

PROPOSTA COMERCIAL

PREGÃO ELETRÔNICO – PEE 2025000020

Objeto: Renovação de licenças das soluções Veeam de Backup, suporte e manutenção do ambiente de replicação / recuperação, local e remoto e monitoramento via Veeam One e Veeam Backup for Microsoft 365 para proteção do ambiente de dados em nuvem Microsoft 365 com armazenamento em Cloud.

SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL | ADMINISTRAÇÃO REGIONAL NO ESTADO DE SÃO PAULO – SENAC SP

Apresentamos proposta comercial, nos seguintes termos:

ITEM	ESPECIFICAÇÃO	QUANT.	VALOR MENSAL	VALOR TOTAL 12 MESES
1	Renovação SaaS de Veeam Availability Suite Enterprise Plus – <u>VCSP Rental</u> – 900 Servidores Virtuais – Garantia e atualizações por 12 meses.	900 VMs	R\$ 1.550.000,00	R\$ 18.600.000,00
2	Contratação SaaS de Veeam Backup para Microsoft 365 – <u>VCSP- Rental</u> – Garantia e atualizações por 12 meses	4000 Usuários	R\$ 1.350.000,00	R\$ 17.550.000,00
3	Serviços de armazenamento dos dados de backup em nuvem, gerenciamento das soluções locais e em cloud, serviço de suporte e manutenção ao ambiente por 12 meses.	1	R\$ 1.200.000,00	R\$ 14.400.000,00
<p>1. REQUISITOS PARA SOLUÇÃO VEEAM AVAILABILITY ENTERPRISE PLUS</p> <p>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.</p> <p>1.2. A solução não deverá necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais.</p> <p>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.</p> <p>1.4. Deverá ter a capacidade e realizar a replicação de dados armazenados entre storages ou máquinas de configuração e de fabricantes diferentes.</p> <p>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.</p> <p>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.</p> <p>1.7. Deverá prover a de duplicação e compressão das máquinas virtuais diretamente e durante a operação de backup.</p> <p>1.8. Deverá ser capaz de proteger, de forma indistinta uma máquina virtual completa ou discos virtuais específicos de uma máquina virtual.</p> <p>1.9. Deverá ser fornecida com ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador.</p> <p>1.10. Deverá ter a capacidade de integração através de API's dos fabricantes de infraestrutura virtualizada para a proteção de dados.</p> <p>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).</p> <p>1.12. Deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (backup) a saber:</p> <p>1.12.1. Direct storage access</p> <p>1.12.2. Virtual appliance (Hot Add)</p> <p>1.12.3. Network (NBD)</p> <p>1.13. 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.</p> <p>1.14. 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.</p> <p>1.15. 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).</p> <p>1.16. Deverá proporcionar proteção quase contínua de dados (near-CDP), permitindo a minimização dos Objetivos de Pontos de Recuperação (RPO).</p> <p>1.17. 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 também "comprimidos".</p> <p>1.18. 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.</p> <p>1.19. 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.</p> <p>1.20. 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.</p> <p>1.21. 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.</p> <p>1.22. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.</p> <p>1.23. Deverá permitir realizar a truncagem de logs transacionais (transaction logs) para máquinas virtuais com Microsoft Exchange, SQL Server e Oracle.</p> <p>1.24. Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos.</p> <p>1.25. Deverá permitir recuperar no nível de objetos de qualquer aplicação virtualizada, em qualquer sistema operacional, utilizando as ferramentas de gestão das aplicações existentes.</p> <p>1.26. Deverá incluir ferramentas de recuperação, mediante as quais os administradores de servidores de correio eletrônico, tais como Microsoft Exchange 2010 sp1, 2013 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.</p> <p>1.27. 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.</p> <p>1.28. 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.</p> <p>1.29. Deverá oferecer visibilidade instantânea, capacidades avançadas de busca e recuperação rápida de elementos individuais para Microsoft Sharepoint, desde a versão 2010, sem a necessidade de agentes. (Recuperação granular).</p> <p>1.30. 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 rápida no servidor de e-mail.</p> <p>1.31. 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.).</p> <p>1.32. 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).</p> <p>1.33. 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.</p> <p>1.34. Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção.</p> <p>1.35. 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.</p> <p>1.36. 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.</p> <p>1.37. 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.</p>				

- 1.38. Deverá operar em ambientes virtualizados através das soluções da VMware e Hyper-V, incluindo: VMware vSphere 7.x e Microsoft Hyper-V 2008-R2 e superiores.
- 1.39. 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.
- 1.40. Deverá ter a capacidade de monitoramento e análise de capacidade do ambiente para crescimento, ajustes e planejamentos de crescimento.
- 1.41. 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:
- 1.41.1. Microsoft Active Directory Server 2016 em diante;
- 1.41.2. Microsoft Exchange Server 2016 em diante;
- 1.41.3. Microsoft SQL Server 2008 em diante;
- 1.41.4. Microsoft Sharepoint 2010 em diante;
- 1.41.5. Oracle Database 12 em diante.
- 1.42. Deverá ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos backups realizados.
- 1.43. 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.
- 1.44. 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.
- 1.45. 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.
- 1.46. 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.
- 1.47. 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).
- 1.48. Deverá integrar uma solução unificada de monitoração de ambientes virtualizados, com fornecimento de relatórios capazes de apresentar informações do tipo:
- 1.48.1. Relatórios que permitam o planejamento de capacidade;
- 1.48.2. Relatórios que permitam determinar a ineficiência dos recursos em uso;
- 1.48.3. Relatórios que facilitem a visibilidade de tendências negativas e anomalias;
- 1.48.4. Quadros de controle claros, apresentáveis e integráveis em sites web.
- 1.49. Deverá correlacionar a execução de trabalhos de backup e réplica com os objetos do ambiente virtual.

2. REQUISITOS PARA SOLUÇÃO VEEAM BACKUP FOR MICROSOFT 365

- 2.1. A solução deve suportar em modo de produção, o backup, e recuperação dos dados de usuários em nuvem Microsoft para os aplicativos:
- 2.1.1. Exchange Online;
- 2.1.2. SharePoint Online;
- 2.1.3. OneDrive for Business;
- 2.1.4. Microsoft Teams.
- 2.2. Possibilitar o gerenciamento e proteção de dados em sistema híbrido (ambientes locais e em nuvem);
- 2.3. Ser escalável, permitindo múltiplos repositórios e em diversas localidades;
- 2.4. Disponibilizar serviços de customização / automação via API RESTful e PowerShell;
- 2.5. Deve poder atender a requisitos de segurança e conformidade como:
- 2.5.1. Armazenar dados com base em políticas de retenção de longo prazo para fins regulatórios ou de conformidade;
- 2.5.2. Garantir que a empresa recupere exatamente o que precisa, como e-mails, itens de calendário e inclusive a mailbox como um todo;
- 2.5.3. Permitir a recuperação direta dos dados para a nuvem do Microsoft365;
- 2.5.4. Dispor de recurso para pesquisa avançada (eDiscovery) e granular;
- 2.5.5. Pesquisa rápida e recuperação granular de objetos individuais;
- 2.5.6. Possibilitar segurança dos dados de backup do Microsoft365 com autenticação multi fator.

3. SERVIÇO DE SUPORTE E GERENCIAMENTO DAS SOLUÇÕES

- 3.1. A Contratada deverá manter as instalações existentes. Em caso de impossibilidade, a mesma deverá ser responsável por todo o processo de migração do repositório atual, instâncias de gerenciamento, proxy e de console, onde todo este processo deverá estar coberto por esse certame;
- 3.2. A Contratada terá que manter todo o histórico e as versões de recuperação já existentes desde a instalação da solução, possibilitando a recuperação pelo período de 3 anos ininterruptos (Microsoft365);
- 3.3. É de responsabilidade da Contratada:
- 3.3.1. O gerenciamento total e ininterrupto da infraestrutura e da solução VEEAM BACKUP FOR MICROSOFT 365, mantendo as versões da ferramenta atualizada conforme orientações do fabricante;
- 3.3.2. O suporte, consultoria e auxílio na resolução dos problemas (e novas implementações) na rede privada do contratante com VEEAM AVAILABILITY SUITE ENTERPRISE PLUS mantendo as versões da ferramenta atualizada conforme orientações do fabricante e suportando as rotinas de backup, replicação existentes;
- 3.4. 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);
- 3.5. 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 proxy's 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 eDiscovery para consulta de dados;
- 3.6. 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;
- 3.7. A entrega do material gerado dessa reunião deverá ser entregue em até 5 dias, para validação pelos técnicos do Senac.
- 3.8. A instalação da solução deve ocorrer imediatamente após a reunião inicial.
- 3.9. 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:
- 3.9.1. Todos os itens do Projeto;
- 3.9.2. Descrição do plano de implantação;
- 3.9.3. Características dos serviços;
- 3.9.4. Desenho completo da topologia utilizada;
- 3.9.5. Descrição dos componentes da topologia;
- 3.9.6. Jobs a serem configurados;
- 3.9.7. Cenários críticos de recuperação de desastres contemplados;
- 3.9.8. Atividades operacionais;
- 3.9.9. Dados para abertura de chamados e escalation list;
- 3.9.10. Procedimentos para interrupções programadas;
- 3.10. 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;
- 3.11. 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 a Contratada no formato de política de backup;
- 3.12. 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;
- 3.13. 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.
- 3.14. A 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.

3.15. 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.

3.15.1. O projeto deverá ser executado seguindo as etapas abaixo:

3.15.1.1. Planejamento;

3.15.1.2. Implantação;

3.15.1.3. Testes;

3.15.1.4. Treinamento e documentação;

3.15.1.5. Migração;

3.15.1.6. Operação assistida.

4. ARMAZENAMENTO EM NUVEM PRIVADA

4.1. O backup deverá ser realizado em uma solução do fornecedor que suporte o volume de 85 terabytes de espaço livre para armazenamento da solução Microsoft365;

4.2. O ambiente deve ter estabilidade de 99,99%, não será permitindo nenhuma parada por queda de energia;

4.3. Se faz necessário a elasticidade e o escalonamento do volume se houver necessidade de crescimento espontâneo ou programado para que não tenha interrupção do ambiente em até 15% do volume contratado;

4.3.1. Deve ser disponibilizado em até 30 minutos eventual crescimento;

4.4. Os dados devem permanecer em ambiente privado dentro do território nacional, seguindo a lei de proteção de dados;

4.5. Deve ser disponibilizado uma console web para administração do Senac;

4.6. A console deve ter níveis hierárquicos diferentes, para administradores e usuários;

4.7. Os volumes do storage não podem ser compartilhados com outras empresas;

4.8. Deve contemplar 2 servidores virtuais sendo cada com 8CPUs e 32GB RAM para administração da solução;

4.9. A política de retenção e backup são de responsabilidade do Senac e a empresa vencedora deve seguir essas regras;

4.10. O Disco de armazenamento não pode ser superior a 14TB cada, e cada conjunto de discos deve ter a proteção e redundância em RAID 01;

4.11. Os serviços de download e upload de dados para este repositório devem constar nos valores apresentados, sem custo adicional ao Senac, e sem limite de transferências mensais.

5. SERVIÇOS SUPORTE TÉCNICOS ESPECIALIZADOS PARA AS SOLUÇÕES

5.1. Os serviços de suporte técnico, manutenção e atualização de versões devem ser prestados por 12 (doze) meses aos produtos:

5.1.1. Veeam Availability Suite Enterprise Plus

5.1.2. Veeam One

5.1.3. Veeam Backup para Microsoft365

5.2. Disponibilização e instalação assistida de novas versões;

5.3. Disponibilização e instalação assistida de atualizações críticas e não críticas, corretiva e evolutiva;

5.4. Relatórios pós atualizações e atualizações de versão;

5.5. Acesso ao site do fabricante para permitir a abertura de chamados;

5.6. Acesso a base de conhecimento / fórum da ferramenta.

5.7. 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.

5.8. O suporte técnico deverá ser prestado segundo as seguintes condições, entre outras:

5.8.1. Ajustes na topologia;

5.8.1.1. Atualizações de versões;

5.8.1.2. Ativação de novas funcionalidades;

5.8.1.3. Troubleshooting;

5.8.1.4. Melhorias no ambiente;

5.8.1.5. O suporte será, obrigatoriamente, presencial;

5.8.2. 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.

5.8.3. Direito a um número ilimitado de solicitações de suporte;

5.8.4. Cada chamado deverá conter, no mínimo, o registro das informações abaixo:

5.8.4.1. Número do registro/ocorrência (a ser fornecido pela Contratada);

5.8.4.2. Identificação do atendente;

5.8.4.3. Identificação do solicitante;

5.8.4.4. Data e hora da solicitação;

5.8.4.5. Descrição da ocorrência;

5.8.4.6. Data e hora da solução e fechamento do chamado.

5.8.4.7. Relatório de fechamento de chamado.

5.8.5. 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.

5.8.6. 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.

5.8.7. 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:

Criticidade	Descrição	Atendimento	Resolução do Problema
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados. Exemplos: serviço inativo.	Em até 01 hora	Em até 04 horas
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade, a curto prazo, possa ser afetada negativamente. Exemplo: Servidor não responde a comandos ou responde com resultados inesperados. Arquivos de log corrompidos ou inexistentes.	Em até 3 horas	Em até 06 horas
Severidade 3 (Baixa)	Demais problemas que não afetem diretamente o ambiente de produção. Exemplos: Problemas na geração de relatórios, dúvidas gerais de operação / configuração.	No mesmo dia ou NBD	Em até 24 horas

5.9. A Contratada deverá disponibilizar 576 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, este especialista deve seguir aos solicitados:

5.9.1. As horas de consultoria deveram ser divididas em 12h semanais, sendo acordados previamente, os dias que o consultor deverá comparecer, as agendas de atividades / RDMS, que demandem trabalhos fora do horário comercial.

5.9.2. 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 4.9.

5.9.3. O recurso deverá estabelecer, acompanhar e intermediar toda e qualquer comunicação com o fabricante da solução ofertada.

5.9.4. O recurso deverá possuir certificação técnica oficial do fabricante da solução ofertada.

5.9.5. 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:

5.9.5.1. Criação de scripts pré e pós backup;

5.9.5.2. Customização de scripts junto aos DBAs da contratante para rotinas de backup específicas;

5.9.5.3. Criação de relatórios customizados na ferramenta de replicação;

5.9.5.4. Customização / parametrização do software de monitoramento Veeam One para as métricas informadas pelos analistas responsáveis da contratante.

5.9.5.5. Criação de rotinas de certificação da integridade dos dados (Sure Backup / Sure Replica) junto aos analistas das principais aplicações do Senac São Paulo.

5.9.5.6. Criação de regras e cenários adicionais para o funcionamento da função de VirtualLab.

5.9.5.7. Criação de Relatório de capacidade para ambiente e componentes de backup e de replicação;

5.9.5.8. Criação de Relatório do tipo saúde do ecossistema (health check) de backup e de replicação;

5.9.5.9. Criação de Relatórios de métricas e de sla para a replicação, como Recovery Point Objective (RPO) e Recovery Time Objective (RTO);

5.9.5.10. Criação de Relatório de ajustes e melhorias possíveis no ambiente;

5.9.5.11. Criação de um calendário para validações semanal da rotina de replicação de dados, assim como dos testes para certificar a subida de ambiente crítico em site secundário do contratante, para fins de auditoria interna do contratante.

VALOR TOTAL DA CONTRATAÇÃO R\$ 50.550.000,00 (CINQUENTA MILHÕES E QUINHENTOS E CINQUENTA MIL REAIS)

Prazo de Validade da Proposta	Conforme Edital
Local de Entrega	Conforme Edital
Prazo de entrega	Conforme Edital
Garantia	Conforme Edital
Procedência dos objetos	Fabricação Nacional / Importação de Respective Distribuidores Legais no Brasil.
Assistência Técnica	Conforme Edital
Termo de Garantia	Conforme Edital

A empresa **DECLARA** que:

- 1 – Estão inclusas no valor cotado todas as despesas com mão de obra e, bem como, todos os tributos e encargos fiscais, sociais, trabalhistas, previdenciários e comerciais e, ainda, os gastos com transporte e acondicionamento dos produtos em embalagens adequadas.
- 2 – O prazo de início de fornecimento/execução dos serviços de acordo com o estabelecido no termo de referência do edital desse processo.
- 3 – Não possui como sócio, gerente e diretores, servidores do Serviço Nacional de Aprendizagem Comercial – Senac, Administração Regional no Estado de São Paulo, e ainda cônjuge, companheiro ou parente até terceiro grau.
- 4 – O prazo de início da entrega dos equipamentos será de acordo com os termos estabelecidos no edital deste processo a contar do recebimento, por parte da contratada, da ordem de compra ou documento similar, no local definido e que todos os equipamentos serão avaliados, sob pena de devolução de não aceite, caso não atenda a discriminação do termo de referência do referido edital ou de má qualidade.
- 5 – Cumpre todas as exigências estabelecidas no Termo de Referência do Pregão Eletrônico – PEE 2025000020.
- 6 – Não possui impedimentos legais para contratar com a administração pública.

Observações:

- 1) Validade da Proposta: **90** (noventa) dias;
- 2) Condições de Pagamento: O pagamento será realizado em única vez diretamente à Contratada em até 28 (vinte e oito) dias após recebimento do acordo de compra, através de emissão de nota fiscal e boleto bancário;
- 3) Prazo de Entrega: As licenças deverão estar disponíveis por e-mail, ou site do Fabricante para visualização e uso, em até 10 dias úteis a partir do recebimento do Acordo de Compra, e as licenças deverão ser nominais ao Senac São Paulo;
- 4) Vigência: 12 (doze) meses, a partir do recebimento do Acordo de Compra;

Ao indicar SaaS indica-se que quer como serviço a licença Veeam. Para atender ao modelo VCSP, a oferta foi ajustada para Veeam Availability Suite Enterprise Plus – VCSP Rental - 900 Servidores Virtuais – Garantia e atualizações por 12 meses, com precificação baseada no consumo e vinculada a um contrato vencido, conforme política de licenciamento da Veeam.