER

2.1. Arquitetura

- 2.1.1. A solução deve ter um único console para todas as funções de CASB;
- 2.1.2. A solução deve possuir agente único para estações de trabalho Windows e MacOS;
- 2.1.3. A solução deve oferecer suporte a qualquer aplicativo HTTP(S) de qualquer dispositivo sem um agente;
- 2.1.4. A solução deve comprovar 99,99% de disponibilidade do datacenter em nuvem.

2.1.5. A solução deve suportar mais de 300 PoPs (pontos de presença) espalhados pelo planeta para prover baixa latência de acesso;

2.1.6. A solução deve oferecer suporte ao Controle de Acesso Contextual;

2.2. **Conformidade e Certificações**

2.2.1. A solução deve ter certificação SOC-2 Tipo 2;

2.2.2. A solução deve ter as certificações ISO27001, ISO27017 e ISO27018;

2.2.3. Solução deve ter certificação FedRamp;

2.2.4. A solução deve ter um status em tempo real do serviço;

2.3. **Integrações**

2.3.1. A solução deve ter suporte a túneis IPSec;

2.3.2. A solução deve ter suporte a túnel GRE universal;

2.3.3. A solução deve possuir datacenters redundantes;

2.3.4. A solução deve oferecer suporte à integração com qualquer IdP compatível com SAML;

2.3.5. A solução deve oferecer suporte ao Agente de Sincronização do Active Directory.

2.3.6. Suporta o envio de dados de ameaças para um SIEM através de syslog;

2.3.7. A solução deve ter capacidade de exportação de logs para soluções de SIEM;

2.3.8. A solução deve ser integrada aos provedores de identidade para direcionar o tráfego por meio de proxy reverso após a autenticação;

2.3.9. A solução deve oferecer suporte para integração com soluções MDM/EMM para compilar uma lista de identificadores exclusivos de dispositivo;

2.4. **Registro em log e alertas**

2.4.1. A solução deve oferecer suporte à filtragem de violações com base em vários contextos, por exemplo: usuário, política, padrão de dados, intervalo de datas, etc.);

2.4.2. A solução deve oferecer suporte à classificação de violações com base em títulos da coluna (por exemplo, gravidade, política, status, data, etc.);

2.4.3. A solução deve fornecer o número de violações detectadas no documento ou objeto, usuário e a atividade;

2.4.4. A solução deve fornecer trechos do documento que desencadearam a violação com conteúdo correspondente realçado;

2.4.5. A solução deve suportar a marcação de violações com um status (por exemplo, falso positivo, novo, aberto, resolvido);

2.5. **Monitoramento histórico e em tempo real**

2.5.1. A solução deve oferecer suporte à capacidade de filtrar com base no tipo de atividade ou nas últimas semanas/dias;

2.5.2. A solução deve suportar a capacidade de digitar parâmetros de filtragem em uma barra de pesquisa/filtro para exibir atividades específicas, usuários, etc.

2.5.3. A solução deve oferecer suporte a atividades de filtragem com base em um intervalo de datas específico ou até 30 dias anteriores;

2.5.4. A solução deve permitir a visualização da postura de segurança e a exposição de risco para acompanhamento do impacto de segurança dos investimentos em cloud com os seguintes requisitos:

- i. Visibilidade do Retorno de Investimento com relação as violações de dados evitadas;
- ii. Score Card de segurança mostrando a utilização geral da plataforma de segurança, incluindo a adoção pelo usuário;
- iii. Volume de dados confidenciais acessados por canal;
- iv. Visão de Ameaças (malware);

2.6. **Administração**

2.6.1. A solução deve oferecer suporte a MFA para acesso ao Portal de Administração;

2.6.2. A solução deve oferecer suporte ao RBAC (Controle de Acesso Baseado em Função);

2.6.3. A solução deve oferecer suporte a uma função de administrador para criar e editar políticas;

2.6.4. A solução deve oferecer suporte a uma função de administrador específica para configurar novos aplicativos SaaS suportados, criar novos usuários e visualização dos alertas;

2.6.5. A solução deve oferecer suporte a diferentes modos de exibição personalizados para grupos de usuários e dashboards/relatórios específicos;

2.7. **Gestão de Identidades**

2.7.1. A solução deve oferecer suporte à funcionalidade nativa de login único;

2.7.2. A solução deve oferecer suporte a recursos de IdP/IAM de entrada no caso de não haver nenhuma solução IDP/IAM disponível;

2.7.3. A solução deve oferecer suporte à autenticação multifator para aplicativos em nuvem como um mecanismo de mitigação de risco;

2.7.4. A solução deve oferecer suporte à integração com o Active Directory e o Azure AD para autenticação de usuário e sincronização de grupo de segurança e OU (Organization Unit);

2.7.5. A solução deve oferecer suporte à integração via SAML 2.0 com qualquer solução de gerenciamento de identidade para autenticar o acesso a serviços de nuvem sancionados;

2.8. **Notificações**

2.8.1. A solução deve oferecer suporte ao envio de um email para o usuário final quando uma política é acionada;

2.8.2. A solução deve oferecer suporte ao envio de um email para um administrador quando uma política é acionada.;

2.8.3. A solução deve oferecer suporte à criação de um incidente/alerta quando uma política é acionada;

2.9. **Controle de acesso contextual**

2.9.1. A solução deve oferecer suporte à permissão de políticas acesso específicas para dispositivos gerenciados;

2.9.2. A solução deve permitir o bloqueio de acesso a aplicações SaaS utilizadas/sancionadas pelo órgão quando a origem for de dispositivos não gerenciados;

2.9.3. Solução deve oferecer suporte ao bloqueio de acesso a aplicativos não sancionados;

2.9.4. Deve suportar políticas baseadas em departamento, geolocalização, dispositivo e Sistema Operacional e Navegadores (utilizando cabeçalho HTTP User-Agent);

2.9.5. Permitir que dispositivos pessoais visualizem conteúdo online, mas não baixem ou carreguem arquivos de aplicações SaaS;

2.9.6. A solução deve oferecer suporte à identificação de dispositivos gerenciados usando um agente;

2.9.7. A solução deve oferecer suporte à identificação de dispositivo gerenciado por um certificado de cliente;

2.9.8. A solução deve oferecer suporte à identificação de dispositivo gerenciado por um atributo SAML;

2.9.9. A solução deve suportar aplicar um adiamento do login do usuário, baseado em seu comportamento e risco, esse período deve ser configurado pelo administrador via política;

2.9.10. A solução deve oferecer suporte à configuração de um tempo limite ocioso personalizado, antes de impor a nova autenticação;

2.9.11. A solução deve oferecer suporte ao acionamento de MFA com base em grupo, dispositivo, localização, comportamento, intervalo de tempo ou qualquer combinação de critérios;

2.10. **Logs**

2.10.1. Deve suportar filtragem de violações com base em várias informações, por exemplo: usuário, política, tipo de detecção, intervalo de datas, etc.

2.10.2. A solução deve suportar a classificação de violações com base em cabeçalhos de coluna, por exemplo: gravidade, política, status, data, etc.

2.10.3. Deve fornecer o quantitativo de violações encontradas em documentos, objetos, usuários e na atividades;

2.11. **Análise e Controle de Geolocalização**

2.11.1. A Solução deve suportar detecção e bloqueio de logins de países não autorizados;

2.11.2. A solução deve suportar a detecção de logins simultâneos de locais geograficamente distantes, permitindo impor um fator adicional de autenticação, quando esse tipo de comportamento ocorrer;

2.11.3. A solução deve oferecer suporte à criação de locais personalizados para identificar sites e localidades remotas reconhecidas pelo órgão;

2.12. **Forense**

2.12.1. A solução deve oferecer suporte à capacidade de filtrar a trilha de auditoria de um usuário especificado para o período de tempo em torno do incidente;

2.12.2. A solução deve oferecer suporte à capacidade de exibir um feed de atividade para um usuário especificado;

2.13. **Funcionalidades de CASB para aplicações SaaS**

2.13.1. Suporte a realizar proxy inline de aplicativos SaaS

2.13.2. A solução deve oferecer suporte ao acesso inline a qualquer aplicativo HTTP(S) de qualquer dispositivo sem a necessidade um agente instalado no dispositivo do usuário;

2.13.3. A solução deve oferecer suporte à configuração pré-definida para uso e integração com o Microsoft 365;

2.13.4. A solução deve oferecer suporte à configuração pré-definida para uso e integração com o Google Workspace;

2.13.5. A solução deve oferecer suporte à configuração pré-definida para uso e integração com o Salesforce;

2.13.6. A solução deve oferecer suporte à configuração pronta para uso do DropBox;

2.13.7. A solução deve oferecer suporte à configuração pronta para uso para Box.com;

2.13.8. A solução deve oferecer suporte à configuração pronta para uso do ServiceNow;

2.13.9. A solução deve oferecer suporte à configuração pronta para uso do Slack;

2.13.10. A solução deve oferecer suporte à configuração pronta para uso para a Atlassian;

2.13.11. A solução deve oferecer suporte à configuração pronta para uso para a AWS;

2.13.12. Deve suportar o bloqueio de acesso a aplicativos não sancionados;

2.14. **Prevenção de Ameaças Avançadas**

2.14.1. A solução deve oferecer suporte à detecção de malware hospedado em serviços de nuvem;

2.14.2. A solução deve suportar o monitoramento de dados armazenados em aplicativos em nuvem e detectar se há malware presente nos arquivos;

2.14.3. A solução deve suportar a varredura de armazenamento de dados em nuvem em busca de novas assinaturas / variantes de malware;

2.14.4. A solução deve oferecer suporte à funcionalidade de detecção avançada de ameaças integrada ao CASB;

2.14.5. A solução deve oferecer suporte para detectar e colocar em quarentena malwares de dia zero presente em serviços de nuvem;

2.14.6. A solução deve oferecer suporte a mais de um mecanismo de Antimalware;

2.15. **Integrações com Aplicações SaaS via API**

2.15.1. A solução deve oferecer suporte à varredura de todos os arquivos e pastas armazenados em aplicativos SaaS e detectar violações de políticas de DLP especificadas;

2.15.2. A solução deve oferecer suporte à exclusão de uma lista especificada de usuários de uma varredura;

2.15.3. A solução deve oferecer suporte ao direcionamento de uma varredura para uma lista especificada de usuários;

2.15.4. A solução deve oferecer suporte à varredura somente de novos arquivos e pastas adicionados ao Microsoft Onedrive desde a última verificação executada;

2.15.5. A solução deve oferecer suporte à varredura apenas de novos arquivos e pastas adicionados ao Google Drive desde a última varredura executada;

2.15.6. A solução deve oferecer suporte à quarentena de um arquivo que violou uma política de DLP em um aplicativo SaaS;

2.15.7. A solução deve oferecer suporte ao fornecimento de uma lista de todos os arquivos atualmente em quarentena com base em políticas;

2.15.8. Deve registrar e monitorar aplicativos SaaS via API;

- 2.15.9. A solução deve suportar uma ação de correção manual pelo administrador, permitindo por exemplo, liberar um arquivo que estava em quarentena.
- 2.15.10. A solução deve suportar a marcação de violações com um status, por exemplo: falso positivo, novo, aberto e resolvido;
- 2.15.11. A solução deve oferecer suporte a um painel interativo mostrando violações de DLP em aplicativos de nuvem;
- 2.15.12. A solução deve oferecer suporte para identificar todos os arquivos e categorizá-los automaticamente;

2.16. **Shadow IT**

- 2.16.1. A solução deve oferecer suporte à detecção e exibição de "Shadow IT" descobrindo uma gama completa de aplicativos de nuvem em uso.
- 2.16.2. A solução deve oferecer suporte à descoberta e classificação automáticas de centenas de milhares de aplicativos de nuvem não sancionados
- 2.16.3. A solução deve suportar a análise de logs de firewall/proxy de terceiros para gerar um relatório sobre todos os aplicativos ShadowIT que estão sendo usados em seu ambiente;
- 2.16.4. A solução deve oferecer suporte ao resumo do número agregado de serviços de nuvem em uso e do número de serviços de alto risco em uso;
- 2.16.5. A solução deve oferecer suporte à filtragem por categoria de serviço de nuvem, nível de risco, tipo de dispositivo, país, departamento e outros atributos;
- 2.16.6. A solução deve oferecer suporte à listagem de todos os usuários de cada serviço de nuvem com base em seu respectivo nome baseado no Active Directory;
- 2.16.7. Deve possuir, no mínimo, 24 (vinte e quatro) portas 10/100/1000 BaseT full-duplex ativas simultaneamente, autossense com conectores RJ-45 diretamente conectada ao chassi, sem conversores externos, com MDI/MDIX automático.

3. **ITENS 02 e 05 - CONFIGURAÇÃO E INSTALAÇÃO**

- 3.1. A solução de TIC deverá ser plenamente implementada pela Contratada no ambiente do MinC nas quantidades solicitadas em no máximo 60 (sessenta) dias corridos, a partir da assinatura da Ordem de Fornecimento ou Ordem de Serviço.
- 3.2. A empresa que realizar a implantação deverá ter técnicos treinados em toda a solução ofertada. Os serviços deverão ser prestados por técnicos devidamente capacitados, certificados pela fabricante da solução a qual deverá atuar quanto a implementação e demais procedimentos relacionados a configuração e implementação de políticas e demais requisitos exigidos.
- 3.3. Os serviços que eventualmente acarretem risco para os sistemas em produção ou requeiram parada de servidores, equipamentos e rede elétrica, somente poderão ser executados fora de expediente, em horários previamente acordados com a área de TI do local de instalação;
- 3.4. Caberá à Contratada o irrestrito cumprimento das seguintes prerrogativas:
- i. Responsabilizar-se pela completa implantação do projeto, ou seja, todos os custos necessários à operacionalização dos equipamentos;
 - ii. Responsabilizar-se por todos os instrumentais necessários durante o período de implantação e testes de aceitação;
 - iii. Instalar e configurar todos os produtos do fornecimento da solução;
 - iv. Executar a integração de todos os produtos da solução, de modo a não prejudicar as atividades mantidas nos locais, podendo ser exigida a realização de algumas fases em horários noturnos e fins de semana para que seja cumprido o cronograma de entrega;
 - v. Elaborar a "Documentação e Finalização do Projeto", que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e/ou gerencial.

4. **ITENS 03 e 06 - REPASSE DE CONHECIMENTO**

- 4.1. A CONTRATADA deverá repassar à CONTRATANTE todas as informações solicitadas e documentação da solução, além de disponibilizar treinamento conforme especificações a serem fornecidas no Termo de Referência.
- 4.2. O treinamento será demandado à CONTRATADA pela CONTRATANTE após a efetiva implementação e estruturação da solução de segurança em seu parque tecnológico, quando acordarão o cronograma para realização do treinamento.
- 4.3. O treinamento deverá ser em Brasília – DF, para a equipe técnica do CONTRATANTE.

- 4.4. Todos os custos relativos à realização do treinamento são de exclusiva responsabilidade da CONTRATADA.
- 4.5. O treinamento deverá capacitar as equipes técnicas do CONTRATANTE a operar, configurar, administrar e resolver problemas usuais na solução adquirida, englobando tanto os componentes de hardware quanto de software.
- 4.6. Deverá ser ofertada para 1 (uma) turma com no máximo 10 alunos e com carga horária mínima de 40 (quarenta) horas.
- 4.7. Deverá ser fornecido certificado de conclusão emitido pelo fabricante.
- 4.8. Os horários do curso deverão seguir a conveniência do CONTRATANTE, podendo sua realização ocorrer apenas em um dos períodos do dia (manhã ou tarde).
- 4.9. Deverá ser fornecido material didático completo e com conteúdo oficial do fabricante.



Documento assinado eletronicamente por **Ramon Leonn Victor Medeiros, Integrante Técnico da Equipe de Planejamento da Contratação**, em 27/12/2023, às 16:16, conforme horário oficial de Brasília, com fundamento no art. 30, inciso II, da Portaria nº 26/2016, de 01/04/2016, do Ministério da Cultura, Publicada no Diário Oficial da União de 04/04/2016.



A autenticidade deste documento pode ser conferida no site https://sei.cultura.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1562329** e o código CRC **3A2E15FB**.