

Objeto: Aquisição de softwares Veeam na modalidade de subscrição (SaaS), licenciados com direito a suporte e manutenção.

SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL – SENAC

Apresentamos proposta comercial, nos seguintes termos:

LOTE - AQUISIÇÃO DE SOFTWARES VEEAM NA MODALIDADE DE SUBSCRIÇÃO (SAAS), LICENCIADOS COM DIREITO A SUPORTE E MANUTENÇÃO				
ITEM	DESCRIÇÃO	QTD.	VALOR UNITÁRIO	VALOR TOTAL
1	SaaS de Veeam Data Cloud for Microsoft 365 Advanced Bundle including Entra ID – Garantia e atualizações por 12 meses (HVDCMFE-0U-R0000-00) Proteção Microsoft 365 - 4.000 Usuários Proteção Microsoft EntraID - 16.000 Usuários	1	R\$ 1.224.300,00	R\$ 1.224.300,00
2	SaaS de Veeam Data Platform Premium – Subscrição – Garantia e atualizações por 12 meses (H-VDPPRM-VV-R0000-00) Proteção de 900 Servidores Virtuais	1	R\$ 906.750,00	R\$ 906.750,00
3	Serviços de gerenciamento das soluções em cloud, serviço de suporte e manutenção ao ambiente por 12 meses	1	R\$ 98.950,00	R\$ 98.950,00
VALOR TOTAL R\$ 2.230.000,00 (DOIS MILHÕES DUZENTOS E TRINTA MIL REAIS)				

DESCRIÇÃO DOS SERVIÇOS/TERMO DE REFERÊNCIA –**Conforme edital e anexos.**

1. OBJETO Aquisição de softwares Veeam na modalidade de subscrição (SaaS), licenciados com direito a suporte e manutenção.

2. JUSTIFICATIVA O Senac São Paulo utiliza a solução Veeam como plataforma de backup e replicação de dados em seu Data Center e nas unidades distribuídas no Estado, sendo esta a ferramenta institucional adotada para execução das rotinas de proteção, recuperação e continuidade dos serviços de tecnologia da informação. A solução é atualmente empregada na replicação de dados entre o datacenter da Sede e o campus Santo Amaro, bem como no armazenamento e gerenciamento dos backups dos ambientes virtualizados, permitindo a cópia e recuperação de máquinas virtuais e dados associados, tanto em nível local quanto em ambiente de contingência. A infraestrutura implementada possibilita a execução de rotinas de backup em disco, replicação entre sites e restauração de dados e serviços em cenários de falhas, indisponibilidades, erros operacionais ou eventos que comprometam a integridade dos ambientes, garantindo a continuidade operacional das atividades institucionais. Adicionalmente, considerando a adoção crescente de serviços em nuvem, especialmente a plataforma Microsoft 365 e o serviço de identidade Entra ID, faz-se necessária a contratação de solução complementar de proteção de dados no modelo SaaS, com capacidade de backup e recuperação de informações de Exchange Online, SharePoint Online, OneDrive e Microsoft Teams, bem como dos objetos de identidade gerenciados no Entra ID. A referida solução deve possibilitar a recuperação de dados em diferentes níveis de granularidade, além de disponibilizar mecanismos de consulta e localização de informações armazenadas, contribuindo para atividades de auditoria, governança e atendimento a requisitos de conformidade. A contratação pretendida visa, portanto, assegurar a continuidade das operações de backup e replicação já existentes, bem como a ampliação da proteção de dados para os ambientes em nuvem, em conformidade com as diretrizes internas de segurança da informação do Senac São Paulo e com a legislação aplicável, em especial a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).

3. ESCOPO DE SERVIÇO O presente Termo de Referência contempla a contratação de licenciamento de software, na modalidade de subscrição (SaaS), bem como serviços de suporte, manutenção e gerenciamento das soluções de backup e proteção de dados utilizadas pelo Senac São Paulo. A tabela a seguir apresenta os itens que compõem o escopo da contratação, com seus respectivos quantitativos e descrições..

Item	Descrição	Quant.
1	SaaS de Veeam Data Cloud for Microsoft 365 Advanced Bundle including Entra ID – Garantia e atualizações por 12 meses (H- VDCMFE-0U-R0000-00) Proteção Microsoft 365 - 4.000 Usuários Proteção Microsoft EntraID - 16.000 Usuários	n/a
2	SaaS de Veeam Data Platform Premium– Subscrição – Garantia e atualizações por 12 meses (H-VDPPRM-VV-R0000-00) Proteção de 900 Servidores Virtuais	900
3	Serviços de gerenciamento das soluções em cloud, serviço de suporte e manutenção ao ambiente por 12 meses	1

3.1. REQUISITOS PARA SOLUÇÃO VEEAM DATA PLATFORM PREMIUM 3.1.1. A contratada deverá incluir as funcionalidades de proteção (backup) e replicação integradas em uma única solução a todos os ambientes virtualizados, incluindo retorno (rollback) de réplicas e replicação desde e até a infraestrutura virtualizada. 3.1.2. A solução não deverá necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais. 3.1.3. Deverá garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através das soluções de virtualização VMware ou Hyper-V, conforme contratada. 3.1.4. Deverá ter a capacidade de realizar a replicação de dados armazenados entre storages ou máquinas de configuração e de fabricantes diferentes. 3.1.5. Deverá proteger o ambiente, sem interromper a atividade das máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção (backup) e migrações em conjunto. 3.1.6. Deverá ter a capacidade de testar a consistência do backup e replicação (S.O., aplicação, VM), emitindo relatório de auditoria para garantir a capacidade de recuperação. 3.1.7. Deverá prover a deduplicação e compressão das máquinas virtuais diretamente e durante a operação de backup. 3.1.8. Deverá ser capaz de proteger, de forma indistinta uma máquina virtual completa ou discos virtuais específicos de uma máquina virtual. 3.1.9. Deverá ser fornecida com ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador. 3.1.10. Deverá ter a capacidade de integração através de API's dos fabricantes de infraestrutura virtualizada para a proteção de dados. 3.1.11. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de "rastreamento de blocos modificados" (CBT – changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação). Deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (backup) a saber: 3.1.11.1. Direct storage access 3.1.11.2. Virtual appliance (Hot Add) 3.1.11.3. Network (NBD) 3.1.12. Deverá proporcionar um controle centralizado de implementação distribuída, para isso deverá incluir uma console web, integrada ou não, que possibilite uma visão consolidada de sua arquitetura distribuída e conjunto de múltiplos servidores de proteção e replicação, relatórios centralizados, alertas consolidados e restauração de autosserviço de máquinas virtuais no nível de sistema de arquivos (granular), com delegação de permissões sobre máquinas virtuais individuais. 3.1.13. Deverá poder manter um backup sintético, eliminando assim a necessidade de realizar backups completos (full) periódicos, incremental permanente, o que permitirá economizar tempo e espaço. 3.1.14. Deverá contar com tecnologia de deduplicação também para o ambiente de máquinas virtuais para gerar economia de espaço de armazenamento no repositório de backups sem a necessidade de hardware de terceiros (appliance deduplicadora). 3.1.15. Deverá proporcionar proteção quase contínua de dados (near-CDP), permitindo a minimização dos Objetivos de Pontos de Recuperação (RPO). 3.1.16. Deverá prover/devolver o serviço aos usuários através da inicialização da máquina virtual que falhou, diretamente do arquivo de backup, armazenado no repositório de backup de segurança, sem necessidade, inclusive de "hidratação" dos dados gravado no repositório do backup, os quais obrigatoriamente deverão estar "deduplicados" e "comprimidos". 3.1.17. Deverá permitir a recuperação de mais de uma máquina virtual e/ou ponto de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais. 3.1.18. Todo serviço de migração das máquinas virtuais do repositório de backup até o armazenamento na produção restabelecida, não deverá afetar a disponibilidade e acesso pelo usuário, sem paradas. 3.1.19. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar. 3.1.20. Deverá permitir realizar buscas rápidas mediante os índices dos arquivos que sejam controlados por um sistema operacional Windows, quando este seja o sistema operacional executado dentro da máquina virtual da qual se tenha realizado o backup. 3.1.21. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows. 3.1.22. Deverá permitir realizar a truncagem de logs transacionais

(transaction logs) para máquinas virtuais com Microsoft Exchange, SQL Server e Oracle. 3.1.23. Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos. 3.1.24. Deverá permitir recuperar no nível de objetos de qualquer aplicação virtualizada, em qualquer sistema operacional, utilizando as ferramentas de gestão das aplicações existentes. 3.1.25. Deverá incluir ferramentas de recuperação, mediante as quais os administradores de servidores de correio eletrônico, tais como Microsoft Exchange 2016 sp1 e superiores, possam recuperar objetos individuais, tais como contatos, mensagens, compromissos, anexos, entre outros, sem a necessidade de recuperar os arquivos da máquina virtual como um todo ou reiniciar a mesma. 3.1.26. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de serviços de diretório, tais como Microsoft Active Directory, possam recuperar objetos individuais, tais como usuários, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma. 3.1.27. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de banco de dados, tais como Microsoft SQL Server, possam recuperar objetos individuais, tais como bases, tabelas, registros, entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma. 3.1.28. Deverá oferecer visibilidade instantânea, capacidades avançadas de busca e recuperação rápida de elementos individuais para Microsoft Sharepoint, desde a versão 2016, sem a necessidade de agentes. (Recuperação granular). 3.1.29. Deverá incluir ferramentas de recuperação de elementos individuais para Microsoft Exchange 2016 em diante, sem que seja necessário inicializar a máquina virtual a partir do backup e que possa ser extraído a frio (ex. mensagens, tarefas, contatos etc.) e sem requerer infraestrutura intermediária (staging), fazer busca rápidas no servidor de e-mail. 3.1.30. Deverá oferecer testes automatizados de recuperação para todas as máquinas virtuais protegidas, gerando confiabilidade de 100% na execução correta das máquinas virtuais e de suas aplicações (DNS Server, Controlador de domínio, Servidor de e-mail etc.). 3.1.31. Deverá permitir criar uma cópia da máquina virtual de produção, para criação de ambiente de homologação, teste, QA etc.; em qualquer estado anterior para a resolução de problemas, provas de procedimentos, capacitação, entre outros. Deverá ser possível executar uma ou várias máquinas virtuais a partir do arquivo de backup, em um ambiente isolado, sem a necessidade de espaço de armazenamento adicional e sem modificar os arquivos de backup (read-only). 3.1.32. Deverá oferecer arquivamento em fita, suportando VTL (Virtual Tape Libraries), biblioteca de fitas e drives LTO3 ou superior, possibilitando a gravação paralela em múltiplos drives, além da criação de pools de mídia globais e pools de mídia GFS. 3.1.33. Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção. 3.1.34. Deverá ser fornecida com a funcionalidade de acelerar a rede "WAN" para geração de cópia ou replicação das máquinas virtuais, sem utilização de agentes, nem configurações de rede especiais. 3.1.35. Deverá incluir suporte para VMware vCloud Director com visibilidade integrada da infraestrutura vCD no console de backup, fazendo backup de meta-dados e dos atributos associados com vApps e VMs, permitindo a recuperação diretamente ao vCD. 3.1.36. Deverá incluir um plug-in para VMware vSphere Web Client, a fim de permitir o monitoramento da infraestrutura de backup diretamente do vSphere Web Client, com visibilidade detalhada e geral do estado dos trabalhos e recursos de backup. 3.1.37. Deverá operar em ambientes virtualizados através das soluções da VMware e Hyper-V, incluindo: VMware vSphere 7.x e Microsoft Hyper-V 2012-R2 e superiores. 3.1.38. Deverá ter a capacidade de monitoramento em tempo real, sem a necessidade de agentes, da infraestrutura virtual e de backup, inclusive máquinas virtuais, simultaneamente para Hyper-V e VMware, com notificação de problemas de backup e desempenho, com geração de alertas e base de conhecimento embutida para resolução dos mesmos. 3.1.39. Deverá ter a capacidade de monitoramento e análise de capacidade do ambiente para crescimento, ajustes e planejamentos de crescimento. 3.1.40. Deverá garantir a recuperação granular e consistente, sem necessidade de agentes adicionais para o ambiente virtualizado através das soluções acima, principalmente para os seguintes softwares: 3.1.40.1. Microsoft Active Directory Server 2016 em diante; 3.1.40.2. Microsoft Exchange Server 2016 em diante; 3.1.40.3. Microsoft SQL Server 2016 em diante; 3.1.40.4. Microsoft Sharepoint 2016 em diante; 3.1.40.5. Oracle Database 12 em diante. 3.1.41. Deverá ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos backups realizados. 3.1.42. Deverá regular de forma dinâmica e parametrizável, a exigência sobre os sistemas protegidos, de forma tal, que se possa definir limites de utilização de performance em discos para diminuir o impacto na infraestrutura de produção, durante as atividades de backup. 3.1.43. Deverá permitir um método de fácil de recuperação, desde ambientes de contingência, com as ações pré-configuradas para evitar ações manuais em caso de desastre, similar a um botão de emergência. 3.1.44. Deverá oferecer a possibilidade de armazenar os arquivos de backup de forma criptografada, com algoritmo mínimo de 256 bits, ativando e desativando tal operação, assim como assegurar o trânsito da informação através desse cenário, mesmo que impacte a performance da gravação. 3.1.45. Deverá permitir a criação de níveis de delegação de tarefas (perfis) de recuperação no nível de elementos da aplicação, inclusive para outros usuários, de forma a diminuir a carga de atividades executadas pelo administrador da plataforma. 3.1.46. Deverá dispor de funcionalidades integradas que permitam a seleção de um repositório de backup que esteja alojado em um provedor de serviços na nuvem (backup ou replicação na nuvem – cloud providers). 3.1.47. Deverá integrar uma solução unificada de monitoração de ambientes virtualizados, com fornecimento de relatórios capazes de apresentar informações do tipo: 3.1.48. Relatórios que permitam o planejamento de capacidade; 3.1.49. Relatórios que permitam determinar a ineficiência dos recursos em uso; 3.1.50. Relatórios que facilitem a visibilidade de tendências negativas e anomalias; 3.1.51. Quadros de controle claros, apresentáveis e integráveis em sites web. 3.1.52. Deverá correlacionar a execução de trabalhos de backup e réplica com os objetos do ambiente virtual. 3.1.53. Deverá oferecer a capacidade de relatar o cumprimento das políticas de proteção de dados e disponibilidade de acordo com parâmetros definidos. 3.1.54. Deve suportar múltiplas operações dos componentes/servidores participantes da estrutura de backup, permitindo atividades de backup e recuperação simultâneas; 3.1.55. Deve suportar repositório de backup com aumento de escala ilimitado para o armazenamento de dados com suporte aos seguintes sistemas de armazenamento: 3.1.55.1. Microsoft Windows; 3.1.55.2. Linux; 3.1.55.3. Pastas compartilhadas; 3.1.55.4. Appliances deduplicadoras. 3.1.56. Suportar servidores proxy de backup virtuais ou físicos para backup de máquinas virtuais; 3.1.57. Deve estar homologado para o Oracle Database 12c nos sistemas operacionais Windows ou Linux sem a necessidade de instalação de agentes; 3.1.58. Deve possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem; 3.1.59. Deve estar licenciado para utilização de no mínimo 1 biblioteca de fita com número independentemente da quantidade de drives e slots operando simultaneamente e com compartilhamento entre os jobs de backup. 3.1.60. Deve ser ofertada a versão mais atual do software de backup, liberada oficialmente pelo fabricante do software. Caso haja necessidade, por razões de compatibilidade com os demais componentes de hardware e software do ambiente de backup, a contratante se reserva o direito de utilizar a versão do software imediatamente anterior à versão mais atual, sem nenhum ônus adicional para a contratante.

3.2. REQUISITOS PARA SOLUÇÃO VEEAM DATA CLOUD FOR MICROSOFT 365

3.2.1. CARACTERÍSTICAS DA SOLUÇÃO

3.2.1.1. A solução ofertada não pode ser do tipo comunidade, software livre, ou possuir componentes e módulos sem suporte oficial do fabricante Veeam; 3.2.1.2. Deverá ser oferecida no modelo SaaS (Software como serviço), no caso Veeam Data Cloud, não necessitando de nenhuma infraestrutura local ou IaaS (Infraestrutura como serviço) para seu pleno funcionamento; 3.2.1.3. A solução SaaS (Software como serviço) Veeam Data Cloud for M365 de proteção de dados para Microsoft Office 365 deverá comprovar através de documentações oficiais a segurança física e lógica de seus data centers assim como a garantia da privacidade dos dados apresentando as certificações abaixo: i) SOC 2 Tipo II. ii) ISO/IEC 27001 iii) ISO/IEC 27012 iv) HIPAA / HITECH Tipo 2. 3.2.1.4. Cada licença ofertada deverá permitir operações de backup/restore de 100 (cem) gigabytes de Back-End (volume de dados no destino do backup) por usuário, somando-se todos os serviços Microsoft Office 365 (Exchange Online, OneDrive, SharePoint Online e Teams). A solução deve possuir política de uso justo, permitindo sem cobranças adicionais chegar a 300 (trezentos) gigabytes de Back-End por usuário. 3.2.1.5. Caso o consumo de espaço seja ultrapassado a franquia de dados, fica de responsabilidade da CONTRATADA os custos adicionais de armazenamento. 3.2.1.6. Licenciamento da solução: i) Prover licenciamento do tipo assinatura/locação pelo período de 12 meses, sendo licenciado por usuário ativo do Office 365; ii) Deverá incluir novos usuários automaticamente, iniciando cobrança de licenciamento após utilização. iii) A solução de Proteção de Dados a ser ofertada deve atender integralmente os requisitos especificados neste Termo, devendo ser fornecida com todas as licenças que forem necessárias para entrega funcional da solução; iv) Deverão ser fornecidas licenças no modelo de locação para 4000 usuários, incluindo todas as funcionalidades solicitadas para proteção de dados do Microsoft Office 365; v) Prover suporte técnico durante toda a vigência do contrato; vi) A solução proposta não deverá ter nenhum tipo de cobrança ou custo para restauração, independentemente da quantidade de dados restaurados; vii) Caso a solução possua algum tipo de cobrança para operações de restauração, o custo será de responsabilidade da CONTRATADA; viii) A solução deverá ser capaz de fazer backup e recuperar dados no Microsoft Office 365, com base em um licenciamento por usuário; ix) Todas as funcionalidades solicitadas neste documento devem estar operacionais e disponíveis durante toda a vigência da contratação; x) A solução ofertada deverá estar na versão estável mais atual do produto, não serão aceitos produtos obsoletos ou fora de linha de produção do Fabricante. xi) Durante o período de vigência do contrato o CONTRATANTE terá direito, sem ônus adicional, a todas as atualizações de versão e releases dos softwares que fazem parte da solução ofertada; xii) O fornecedor concederá à CONTRATANTE garantia integral durante o período de vigência do contrato, com atendimento 24 horas por dia e sete dias por semana, a contar da data de homologação do produto, contra qualquer defeito ou problema em toda a solução; xiii) As manutenções preventivas e corretivas serão de responsabilidade do fornecedor, sem custos adicionais ao CONTRATANTE; 3.2.2. CARACTERÍSTICA DE GERENCIAMENTO DA SOLUÇÃO

3.2.2.1. Deverá possuir uma console de gerenciamento acessível via web browser; 3.2.2.2. Suportar controle de acesso com, no mínimo, os seguintes papéis: i) Administrador geral; ii) Suporte/Operador geral; iii) Suporte/Operador limitado; iv) Auditoria; 3.2.2.3. Oferecer suporte ao mecanismo de autenticação moderna (Modern authentication) para operações de backup e suporte a autenticação multifator (MFA) para processos de restauração; 3.2.2.4. A solução deve criptografar a comunicação entre o Office 365 e a infraestrutura de backup usando SSL; 3.2.2.5. A solução deve implementar o conceito de Zero Trust possuindo mecanismos que bloqueiem a alteração/deleção de dados de backups já armazenados; 3.2.2.6. Deve possuir mecanismo que permitam limitar a origem da conexão com a console da solução. 3.2.2.7. A implementação deve permitir a configuração ou geração de políticas de backup; 3.2.2.8. Os dados de backup armazenados deverão possuir no mínimo 3 cópias localmente redundantes; 3.2.2.9. Deve possuir portal de autosserviço que permita os usuários finais executarem seus próprios processos de restauração de dados através de uma interface familiar; 3.2.2.10. Self-service restore (limitado a caixa postal e OneDrive do próprio usuário); 3.2.2.11. Deverá permitir escolher em qual país/região armazenar os dados de backup, suportando no mínimo as seguintes regiões: i) Brasil; ii) Estados Unidos; iii) Europa; 3.2.2.12. Suportar

proteção de dados de, no mínimo, os seguintes itens do Microsoft Office 365: i) MICROSOFT EXCHANGE ii) ONEDRIVE iii) SHAREPOINT iv) EQUIPES/CANAIS DO TEAMS 3.2.3. Funcionalidades de restauração 3.2.3.1. Operação de recuperação dos dados, no mínimo, nos seguintes níveis de granularidade: i) MICROSOFT EXCHANGE ii) CAIXA POSTAL COMPLETA iii) ITENS INDIVIDUAIS (PASTAS, ARQUIVOS, EMAIL, CONTATOS, CALENDÁRIO); iv) ONEDRIVE v) PASTA COMPLETA; vi) ARQUIVOS INDIVIDUAIS; vii) EQUIPES DO TEAMS viii) POSTS de CONVERSAS; x) PASTAS E ARQUIVOS INDIVIDUAIS; x) SHAREPOINT xi) SITE COMPLETO; xii) PASTAS; xiii) ARQUIVOS INDIVIDUAIS; xiv) Realizar a proteção do ambiente Microsoft Office 365, no mínimo, de 1 vez ao dia; 3.2.4. Deverá reter as imagens (backup) por todo o período de contrato sem custo adicional; 3.2.5. Para operação de recuperação de versões anteriores de um backup deverá disponibilizar, no mínimo, as seguintes formas de recuperação dos dados: 3.2.5.1. Recuperação para o local de origem; 3.2.5.2. Fazer download do arquivo; 3.2.6. Deverá criar versões referente a cada imagem (backup) executada; 3.2.7. Deve possuir mecanismo que permita comparar o conteúdo de mensagem de e-mail armazenada em backup com a versão produtiva, simplificando assim as operações de recuperação granular; 3.2.8. A solução deverá criar tarefas de backup na mesma organização do Office 365, permitindo a inclusão ou exclusão de tipos de objetos de acordo com as necessidades da organização. 3.2.9. A solução deverá ter a capacidade de procurar itens do Exchange a partir de uma interface guiada sem a necessidade de processos de recuperação anteriores; 3.2.10. A solução deve ter a capacidade de recuperar uma caixa de correio inteira ou selecionar individualmente quaisquer itens e recuperá-los para qualquer caixa de correio existente, ou exportá-los para arquivos .PST ou .EML; 3.3.SOLUÇÃO PROTEÇÃO DE ENTRA ID 3.3.1. Solução Veeam Data Cloud for Entra ID com proteção do tenant Entra ID sem necessidade de infraestrutura física local. 3.3.2. Incluir proteção de objetos como usuários, grupos e registros de aplicativos (o fornecedor deve listar a cobertura completa e limitações). 3.3.3. Permitir recuperar objetos individuais do Entra ID (ex.: usuário/grupo/applications) para suportar cenários como exclusão acidental ou alteração indevida. 3.3.4. Possibilidade de localizar itens com comparação da imagem de backup com o ambiente produtivo e executar restauração de forma direcionada (conforme recursos do portal). 3.3.5. Registro de atividades e evidências operacionais (execuções e ações de recuperação), para fins de compliance e governança. 3.3.6. Permitir administração centralizada por portal (mesmo portal Veeam Data. Cloud for M365), com visibilidade de status e falhas (e alertas/relatórios conforme capacidades contratadas). 3.3.7. Permitir exportar o conteúdo de backup, possibilitando o armazenamento dos dados em repositórios externos da solução; 3.4.SERVIÇO DE SUPORTE E GERENCIAMENTO DAS SOLUÇÕES 3.4.1. A Contratada deverá manter as instalações existentes. Em caso de impossibilidade, a mesma deverá ser responsável por todo o processo de migração do repositório de gerenciamento, proxy e de console, onde todo este processo deverá estar coberto por esse certame; 3.4.2. A Contratada terá que manter todo o histórico e as versões de recuperação já existentes desde a instalação da solução, possibilitando a recuperação de imagens de backup ainda retidos nos repositórios; 3.4.3. Custos de Transição: 3.4.3.1. A proposta comercial deverá incluir, de forma explícita e detalhada, todos os custos associados à estratégia de transição escolhida. Caso a opção seja pela Estratégia de Migração Completa, deverão ser discriminados os custos de Taxas de Saída de Dados (Egress), taxas de entrada na nuvem de destino, infraestrutura temporária e mão de obra especializada. O valor total correspondente deverá estar incluso no preço final da proposta, não sendo admitidos quaisquer pleitos ou cobranças adicionais a este título. 3.4.4. É de responsabilidade da Contratada 3.4.4.1. O gerenciamento total e ininterrupto da solução VEEAM DATA CLOUD FOR MICROSOFT 365, mantendo as versões da ferramenta atualizada conforme orientações do fabricante; 3.4.4.2. O suporte, consultoria e auxílio na resolução dos problemas (e novas implementações) na rede privada do contratante com VEEAM DATA PLATFORM PREMIUM mantendo as versões da ferramenta atualizadas conforme orientações do fabricante e suportando as rotinas de backup, replicação existentes; 3.4.4.3. Toda e qualquer atualização que possa causar interrupção nas rotinas de proteção dos ambientes, deve ser agendada junto a área de Tecnologia da Informação do Senac São Paulo (GTI); 3.4.4.4. A Contratada ficará responsável por realizar um plano de capacidade para dimensionamento correto da ferramenta, da massa de dados atual e futura para repositórios de dados, topologia e quantidade instâncias proxies para a passagem dos dados entre os serviços de nuvem e local/nuvem. Também deverá criar todas as rotinas de proteção dos dados, conforme política interna definida pelo Senac São Paulo, instalação e configuração das console de recuperação de cada serviço, incluindo a console de busca para consulta de dados; 3.4.4.5. A reunião inicial para elaboração de cronograma com prazos, datas e responsáveis pelas atividades deverá ocorrer em até 10 dias corridos, após a ordem de início; 3.4.4.6. A entrega do material gerado dessa reunião deverá ser entregue em até 5 dias, para validação pelos técnicos do Senac. 3.4.4.7. A instalação da solução deve ocorrer imediatamente após a reunião inicial. 3.4.4.8. A Contratada deverá elaborar o plano de testes e Validação, em conjunto com os técnicos do Senac, em até 10 dias após a instalação da solução. Ao final da instalação a contratada se compromete a disponibilizar toda documentação referente à instalação e configuração da solução contendo no mínimo: i) Todos os itens do Projeto; ii) Descrição do plano de implantação; iii) Características dos serviços; iv) Desenho completo da topologia utilizada; v) Descrição dos componentes da topologia; vi) Jobs a serem configurados; vii) Cenários críticos de recuperação de desastres contemplados; viii) Atividades operacionais; ix) Dados para abertura de chamados e escalation list; x) Procedimentos para interrupções programadas; 3.4.4.9. Os serviços de instalação e implementação deverão ser executados de forma a não comprometer os ambientes de produção durante o período de funcionamento do Senac, ou seja, de segunda a sexta, das 22h às 08 horas; 3.4.4.10. Após aceite do plano de implantação por parte do Senac São Paulo, a Contratada deve instalar e configurar o produto, permitindo ao Senac SP executar as novas rotinas de cópia de segurança, a serem apresentadas no formato de política de backup; 3.4.4.11. A Contratada deve auxiliar o Senac SP na atualização da política de backup, apresentando as melhores práticas de mercado, as práticas que melhor se adequem a realidade do Senac SP e do software de cópias de segurança desta contratação; 3.4.4.12. Todos os ambientes computacionais e elementos da topologia de backup do Senac SP devem estar integrados e administrados em uma console única, já customizadas as políticas de acesso conforme orientação da área de SI do Senac SP. 3.4.4.13. Contratada do software de backup deverá ser responsável por configurar o acesso e utilização de robôs de backup presentes no ambiente do Senac, indexando e catalogando os dados no software ofertado, quando solicitado pela equipe técnica do Senac SP, realizando testes de backup, restore e replicação à critérios do Senac SP, a fim de validar o bom funcionamento do serviço realizado. 3.4.4.14. Um cronograma detalhado em arquivo em formato MS-Project digital e formato PDF deverá ser entregue pela Contratada até 5 (cinco) dias úteis após o início do projeto. Suas atualizações deverão ser entregues pelo Gerente do Projeto semanalmente no último dia útil de cada semana, refletindo a realidade das atividades executadas até o momento. 3.4.4.15. O projeto deverá ser executado seguindo as etapas abaixo: i) Planejamento; ii) Implantação; iii) Testes; iv) Treinamento e documentação; v) Migração; vi) Operação assistida. 3.5.SERVIÇOS SUPORTE TÉCNICOS ESPECIALIZADOS PARA A SOLUÇÃO VEEAM DATA PLATFORM PREMIUM 3.5.1. Os serviços de suporte técnico, manutenção e atualização de versões devem ser prestados por 12 (doze) meses aos produtos: 3.5.1.1. VEEAM DATA PLATFORM PREMIUM, incluindo VEEAM ONE 3.5.1.2. Disponibilização e instalação assistida de novas versões; 3.5.1.3. Disponibilização e instalação assistida de atualizações críticas e não críticas, corretiva e evolutiva; 3.5.1.4. Relatórios pós atualizações e atualizações de versão; 3.5.1.5. Acesso web ou telefone para permitir a abertura de chamados; 3.5.1.6. Acesso a base de conhecimento / fórum da(s) ferramenta(s). 3.5.1.7. Todos os chamados técnicos, serão direcionados para a Contratada, à qual caberá analisar o problema relatado e acionar, caso seja necessário, o fabricante, respeitados o Acordo de Níveis de Serviços estabelecidos. 3.5.1.8. O suporte técnico deverá ser prestado segundo as seguintes condições, entre outras: i) Ajustes na topologia; ii) Atualizações de versões; iii) Ativação de novas funcionalidades; iv) Troubleshooting; v) Melhorias no ambiente; vi) O suporte será, obrigatoriamente, presencial; vii) A contratada deverá disponibilizar telefone local São Paulo ou 0800 e e-mail para abertura de chamados técnicos em horário 24X7, ou seja, 24 horas por dia e 7 dias por semana), durante o período de 12 meses. viii) Direito a um número ilimitado de solicitações de suporte; 3.5.2. Cada chamado deverá conter, no mínimo, o registro das informações abaixo: 3.5.2.1. Número do registro/ocorrência (a ser fornecido pela Contratada); 3.5.2.2. Identificação do atendente; 3.5.2.3. Identificação do solicitante; 3.5.2.4. Data e hora da solicitação; 3.5.2.5. Descrição da ocorrência; 3.5.2.6. Data e hora da solução e fechamento do chamado. 3.5.2.7. Relatório de fechamento de chamado. 3.5.2.8. O horário da abertura do chamado será a data e hora da ligação realizada pelo profissional do Senac informando o problema ocorrido. Caso o atendente não possa informar o número de chamado neste momento, o mesmo deverá, obrigatoriamente, informar um número de Protocolo que registre a data e hora da ligação realizada. 3.5.2.9. O horário de abertura do chamado marcará o início da contagem do prazo de atendimento e solução das ocorrências (SLA), independente do retorno da Contratada. 3.5.2.10. O suporte técnico deverá ser acionado em caso de qualquer indisponibilidade da solução, devendo ter como objetivos de atendimento, os índices de criticidade a seguir:

Severidade	Descrição	SLA de meta de resposta de produção
	Tarefa de backup primária - tarefas de backup concluídas a partir dos dados de produção da fonte	
	Tarefa de backup secundária - tarefas de backup redundantes das tarefas de backup primárias enviadas para locais secundários (fita, cópia de backup, storage de objetos etc.).	

Severidade 1	Dados de produção perdidos precisam ser restaurados com urgência usando um ou mais produtos da Veeam	1 hora
	Incapacidade de acessar a interface de usuário de um ou mais produtos da Veeam, o que levaria à perda total de controle sobre as tarefas de backup, replicação e restauração	
	Nenhuma tarefa de backup e replicação está operando dentro de uma aplicação Veeam inteira que faz o backup de vários servidores ou ambientes	
	O uso normal dos produtos da Veeam resulta em falhas inesperadas dos sistemas de infraestrutura de produção	
	Tarefas de recuperação com falha, resultando em violações de conformidade normativa definidas por um sistema ou entidade governamental reconhecidos	
	Os pontos acima não têm solução provisória imediata ou solução disponível	
	Exemplos: Interrupções anormais e excessivas que afetam todo o monitoramento, backups e agendamentos ou um sistema de produção inativo/off-line que não pode ser restaurado; falha de aplicação ou sistema causada por um produto da Veeam.	
Severidade 2	Impacto negativo em várias tarefas do backup primário, mas o sistema de produção não está desativado	3 horas
	As operações de produção são afetadas, mas o impacto é limitado	
	Tarefas de monitoramento para coleta de informações da infraestrutura estão falhando	
	Exemplos: Tempos de resposta da aplicação ou desempenho do sistema estão criticamente lentos ou tarefas primárias de backup ou monitoramento são afetadas.	
Severidade 3	Falhas limitadas em tarefas de backup primário	6 horas
	Falhas em tarefas de backup secundário	
	As operações de verificação de recuperação não são bem-sucedidas	
	As tarefas de monitoramento para coletar informações de componentes da Veeam estão falhando	
	Exemplos: Tempos de resposta da aplicação ou desempenho do sistema estão degradados, ou tarefas de backup secundário ou monitoramento são afetadas.	
Severidade 4	Problema ou questão menor que não afeta a função do produto e pode ser contornada facilmente.	8 horas
	A resolução do problema é classificada como não prioritária pelos usuários do software.	
	Exemplos: Perguntas de "como fazer", o texto de uma mensagem ou página da documentação está mal redigido ou tem erro de grafia, comentários gerais ou a resolução do problema não é sensível ao tempo.	

3.5.3. A Contratada deverá disponibilizar 1152 horas para uso em

consultoria, on site, sendo requerido um recurso especialista na ferramenta, onde serão utilizados durante a vigência do período de contrato. Este recurso será utilizado para que a equipe Senac absorva o conhecimento de operação junto especialista, e que o mesmo possa garantir a estabilidade do ambiente. 3.5.3.1. As horas de consultoria deveram ser divididas em 24h semanais, sendo acordados previamente, os dias que o consultor deverá comparecer, as agendas de atividades / RDMS, que demandem trabalhos fora do horário comercial, podendo ser usadas em finais de semanas ou feriados. 3.5.4. As atividades que necessitem execução ou acompanhamento fora do horário comercial serão agendadas com no mínimo 15 (quinze) dias de antecedência através de GMUD e não devem superar 20% das horas de consultoria no item 5.2. 3.5.5. O recurso deverá estabelecer, acompanhar e intermediar toda e qualquer comunicação com o fabricante da solução ofertada. 3.5.6. O recurso deverá possuir certificação técnica oficial do fabricante da solução ofertada. 3.5.7. Este recurso deve ter a capacidade para administrar o ambiente, assim como realizar customizações nos itens abaixo para que o ambiente possa se manter estável e performático: 3.5.7.1. Criação de scripts pré e pós backup; 3.5.7.2. Customização de scripts junto aos DBAs da contratante para rotinas de backup específicas; 3.5.7.3. Criação de relatórios customizados na ferramenta de replicação; 3.5.7.4. Customização / parametrização do software de monitoramento Veeam One para as métricas informadas pelos analistas responsáveis da contratante. 3.5.7.5. Criação de rotinas de certificação da integridade dos dados (Sure Backup / Sure Replica) junto aos analistas das principais aplicações do Senac São Paulo. 3.5.7.6. Criação de regras e cenários adicionais para o funcionamento da função de VirtualLab. 3.5.7.7. Criação de Relatório de capacidade para ambiente e componentes de backup e de replicação; 3.5.7.8. Criação de Relatório do tipo saúde do ecossistema (health check) de backup e de replicação; 3.5.7.9. Criação de Relatórios de métricas e de sla para a replicação, como Recovery Point Objective (RPO) e Recovery Time Objective (RTO); 3.5.7.10. Criação de Relatório de ajustes e melhorias possíveis no ambiente; 3.5.7.11. Criação de um calendário para validações semanal da rotina de replicação de certificar a subida de ambiente crítico em site secundário do contratante, para fins de auditoria interna do contratante; 3.6. SERVIÇOS SUPORTE TÉCNICOS ESPECIALIZADO PARA A SOLUÇÃO VEEAM DATA CLOUD 3.6.1. Os serviços de suporte técnico, manutenção e atualização de versões devem ser prestados por 12 (doze) meses à solução: 3.6.1.1.

Veeam Data Cloud para Microsoft 365 3.6.1.2. Veeam Data Cloud para Entra ID 3.6.2. Acesso ao site do fabricante para permitir a abertura de chamados; 3.6.3. Acesso a base de conhecimento / fórum da ferramenta. 3.6.4. Todos os chamados técnicos, serão direcionados para a Contratada, à qual caberá analisar o problema relatado e acionar, caso seja necessário, o fabricante, respeitados o Acordo de Níveis de Serviços estabelecidos. 3.6.5. O suporte técnico deverá ser prestado segundo as seguintes condições, entre outras: 3.6.5.1. Ativação de novas funcionalidades; 3.6.5.2. Troubleshooting; 3.6.6. O suporte será, obrigatoriamente, presencial; 3.6.7. A contratada deverá disponibilizar telefone número local São Paulo ou 0800 e e-mail para abertura de chamados técnicos em horário 24X7, ou seja, 24 horas por dia e 7 dias por semana), durante o período de 12 meses. 3.6.8. Direito a um número ilimitado de solicitações de suporte; 3.6.9. Cada chamado deverá conter, no mínimo, o registro das informações abaixo: 3.6.9.1. Número do registro/ocorrência (a ser fornecido pela Contratada); 3.6.9.2. Identificação do atendente; 3.6.9.3. Identificação do solicitante; 3.6.9.4. Data e hora da solicitação 3.6.9.5. Descrição da ocorrência; 3.6.9.6. Data e hora da solução e fechamento do chamado. 3.6.9.7. Relatório de fechamento de chamado. 3.6.9.8. O horário da abertura do chamado será a data e hora da ligação realizada pelo profissional informando o problema ocorrido. Caso o atendente não possa informar o número de chamado neste momento, o mesmo deverá, obrigatoriamente, informar um número de Protocolo que registre a data e hora da ligação realizada. 3.6.9.9. O horário de abertura do chamado demarcará o início da contagem do prazo de atendimento e solução das ocorrências (SLA), independente do retorno da Contratada. 3.7. MONITORAMENTO E RELATÓRIOS 3.7.1. A solução deverá fornecer uma interface para exibir as estatísticas dos objetos processados em cada sessão de backup; 3.7.2. Deverá permitir enviar notificações sobre os resultados das tarefas de backup por e-mail ou disponibilizadas em uma central de notificações; 3.7.3. Disponibilizar logs de auditoria para as operações dos usuários realizadas na plataforma; 3.7.4. Deve possuir dashboard ou relatório que liste a quantidade de usuários protegidos; 3.7.5. Deve possuir dashboard ou relatório que liste a quantidade de licenças consumidas; 3.7.6. Deve possuir dashboard ou relatório que liste a quantidade de armazenamento consumido; 3.7.7. Deve possuir integração com Syslog Server (SIEM); 3.7.8. Deverá prover notificações de backup e Restore através de Email e canal do Teams dedicado. 3.8. DEVERES E RESPONSABILIDADES DA CONTRATANTE 3.8.1. Acompanhar, fiscalizar e conferir o objeto contratual; 3.8.2. Proporcionar todas as facilidades para que a Contratada possa efetuar os serviços dentro das normas estabelecidas no contrato; 3.8.3. Permitir livre acesso dos funcionários da Contratada aos equipamentos, objeto deste termo de referência, para execução dos serviços de instalação, manutenção, garantia e assistência técnica; 3.8.4. Prestar informações e esclarecimentos que venham a ser solicitados pela Contratada; 3.8.5. Comunicar a Contratada as irregularidades observadas na execução do contrato; 3.8.6. Não consentir que terceiro sem autorização execute os serviços de instalação, manutenção, garantia e assistência técnica; 3.8.7. Assegurar aos técnicos credenciados pela Contratada o acesso aos equipamentos para efetuarem o serviço, resguardadas todas as necessidades de sigilo e segurança, bem como dependerá de autorização da Contratada toda e qualquer intervenção nos equipamentos do Senac SP; 3.8.8. Solicitar a correção de defeitos; 3.8.9. Notificar a Contratada sobre imperfeições, falhas ou irregularidades constatadas, para que sejam adotadas as medidas necessárias. 3.8.10. Notificar a Contratada, por escrito, garantida a prévia defesa, sobre aplicação de penalidades em caso de descumprimento total ou parcial do contrato; 3.8.11. Receber os bens e serviços entregues pela Contratada, desde que estejam em conformidade com o objeto contratado. 3.9. DEVERES E RESPONSABILIDADES DA CONTRATADA 3.9.1. Cumprir fielmente as obrigações assumidas no edital de licitação, no contrato e na proposta, de forma que os serviços sejam realizados com esmero e perfeição; 3.9.2. Assegurar a manutenção, suporte técnico e operacional necessários ao pleno e perfeito funcionamento do software, efetuando os ajustes ou reparos para o bom uso da ferramenta, sem qualquer ônus para o Senac 3.9.3. Disponibilizar para download, durante o prazo de vigência contratual, todas as atualizações corretivas, evolutivas, de segurança e releases referentes ao software ofertado, sem quaisquer ônus adicionais para o Senac, num prazo máximo de 15 (quinze) dias corridos, contados da data da atualização ou releases; 3.9.4. As versões do software ofertado devem continuar a ter garantia de perfeito funcionamento e de correções, durante o prazo de manutenção e suporte técnico, mesmo após lançamento de novas versões, até que os mesmos sejam descontinuados; 3.9.5. Providenciar junto à Gerência de Tecnologia da Informação no Senac SP, a identificação dos seus empregados; 3.9.6. Manter, durante o período de vigência do contrato, todas as condições que ensejaram a contratação; 3.9.7. Assumir todos os gastos e despesas que se fizerem necessários para o cumprimento do Contrato, tais como: recursos humanos, ferramentas, transportes, fretes, hardwares, acessórios ou qualquer outro insumo que venham a surgir sem ônus para o Senac SP; 3.9.8. A Contratada disponibilizará para o Senac acesso a central de atendimento (suporte técnico), 3.9.9. Responsabilizar-se pelo bom cumprimento de todo o serviço relacionado ao objeto deste termo de referência, mesmo que em parte tenha sido subcontratado, zelando pela boa qualidade de qualquer das prestações de serviço a que está obrigada; 3.9.10. A Contratada deve manter sigilo de todos os dados ou informações do Senac ou de suas representações obtidas em função da prestação do serviço contratado, devendo assinar termo de confidencialidade, presente em um dos anexos deste documento; 3.9.11. A contratada concede ao Senac São Paulo o direito de uso dos artefatos, documentos, relatórios e procedimentos produzidos no âmbito da prestação dos serviços, para fins institucionais, não implicando cessão de direitos de propriedade intelectual sobre softwares ou soluções de terceiros utilizados na contratação.; 3.10. TRANSFERÊNCIA DE CONHECIMENTO 3.10.1. Após a instalação da solução e ateste dos serviços de instalação, deverá ocorrer a transferência de conhecimento, para os técnicos; 3.10.2. O repasse de conhecimento deverá ser realizado nas dependências da gerência de Tecnologia e Informação, em calendário a ser definido conjuntamente entre a área técnica e a contratada, o mesmo deverá abranger duas turmas de (até) 03 (três) pessoas, a serem definidas pela contratante, e deve ser ministrado um treinamento de 20 (vinte) horas, por turma; 3.10.3. O treinamento deverá ocorrer em São Paulo, nas dependências da contratante (Senac); 3.10.4. O material utilizado para o repasse de conhecimento deverá ter caráter orientado a operação do software ofertado e poderá estar em língua portuguesa ou inglesa. 4. PRAZOS 4.1. As licenças deverão estar disponíveis por e-mail, ou site do Fabricante para visualização e uso, em até 15 dias úteis a partir do recebimento do Acordo de Compra, e as licenças deverão ser providas como serviço ao Senac São Paulo por intermédio da contratada no modelo de cobrança anual por meio de parcela única. 4.2. Todos os softwares e serviços aqui ofertados deverão, obrigatoriamente, ter suporte e garantia por 12 meses. 4.3. Modelo de proposta: Conforme mencionado acima. De acordo com o edital, termo de referência e seus anexos.

Prazo de Validade da Proposta	Conforme Edital
Local de Entrega	Conforme Edital
Prazo de entrega	Conforme Edital
Dados Bancários	Banco SICOOB: AGÊNCIA: 4101 – CONTA: 16.731.001-1
Garantia	Conforme Edital
Procedência dos objetos	Conforme Edital
Assistência Técnica	Conforme Edital
Termo de Garantia	Conforme Edital

I – DA PROPOSTA E DO OBJETO

A presente proposta comercial está integralmente em conformidade com o objeto, as especificações e as condições estabelecidas no Termo de Referência do respectivo processo licitatório. Os preços ofertados incluem todos os custos diretos e indiretos necessários ao cumprimento integral do objeto, tais como tributos, encargos sociais e trabalhistas, fretes, seguros, despesas administrativas e operacionais, não havendo qualquer ônus adicional à Administração.

II – DOS PRAZOS O prazo de início do fornecimento, entrega dos equipamentos e/ou execução dos serviços obedecerá ao disposto no Termo de Referência do processo, contado a partir do recebimento da Ordem de Fornecimento, Ordem de Serviço ou instrumento equivalente emitido pelo órgão contratante. Os produtos e equipamentos fornecidos estarão serão novos, de primeiro uso e em conformidade com as especificações técnicas do Termo de Referência, quando aplicável ao objeto da contratação.

III – DAS CONDIÇÕES JURÍDICAS E DE HABILITAÇÃO

Não possui qualquer impedimento legal para contratar com a Administração Pública, nos termos do art. 14 da Lei nº 14.133/2021, declarando não se enquadrar em nenhuma das hipóteses de vedação ali estabelecidas. Não foi declarada inidônea para licitar ou contratar com o Poder Público, em nenhuma esfera, e não está suspensa de participar de licitações ou impedia de contratar com órgãos ou entidades da Administração Pública Cumpre todas as exigências de habilitação jurídica, técnica, fiscal, social e econômico-financeira estabelecidas no instrumento convocatório.

IV – DAS OBRIGAÇÕES TRABALHISTAS E LEGAIS A presente proposta contempla a integralidade dos custos para atendimento dos direitos trabalhistas assegurados pela Constituição Federal, pela Consolidação das Leis do Trabalho (CLT), pelas normas infralegais e pelas convenções e acordos coletivos de trabalho vigentes na data de sua apresentação. Cumpre as normas relativas à saúde e segurança do trabalho, bem como as disposições da legislação previdenciária aplicáveis ao objeto contratado.

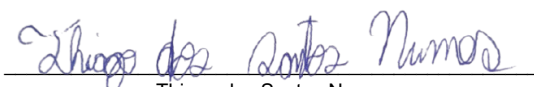
V – DEMAIS DECLARAÇÕES

As informações prestadas nesta proposta são verídicas e de inteira responsabilidade desta empresa, estando ciente de que a prestação de informações falsas configura infração sujeita às sanções previstas no art. 155 e seguintes da Lei nº 14.133/2021. Concorde integralmente com as condições estabelecidas no instrumento convocatório, sem qualquer ressalva ou condicionante. Em atendimento às disposições do Edital e com o objetivo de preservar o anonimato do licitante durante a fase de apresentação da proposta inicial, informa-se que os dados de identificação da empresa, bem como quaisquer outras informações que possam revelar sua identidade, serão apresentados oportunamente, após o encerramento da fase competitiva e mediante solicitação do Pregoeiro ou da Comissão de Contratação, em conformidade com as regras do certame. A presente medida visa exclusivamente resguardar o sigilo da identidade do licitante nesta etapa do procedimento, evitando eventual desclassificação por identificação indevida da proposta.

Obs.:

- 1) Validade da Proposta: **90 dias**;
- 2) Condições de Pagamento: **28 dias** após a entrega das licenças.
- 3) Prazo de entrega: **15 dias uteis** após o recebimento do acordo de compra.
- 4) Local de Entrega: Conforme Termo de Referência.
- 5) Dados da empresa que efetuará o faturamento: Razão Social: MGDATA TECNOLOGIA LTDA; Endereço: Rua Caetés, 13 | CEP: 35.680-262 | Bairro: Piedade | Município: Itaúna | Estado: Minas Gerais; CNPJ Nº: 23.936.997/0001-91 | Inscrição Estadual Nº: 002684432.00-60; Contato: (37) 3242 – 2122 | E-mail: licitacao@mgdata.com.br.

26 de junho de 2026.


Thiago dos Santos Nunes
Proprietário | Diretor

「 23 936 997/0001-91 」
MGDATA TECNOLOGIA
LTDA.
Rua Caetés, 13
B. Piedade – CEP 35680-262
「 ITAÚNA – MINAS GERAIS 」