

MINUTA

ANEXO IV

CONTRATO Nº _____

CONTRATO DE FORNECIMENTO E PRESTAÇÃO DE SERVIÇOS DE SOLUÇÃO INTEGRADA PARA PROTEÇÃO DE DADOS, CONFORME PROCESSO PREGÃO ELETRÔNICO Nº 21/01.00009-PG.

O Serviço Social do Comércio – Sesc, Administração Regional no Estado de Goiás, entidade sem fins lucrativos e de direito privado, com sede no(a), na cidade de /Estado ..., inscrito(a) no CNPJ sob o nº, neste ato representado por seu Diretor Regional(*nome*), (nacionalidade), (estado civil), carteira de identidade nº _____, expedida pelo _____, CPF nº _____ residente e domiciliado em, doravante denominada CONTRATANTE, e a empresa inscrito(a) no CNPJ/MF sob o nº, sediado(a) na, em doravante designada CONTRATADA, neste ato representada pelo(a) Sr.(a) (*nome*), (nacionalidade), (estado civil), carteira de identidade nº _____, expedida pelo _____, CPF nº _____ residente e domiciliado em, observando-se as condições estabelecidas na modalidade **PREGÃO ELETRÔNICO nº. 21/01.00009-PG**, e, as disposições da **Resolução Sesc nº 1.252/2012-CN**, publicada no D.O.U., resolvem celebrar o presente Contrato, decorrente da Ata de Registro de Preços nº, mediante as cláusulas e condições a seguir enunciadas:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto do presente Contrato é o fornecimento de **Solução Integrada para Proteção dos dados contemplando hardware e software, e informações do ambiente produtivo do Sesc/GO. Incluindo sua implantação, configuração, garantia e suporte para atendimento das necessidades do Sesc/GO**, conforme especificações e quantitativos estabelecidos neste instrumento.

1.2. Este Contrato vincula-se ao Edital e seus anexos, do processo identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

1.3. Discriminação do objeto:

LOTE 1			
ITEM	DESCRIÇÃO	QTD	UND
1	EQUIPAMENTO - APPLIANCE FISICO PARA PROTECAO DE DADOS LOCAL	1	UND
2	EQUIPAMENTO - APPLIANCE FISICO DE REDUNDÂNCIA PARA PROTECAO DE DADOS LOCAL	1	UND
3	SERVICO - GARANTIA E SUPORTE POR 12 MESES PARA APPLIANCE FISICO PARA PROTECAO DE DADOS LOCAL.	1	SVÇ
4	SERVICO - GARANTIA E SUPORTE POR 12 MESES PARA APPLIANCE FISICO DE REDUNDÂNCIA PARA PROTECAO DE DADOS LOCAL.	1	SVÇ
5	SERVICO - SERVICO DE PROTECAO DE DADOS COM LICENCIAMENTO PARA NO MINIMO 1TB.	12	SVÇ

6	SOLUÇÃO DE PROTEÇÃO DE DADOS COM LICENCIAMENTO PARA NO MÍNIMO 1 TB.	12	SVÇ
7	SERVIÇO - INSTALACAO E CONFIGURACAO DA SOLUCAO	1	SVÇ
8	TREINAMENTO DA SOLUÇÃO	4	SVÇ

1.4. CARACTERISTICAS PARA APPLIANCE FÍSICO PARA PROTEÇÃO DE DADOS LOCAL E APPLIANCE FÍSICO DE REDUNDÂNCIA PARA PROTEÇÃO DE DADOS LOCAL.

- 1.4.1. Deve ser novo, sem uso, e estar na linha de produção atual do fabricante;
- 1.4.2. Fazer parte do catálogo de produtos comercializados pelo fabricante e não ter sido descontinuado;
- 1.4.3. Deve constar no site do fabricante (documento oficial e público) como um appliance de backup em disco, em linha de produção;
- 1.4.4. Deve ser do mesmo fabricante do software de proteção da informação, garantindo total integração e desempenho do ambiente;
- 1.4.5. Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, de maneira perpétua, irrestrita e sem necessidade de licenciamentos ou ônus adicionais;
- 1.4.6. Deve obrigatoriamente fazer uso de sistemas de armazenamento de backup em disco, baseado em "Appliance", que se entende como um subsistema com o propósito específico de console de gerenciamento central com base de dados de catálogo independentes, movimentadores de dados de backup, também conhecidos como gerenciadores de mídia, ingestão dos dados de backup com deduplicação e replicação;
- 1.4.7. "Appliance" deve ser composto, de processamento e armazenamento integrado, dedicado única e exclusivamente, à execução das atividades de console de gerenciamento, gerenciadores de mídia, ingestão, deduplicação e replicação dos dados, sem a necessidade de servidores, tradicionais, de backup para gestão em separado;
- 1.4.8. O sistema de armazenamento de backup em disco deve ser duo-processado;
- 1.4.9. As funcionalidades de backup e restore especificadas no item "Solução de Proteção de Informação" devem ser instalados somente no "Appliance" e o mesmo deve possuir gerenciamento de falhas e alarmes embarcado no próprio "Appliance", não devendo utilizar servidores externos para tais funcionalidades, provendo assim, console de gerenciamento único;
- 1.4.10. Deve possuir interface de administração GUI e CLI;
- 1.4.11. Permitir executar múltiplos processos de backup em paralelo e otimizar a restauração de arquivos individuais;
- 1.4.12. Permitir a integração com fitotecas de backup (tape library);
- 1.4.13. O sistema de armazenamento de backup em disco deverá suportar RAID-1 para Sistema Operacional e RAID-6 para dados como sistema de proteção de falhas em disco;
- 1.4.14. O Sistema de armazenamento de backup disco deverá conter disco de "hot spare" caso ocorra perda de um disco. O disco de "hot spare" será usado para substituir e reconstruir automaticamente o dado de backup;

- 1.4.15. Este módulo base deve ser fornecido com, no mínimo 32 TB (trinta e dois terabytes) de capacidade utilizável considerando base 2 (1 terabyte igual a 1024 gigabytes) em RAID-6, sem considerar ganhos com deduplicação e compressão de dados;
- 1.4.16. O sistema de armazenamento de backup deve ser escalável à no mínimo 400TB (quatrocentos terabytes) úteis, apenas com adição de discos, sem considerar ganhos com deduplicação e compressão de dados;
- 1.4.17. O sistema de armazenamento de backup deve possuir no mínimo 256GB (duzentos e cinquenta e seis gigabytes) de memória RAM, expansível até 512GB (quinhentos e doze gigabytes)
- 1.4.18. Deve suportar as seguintes interfaces de interconexão: interfaces Fibre Channel (FC) 16Gb (dezesseis gigabits), interfaces Ethernet 1Gb (um gigabit) , Ethernet 10Gb (dez gigabits) ou Ethernet 25Gb (vinte e cinco gigabits)
- 1.4.19. Deve ser fornecido com no mínimo 1 (uma) porta de 1 GB (um gigabit) Ethernet IPMI para monitoramento, 4 (quatro) portas 1GbE (um gigabit ethernet), 4 (quatro) portas 10GbE SFP (dez gigabits ethernet fibra) e 6 (seis) portas 16Gb FC (dezesseis gigabits Fibre Channel) para interconexão e integração com os servidores clientes;
- 1.4.20. Deve possuir pelo menos 2 (duas) CPUs 12-core cada (doze cores cada CPU) totalizando um mínimo de 24 (vinte e quatro) cores;
- 1.4.21. Deve suportar todas as funcionalidades previstas na API (Application Program Interface) do OST (Open Storage Technology) para backup, tais como:
- 1.4.22. Deduplicação no cliente (deduplicação na origem);
- 1.4.23. Deduplicação otimizada para efeito de replicação;
- 1.4.24. Backup sintético otimizado (funcionalidade que permite criar uma imagem full a partir dos backups incrementais sem movimentação de dados);
- 1.4.25. O appliance deve possuir funcionalidades para proteção dos dados armazenados contra ransomware e outros ataques maliciosos. Caso a solução não tenha esta funcionalidade de forma nativa, é permitida a composição de software para atendimento do item, não sendo permitido soluções open source.
- 1.4.26. Replicação de dados de backup entre domínios de backup diferentes com a inserção automática dos dados de catálogo no domínio alvo e após a replicação permitir continuidade do ciclo de proteção de dados no domínio de destino através de duplicação da imagem para fita magnética ou lógica (VTL);
- 1.4.27. Sobre a deduplicação:
- 1.4.28. A solução de armazenamento de backup em disco deverá possuir tecnologia de deduplicação de dados, ou seja, não armazenar mais de uma vez dados que sejam duplicados;
- 1.4.29. Entende-se por deduplicação dos dados, a funcionalidade que permite eliminar segmentos redundantes e compactar os dados, de forma a reduzir a capacidade de disco destinada ao armazenamento dos dados de backup;
- 1.4.30. A deduplicação deve segmentar automaticamente os dados em blocos de tamanho fixo e variável;

- 1.4.31. A funcionalidade de deduplicação de dados deverá ser executada em linha com a ingestão dos dados e replicação, eliminando a necessidade de armazenamento intermediário para cache dos dados;
- 1.4.32. A deduplicação deverá acontecer antes dos dados serem gravados nos discos do “appliance”;
- 1.4.33. Suportar deduplicação de blocos na origem (client-side deduplication), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir do último backup full, assim como deve ser possível fazer a deduplicação nos clientes de backup, na origem dos dados, antes dos dados serem enviados e gravados no disco do “appliance”.
- 1.4.34. A deduplicação deve ser global, ou seja, identificar dados duplicados tanto do mesmo servidor-cliente de origem do backup como outros servidores-cliente armazenados no mesmo dispositivo de backup, armazenando na solução somente blocos de dados únicos. Caso a deduplicação não seja global deverá ser ofertado 70% a mais de área útil ao especificado.
- 1.4.35. O sistema de armazenamento de backup em disco deve permitir replicar os dados através de rede IP (WAN/LAN);
- 1.4.36. O sistema de armazenamento de backup em disco deve possuir auto suporte do tipo call home para seus componentes de hardware e software, tais como: CPU, disco, fonte, ventiladores, temperatura, capacidade de utilização, firmware, entre outros.
- 1.4.37. O sistema de armazenamento de backup em disco deve permitir o particionamento da área de armazenamento no formato nativo para fins de “disk staging” (partição sem deduplicação) e/ou para o uso da tecnologia do tipo deduplicação;
- 1.4.38. O sistema de armazenamento de backup em disco deve permitir suporte à replicação dos dados no formato deduplicado, com controle e atualização do catálogo do aplicativo de backup;
- 1.4.39. O sistema de armazenamento de backup em disco deve permitir realizar a replicação otimizada dos dados, utilizando recursos como deduplicação, com controle e atualização do catálogo do aplicativo de backup;
- 1.4.40. Os dados replicados pelo sistema de armazenamento devem ser refletidos no catálogo do software de backup;
- 1.4.41. A solução deve verificar constantemente e automaticamente os dados armazenados, sem a utilização de scripts e/ ou composições feitas exclusivamente para esse órgão;
- 1.4.42. A solução deverá permitir múltiplas políticas de disaster recovery para prevenir perda de dados tais como; cópia do catalogo do backup para fita, replicação entre appliances no mesmo domínio de backup e replicação entre appliances em domínios de backup diferentes;
- 1.4.43. A replicação de dados de backup entre “appliances” e para nuvens públicas, deverá ocorrer através de otimizador WAN embutido para economia de largura de banda do link. Caso a solução não tenha esta funcionalidade de forma nativa, é permitida a composição de software para atendimento do item, não sendo permitida soluções open source.

- 1.4.44. Deverá possibilitar a replicação dos dados em disco para outro servidor ou outro dispositivo de mesma natureza. A replicação deverá ser assíncrona e ocorrer em horário pré-determinado;
- 1.4.45. Deve possuir licença para replicação dos dados armazenados no dispositivo de armazenamento para outro dispositivo de mesma natureza em formato desduplicados;
- 1.4.46. Deve possuir desempenho de backup de no mínimo 27TB/hora (vinte e sete terabytes por hora) considerando a desduplicação no destino.
- 1.4.47. Os componentes de FAN e power supply devem ser redundantes;
- 1.4.48. A solução deve permitir o uso de compartilhamento da área de armazenamento com suporte a desduplicação a qualquer plataforma com funcionalidade CIFS ou NFS;
- 1.4.49. A solução deve permitir o uso de compartilhamentos NFS para proteção de bancos de dados Oracle com a utilização do Oracle RMAN, com as seguintes características:
- 1.4.50. Deverá permitir a gravação dos dados a partir do servidor Oracle diretamente via RMAN em um compartilhamento NFS no appliance;
- 1.4.51. O produto do backup estará disponível para restauração diretamente no RMAN, utilizando os dados disponíveis no disco do appliance;
- 1.4.52. Permitir que a os dados copiados diretamente do RMAN sejam duplicados em cópias complementares para fita, disco com ou sem desduplicação;
- 1.4.53. Não serão aceitas soluções compostas por componentes de fabricantes diferentes;
- 1.4.54. Todos os componentes de hardware da solução deverão possuir fontes de alimentação redundantes;
- 1.4.55. Todos os equipamentos devem ser montáveis em rack padrão 19”;
- 1.4.56. Os dados deverão estar em uma das seguintes tecnologias de proteção: RAID-1, RAID-10, RAID-6 ou RAID-60;
- 1.4.57. Deve suportar backup via LAN, SAN e WAN, sem a necessidade de adquirir outras soluções para as localidades remotas;
- 1.4.58. Possuir alimentação elétrica com a seguinte característica:
- 1.4.59. Fontes internas ao equipamento, redundantes e hot-swappable;
- 1.4.60. Fontes devem auto detectar a tensão de trabalho e comutar sem a necessidade de nenhum agente externo entre as tensões de 110 e 220 volts;
- 1.4.61. Os equipamentos fornecidos deverão prover ‘software’ de administração e gerenciamento para total administração e configuração do sistema de forma local ou remota., que permitam também a análise de desempenho e implementação das políticas de segurança física, lógica, e de acesso de usuários;
- 1.4.62. A solução deve ser fornecida com todos os acessórios necessários para a plena configuração, operacionalização, utilização e gerenciamento do equipamento, sem necessidade de aquisições futuras de licenças ou softwares de ativação, tais como:
- 1.4.63. Softwares e manuais necessários para o gerenciamento;
- 1.4.64. Os softwares, drives e firmwares necessários devem estar em suas últimas versões.

1.4.65. Cabos lógicos de gerenciamento/console.

1.4.66. Cabos de energia elétrica padrão IEC 320 plug C13/C14.

1.5. DA SOLUÇÃO DE PROTEÇÃO DE DADOS COM LICENCIAMENTO PARA NO MÍNIMO 1 TB

1.5.1. Licenciamento do Software

1.5.2. Deve ser do mesmo fabricante do appliance de backup em disco, garantindo total integração e desempenho do ambiente;

1.5.3. Deverão ser fornecidas licenças incluindo suporte para backup, restore e tecnologia de deduplicação de dados, onde o licenciamento deve possuir capacidade ilimitada de retenções, cópias dos dados protegidos, replicações para outros ambientes para fins de recuperação de desastres. Poderão ser ofertadas licenças para atender o seguinte ambiente:

1.5.4. Volumetria líquida de dados na origem de 12 (doze) terabytes (TB);

1.5.5. A solução de Proteção de Dados a ser ofertada deve atender integralmente os requisitos especificados neste Contrato, devendo ser fornecida com todas as licenças que forem necessárias para entrega funcional da solução;

1.5.6. Arquitetura e Características Gerais do Software

1.5.6.1. Possuir uma arquitetura em múltiplas camadas permitindo desempenho e escalabilidade horizontal:

1.5.6.1.1. Camada de gerência;

1.5.6.1.2. Camada do serviço de mídia/unidade de disco de retenção dos dados;

1.5.6.1.3. Camada de clientes/agentes multiplataforma de backups;

1.5.6.2. Deve possuir catálogo ou banco de dados centralizado contendo as informações sobre todos os dados e mídias onde os backups foram armazenados, esse banco de dados ou catálogo deve ser próprio e fornecido em conjunto com o produto;

1.5.6.3. Deve possuir mecanismo de verificação e checagem de consistência da base de dados no intuito de garantir a integridade dos dados;

1.5.6.4. Possuir mecanismo de reconstrução do catálogo ou banco de dados centralizado em caso de perda do mesmo, sem a necessidade de recatálogo as imagens de backup;

1.5.6.5. Deve fazer uso de banco de dados relacional para guardar o catálogo de Jobs, arquivos e mídias dos backups;

1.5.6.6. Deve suportar servidor de gerência e catálogo nas seguintes plataformas: Linux ou Windows. Para evitar aumento de complexidade de gestão, não serão aceitos catálogos instalados em máquinas virtuais em plataformas (sistemas operacionais) diferentes da utilizada no servidor de gerência;

1.5.6.6.1. Deverá permitir a configuração de servidores de gerência de catálogo em cluster para promover alta-disponibilidade dos serviços de gerenciamento. A implementação do cluster deverá ser possível pelo menos para as plataformas: Red Hat Enterprise Linux, Oracle Linux, Suse Enterprise Linux e Windows;

1.5.6.7. Deve suportar servidores movimentadores de dados nas seguintes plataformas: Linux e Windows.

- 1.5.6.8. Os servidores movimentadores de dados devem suportar balanceamento de carga para distribuir a carga de entre os mesmos de forma automática
- 1.5.6.9. Os servidores movimentadores de dados devem suportar configuração de recurso automático de failover, ou seja, permitir a configuração de mais de um servidor movimentador de dados em uma política de proteção, de forma que a indisponibilidade de um servidor seja suprida por outro servidor movimentador de dados disponível de forma automática. Esta funcionalidade deverá ser nativa do produto, e não pode ser construída com o uso de soluções baseadas em softwares de cluster de terceiros;
- 1.5.6.10. Deve permitir o backup e restore de arquivos abertos, garantindo a integridade do backup;
- 1.5.6.11. Deve ser capaz de gerenciar múltiplos e diferentes dispositivos de backup (bibliotecas de fitas, drives de backup, dispositivos de disco com e sem desduplicação), conectados localmente (Direct Attached) ou compartilhados entre múltiplos servidores da camada de mídia via SAN (Storage Area Network);
- 1.5.6.12. Possuir a capacidade de escrever múltiplos fluxos de dados provenientes de servidores distintos (multiplexação), divididos em blocos de tamanhos constantes em um único dispositivo físico de gravação;
- 1.5.6.13. Possuir a capacidade de dividir o fluxo de dados proveniente de um servidor em vários dispositivos de gravação (multiple streams);
- 1.5.6.14. Possuir a capacidade de reiniciar backups e restores a partir do ponto de falha, após a ocorrência da mesma;
- 1.5.6.15. Deve possuir mecanismo de instalação e atualização de clientes e agentes de backup de forma remota, através de interface de gráfica, permitindo a instalação de múltiplos clientes de backup simultaneamente;
- 1.5.6.16. Para facilitar o processo de verificação de pré-requisitos e compatibilidade, o fabricante deve possuir mecanismo público de geração de lista de checagem que, através da informação do pacote a ser instalado, do sistema operacional alvo da instalação, gere uma lista que contenha:
 - 1.5.6.16.1. Patches do Sistema Operacional e de dispositivos de hardware que por ventura necessitem estar instalados;
 - 1.5.6.16.2. Componentes do produto suportados para instalação ou uso no Sistema Operacional em questão;
 - 1.5.6.16.3. Requerimentos de Hardware para instalação do produto no Sistema Operacional em questão;
 - 1.5.6.16.4. Componentes de Hardware compatíveis;
 - 1.5.6.16.5. Compatibilidade com aplicações, bancos de dados e sistemas de arquivos (File System);
 - 1.5.6.16.6. Possíveis correções e atualizações adicionais disponíveis para o funcionamento do produto no Sistema Operacional alvo.
- 1.5.6.17. Possuir a capacidade de realizar download e instalação de atualizações, de forma automática, no servidor de backup e clientes;

- 1.5.6.18. Possuir ambiente de gerenciamento de backup e restore via interface gráfica e linha de comando;
- 1.5.6.19. Possuir função de agendamento do backup através de calendário;
- 1.5.6.20. Possuir interface web para gerenciamento, monitoramento e criação de políticas de backup e restore;
- 1.5.6.21. Possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades de administração e operação do software de backup;
- 1.5.6.22. Permitir a programação de tarefas de backup automatizadas em que sejam definidos prazos de retenção dos arquivos;
- 1.5.6.23. Possuir função para definição de prioridades de execução de Jobs de backup;
- 1.5.6.24. Deve permitir o agendamento de jobs de backup, sem utilização de utilitários de agendamento dos hosts;
- 1.5.6.25. Deve permitir a programação de jobs de backup automatizadas em que sejam definidos prazos de retenção das imagens;
- 1.5.6.26. Possuir a função de Backup sintético que permite a criação de uma única imagem de backup a partir de um backup full e qualquer quantidade de backups incrementais. O restore será efetuado da nova imagem full sintética;
- 1.5.6.27. Possuir políticas de ciclo de vida nativas, gerenciar camadas de armazenamento e transferir automaticamente os dados de backup entre camadas através do seu ciclo de vida;
- 1.5.6.28. Permitir a realização do backup completo de servidor para recuperação de desastres;
- 1.5.6.29. Permitir restaurar o backup de recuperação de desastres para hardware diferente do original - para ambiente Windows;
- 1.5.6.30. Permitir o controle da banda de tráfego de rede durante a execução do backup e/ou do restore;
- 1.5.6.31. Suportar integração com OST (OpenStorage) Disk Appliances através de OpenStorage API;
- 1.5.6.32. Suportar a proteção dos dados de aplicações de big data Hadoop, HBase e AHV (Nutanix Acropolis Hypervisor) e bancos de dados NoSQL (Apache HBase e MongoDB)
- 1.5.6.33. Ser capaz de recuperar dados para servidores diferentes do equipamento de origem;
- 1.5.6.34. Ser capaz de utilizar qualquer tecnologia utilizada pela Solução de Armazenamento como destino dos backups seja armazenamento diretamente anexado (DAS), armazenamento em rede NAS ou rede SAN;
- 1.5.6.35. Possuir a função de Disk Staging, ou seja, que permita o envio dos dados para disco e posteriormente do disco para outro tipo de mídia (disco ou fita);
- 1.5.6.36. Permitir que Logical Unit Numbers (LUNs) sejam apresentadas aos servidores da camada de mídia como destino para realização de backups;

- 1.5.6.37. Permitir o compartilhamento de LUNs entre vários servidores de mídia de mesmo sistema operacional;
- 1.5.6.38. Realizar backup e restore de file systems montados em dispositivos Network-Attached Storage (NAS) através do suporte ao protocolo NDMP versão 4 ou superiores;
- 1.5.6.39. Permitir integração do controle de acesso com sistemas de diretório NIS, NIS+ e Active Directory;
- 1.5.6.40. Permitir a replicação de imagens de um servidor de gerência para outro ambiente, possibilitando a inserção das informações de catálogo da imagem de origem para o catálogo do destino, de forma automática e sem a necessidade de licenciamento adicional.
- 1.5.6.41. Possuir Interface única para gerenciamento de todos os servidores independente do S.O que hospeda esse serviço (Windows, Linux); ou ao menos com a separação entre estrutura de backup da Central de Serviços e estrutura de backup das Unidades remotas.
- 1.5.6.42. Deve implementar monitoramento e administração remotos da solução de backup a partir de qualquer servidor ou estação de trabalho Windows;
- 1.5.6.43. A Solução de Backup deverá permitir operações de Backup e Restore através de rede local (LAN_based e Storage Area Network (SAN_based ou LAN_free));
- 1.5.6.44. Deve permitir a verificação da integridade do conteúdo das fitas por software;
- 1.5.6.45. Deve permitir liberação das fitas magnéticas quando todos os arquivos contidos nas mesmas tenham suas datas de retenção expiradas;
- 1.5.6.46. As fitas liberadas devem ficar disponíveis automaticamente para uso de outras tarefas de backup;
- 1.5.6.47. A Solução de Backup deverá, a partir de uma única interface, gerenciar operações de Backup e Restore de diferentes sistemas operacionais (clientes); bem como operações de recuperação bare metal.
- 1.5.6.48. Deve permitir a criação de imagens de servidores físicos Linux e Windows, para recuperação de desastres (funcionalidade conhecida como bare metal restore de forma nativa, i.e., sem a utilização de software de terceiros;
- 1.5.6.49. Para servidores Windows, deve ser possível a recuperação das imagens de recuperação de desastres mesmo em um hardware diferente do original ou em ambiente virtual.
- 1.5.6.50. A funcionalidade de baremetal especificada anteriormente deve suportar em um único servidor de gerência ou servidor de mídia várias versões de Windows – Windows 2008, 2008 R2, 2012 e 2012R2).
- 1.5.6.51. Deve permitir a verificação da integridade dos dados armazenados através de algoritmos de checksum e/ou autocorreção;
- 1.5.6.52. Deve permitir escolher se a criptografia será realizada no agente, com o tráfego de dados via rede já criptografado ou no servidor de backup;
- 1.5.6.53. Deve possuir capacidade nativa de efetuar criptografia dos backups em no mínimo 256 bits nos Clientes de Backup e em dispositivos de mídia que suportem criptografia;

- 1.5.6.54. Deve possuir a capacidade de gerenciar software de snapshot de storages de outros fabricantes (no mínimo, Netapp), com o intuito de automatizar o processo de agendamento de cópias “snapshot” e montagem no servidor de backup “off-host”;
- 1.5.6.55. A Solução de Backup deverá permitir a integração com a funcionalidade de cópias instantâneas (Snapshot) de subsistemas de armazenamento em disco (storage);
- 1.5.6.56. Deverá possuir integração para gerência de Snapshots;
- 1.5.6.57. Deverá permitir a criação e gerenciamento de Snapshots através da ferramenta de administração da Solução de Backup;
- 1.5.6.58. Possibilitar o registro dos Snapshots na base relacional de catálogos da Solução de Backup de forma a possibilitar a realização de buscas;
- 1.5.6.59. Controlar o período pelo qual os Snapshots serão válidos, realizando a expiração automática de um Snapshot assim que o período de retenção configurado seja atingido.
- 1.5.6.60. Deve possibilitar enviar notificações, quando configurado, dos eventos por e-mail;
- 1.5.6.61. Deve possuir a funcionalidade de backup com duplicação dos dados simultânea entre mídias distintas para envio a cofre;
- 1.5.6.62. Possuir mecanismo de auditoria, permitindo a emissão de relatórios onde constem, no mínimo, as seguintes informações:
- 1.5.6.63. Data e hora da operação, Usuário que realizou a operação, Ação realizada (em caso de modificação de configurações, informar qual a configuração anterior e a modificação realizada).
- 1.5.6.64. Auditoria e controle de acesso devem ser funcionais para operações realizadas via interface gráfica e linha de comando.
- 1.5.6.65. Deve prover monitoramento via interface gráfica e em tempo real dos Jobs sendo executados, incluindo visão de nível hierárquico dos jobs.
- 1.5.6.66. Deve suportar operações de backup e restore em paralelo;
- 1.5.6.67. Deve permitir encadear Jobs para que um só comece após outro ter terminado;
- 1.5.6.68. Deve suportar armazenamento nos cloud storages: Amazon S3, Microsoft Azure, Microsoft Azure Stack e Google Cloud Storage;
- 1.5.6.69. A solução de proteção de dados deverá possibilitar o armazenamento deduplicado nos cloud storages: Amazon S3, Microsoft Azure, Google Cloud Storage.
- 1.5.6.70. Permitir o controle da banda de tráfego de rede durante a execução do backup para nuvem.
- 1.5.7. Do Suporte a plataformas:
 - 1.5.7.1. Deve suportar o backup e o restore de diferentes sistemas operacionais tais como:
 - 1.5.7.1.1. Windows (8/10/2008/2008 R2/2012/2012 R2/2016/2019);
 - 1.5.7.1.2. Oracle Linux (6 e 7);
 - 1.5.7.1.3. Red Hat Enterprise Linux (6 e 7);

- 1.5.7.1.4. Suse Enterprise Server (11 e 12);
- 1.5.7.1.5. CentOS (6 e 7);
- 1.5.7.1.6. Debian GNU (7, 8 e 9);
- 1.5.7.1.7. Oracle Solaris (10 e 11);
- 1.5.7.1.8. AIX (6.1, 7.1 e 7.2);
- 1.5.7.1.9. Ubuntu (16, 17 e 18)
- 1.5.7.2. Suportar as seguintes tecnologias de virtualização:
 - 1.5.7.2.1. VMware vSphere: Ser comprovadamente compatível com o VADP (vStorage API for Data Protection) para realizar operações de Backup e Restore de ambientes VMware versão 5.x e superior;
 - 1.5.7.2.2. Suporte ao VMware VCloud, possuindo integração com vCloud Director API possibilitando backup automático das máquinas virtuais e recuperação completa;
 - 1.5.7.2.3. Microsoft Hyper-V: Suporte a Microsoft Hyper-V Server 2008 R2/R2 SP2, Microsoft Hyper-V Server 2012/R2, Microsoft Hyper-V Server 2016 e Microsoft Hyper-V Server 2019.
 - 1.5.7.2.4. Possuir suporte a backup e restore de máquinas virtuais VMware 5.x ou superior através de vStorage API com as seguintes características:
 - 1.5.7.2.4.1. Deve permitir que através de uma única rotina de Backup a qual enviou os seus dados para disco ou tape seja possível recuperar a imagem completa da máquina virtual Windows e Linux (vmdk), somente o vmdk desejado de forma seletiva e também os arquivos de maneira granular sem a necessidade de scripts, área temporária ou montagem dos arquivos vmdk;
 - 1.5.7.2.4.2. Deve suportar o uso da funcionalidade CBT (Change Block Tracking) para as operações de backup;
 - 1.5.7.2.4.3. Deve suportar o backup e restore de máquinas virtuais que utilizam o vTPM (Virtual Trusted Platform Module)
 - 1.5.7.2.4.4. Deve permitir a identificação de aplicações Microsoft Exchange, SQL e SharePoint que residem nas máquinas virtuais, através de integração VADP, permitindo o backup, recuperação integral ou granular dessas aplicações;
 - 1.5.7.2.4.5. Deve permitir a recuperação granular de arquivos/aplicações através da execução de um único backup;
 - 1.5.7.2.4.6. Permitir o descobrimento automático das máquinas virtuais nos ambientes VMware, com capacidade de realizar filtros avançados com critérios que incluam pelo menos:
 - 1.5.7.2.4.6.1. Nome da máquina virtual;
 - 1.5.7.2.4.6.2. Sistema Operacional;
 - 1.5.7.2.4.6.3. DataStore (VMware);
 - 1.5.7.2.4.6.4. vApp;
 - 1.5.7.2.4.6.5. vSAN.

- 1.5.7.2.4.7. Permitir backup BLIB (Block Level Incremental Backup e Restore) e FLIB (File Level Incremental Backup e Restore);
- 1.5.7.2.4.8. Deve possuir a capacidade de balanceamento de carga automático dos backups através de múltiplos backups hosts;
- 1.5.7.2.4.9. Deve suportar Vmware vSphere 5.x e 6.x;
- 1.5.7.2.4.10. Deve permitir restaurar e iniciar a execução de uma máquina virtual instantaneamente, diretamente a partir do seu repositório de backup, sem a necessidade de manter réplicas ou snapshots disponíveis para o processo de recuperação instantânea;
- 1.5.7.2.4.11. Prover otimização do backup e recursos (tape / disco), permitindo que somente blocos utilizados sejam copiados no processo de backup;
- 1.5.7.2.4.12. Permitir realizar restauração, através de um único backup, de Máquina virtual completa ou arquivos de dentro da máquina virtual para ambientes Windows e Linux;
- 1.5.7.2.4.13. Deve permitir a visualização, monitoração e recuperação de máquinas virtuais através de plugin integrado ao vCenter ou vSphere 5.5 Web Client;
- 1.5.7.2.4.14. Deve possuir capacidade de realizar backup de maneira off-host, sem a necessidade de instalação de agentes nas máquinas virtuais;
- 1.5.7.2.4.15. Deve possuir capacidade de realizar backup de máquinas virtuais em estado online ou offline;
- 1.5.7.2.4.16. Deve possuir a capacidade de movimentação dos dados de backup e restore através de SAN e LAN utilizando os métodos de transporte san, nbd ou hotadd;
- 1.5.7.2.4.17. Deve possuir a capacidade de realizar backup de máquinas virtuais existentes em um vApp;
- 1.5.7.2.4.18. Deve possuir a capacidade de recuperação da imagem da máquina virtual, para máquinas que possuam discos vmfs ou RDM;
- 1.5.7.2.4.19. Deve suportar integração com vCloud Director API possibilitando backup automático das máquinas virtuais e recuperação completa;
- 1.5.7.2.4.20. Deve suportar a recuperação de máquinas virtuais que utilizem identificadores do tipo: hostname, display name, BIOS UUID e instance UUID;
- 1.5.7.2.5. Possuir suporte a backup e restore de máquinas virtuais Hyper-V, com as seguintes características:
 - 1.5.7.2.5.1. Deve possuir a capacidade de realizar backup On-Host e Off-host das máquinas virtuais Windows e Linux;
 - 1.5.7.2.5.2. Deve possuir a capacidade de realizar backup de maneira Full, Incremental ou Diferencial sem a necessidade de instalação de agentes nas máquinas virtuais;
 - 1.5.7.2.5.3. Deve suportar ambientes configurados com Cluster Shared Volumes;
 - 1.5.7.2.5.4. Deve permitir que através de uma única rotina de Backup a qual enviou os seus dados para disco ou tape seja possível recuperar a imagem completa da máquina virtual Windows e Linux (vhd), e também arquivos de maneira granular sem a necessidade de scripts, área temporária ou montagem dos arquivos vhd;

- 1.5.7.2.5.5. Deve possuir a capacidade de recuperação das máquinas virtuais para uma área temporária de disco;
- 1.5.7.2.5.6. Deve suportar Microsoft Hyper-V 2008, 2012, 2016 e 2019;
- 1.5.7.3. Deve suportar os seguintes bancos de dados, utilizando agente específico:
 - 1.5.7.3.1. Microsoft SQL Server versões 2008, 2012, 2014, 2016, 2017;
 - 1.5.7.3.2. Oracle/Oracle RAC versões 11g, 12c e 18c.
 - 1.5.7.3.3. Microsoft Exchange 2010, 2013 e 2016;
 - 1.5.7.3.4. Microsoft Sharepoint 2010, 2013 e 2016;
 - 1.5.7.3.5. MySQL 5 e 8;
 - 1.5.7.3.6. PostgreSQL 9, 10 e 11;
 - 1.5.7.3.7. MariaDB 5 e 10;
 - 1.5.7.3.8. Microsoft Active Directory
- 1.5.7.4. Deve suportar backup do Oracle Database, também na arquitetura Oracle RAC, através da integração com RMAN;
- 1.5.7.5. Deve possuir funcionalidade para descoberta automática de instancias Oracle através de consultas periódicas aos clientes de bancos de dados;
- 1.5.7.6. A funcionalidade de descoberta automática de instancias deve ser capaz de gerar os scripts RMAN no momento de execução do backup;
- 1.5.7.7. Deve suportar DAG (DataBase Availability Groups) do MS Exchange;
- 1.5.7.8. Deve suportar backup do Information Store de Microsoft Exchange, com possibilidade de restore granular, ou seja, de e-mails únicos, itens de calendário e também de caixa postal de algum usuário;
- 1.5.7.9. Deve suportar backup do Microsoft Active Directory, com possibilidade de restore granular, ou seja, restauração de todo um diretório, de objetos selecionados e até de atributos individuais;
- 1.5.7.10. Deve suportar backup completo do Sharepoint, com possibilidade de recuperação de uma ou mais databases, documentos individuais, sites, subsites, listas e itens/documentos individuais;
- 1.5.8. Desduplicação por Software
 - 1.5.8.1. Deve possuir capacidade de realizar desduplicação de dados na camada no cliente, servidor de backup e appliances de desduplicação. A solução deve permitir a desduplicação de qualquer capacidade (de acordo com o volume identificado e licenciado) e em qualquer forma de desduplicação (cliente, servidor de backup e appliances);
 - 1.5.8.2. Deve suportar desduplicação em nível de blocos;
 - 1.5.8.3. Deve suportar desduplicação de blocos na origem (client-side), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir do último backup full;

- 1.5.8.4. Deverá suportar o envio de dados desduplicados para a nuvem sem a necessidade de hardwares adicionais;
- 1.5.8.5. A solução de backup deve ser capaz de gerenciar a réplica do backup desduplicado entre appliances de desduplicação.
- 1.5.8.6. Deve possuir a capacidade de desduplicação global de dados no nível de segmentos ou blocos de dados repetidos, entre ambientes físicos e virtuais, mesmo em localidades remotas;
- 1.5.8.7. A solução de backup deverá, a partir de uma única interface, gerenciar operações de backup e restore de diferentes sistemas operacionais (clientes); bem como operações de recuperação bare metal.
- 1.5.8.8. Deve permitir ativar o recurso de desduplicação em volumes apresentados via SAN, DAS ou iSCSI para servidores Windows, Linux e Unix;
- 1.5.8.9. Deve possuir a capacidade de Replicação de Dados entre “pools” de desduplicação de maneira otimizada, enviando somente blocos únicos.
- 1.5.8.10. Deve possuir a capacidade de realizar balanceamento de carga automático entre servidores ou Appliances de Desduplicação ;
- 1.5.8.11. Deverá possibilitar a distribuição automática de carga entre os servidores que executarão o serviço de proteção de dados, ou seja, os dados oriundos dos clientes de backup deverão ser distribuídos de forma automática entre os servidores de backup da solução. Em caso de falha de um dos servidores de backup, o cliente automaticamente irá encaminhar seus dados através de outro servidor de backup ativo. Esta funcionalidade deverá ser nativa do produto, não sendo admitidas soluções baseadas em softwares de cluster de terceiros;
- 1.5.8.12. Deve possuir a capacidade de criptografar os dados armazenados de forma desduplicada;
- 1.5.8.13. As políticas de ciclo de vida da informação devem permitir a replicação das imagens de backup de forma otimizada, fazendo o uso da tecnologia de desduplicação de dados da solução no mesmo site ou entre sites distintos;
- 1.5.8.14. Deve fazer uso de tecnologia de replicação dos dados (não somente os dados protegidos – imagens de backup – mas também do catálogo do software de backup necessário para a recuperação do dado) do site principal para o site de desastre, de forma que em um evento de desastre, os sites sejam independentes no processo de recuperação.
- 1.5.8.15. Deve possuir tecnologia de desduplicação de dados inline por padrão
- 1.5.8.16. Deve permitir que depois de um backup full inicial, os backups subsequentes sejam feitos apenas através do envio das diferenças desduplicadas e que esses backups sejam consolidados como se fosse um backup full com a última data de envio.
- 1.5.8.17. Deve possuir a funcionalidade de backup com duplicação dos dados simultânea entre mídias distintas para envio a cofre;
- 1.5.9. Relatórios e Gerenciamento
- 1.5.9.1. Relatórios Operacionais

- 1.5.9.1.1. Deve prover relatórios gerenciais de backup com no mínimo as seguintes informações:
 - 1.5.9.1.1.1. Backups com sucesso;
 - 1.5.9.1.1.2. Backups com falha;
 - 1.5.9.1.1.3. Volume de backup realizado;
 - 1.5.9.1.1.4. Restores com sucesso;
 - 1.5.9.1.1.5. Restores com falha;
 - 1.5.9.1.1.6. Volume de restore realizado;
 - 1.5.9.1.1.7. Clientes de backup configurados;
 - 1.5.9.1.1.8. Ocupação no destino de backup;
 - 1.5.9.1.1.9. Licenciamento e capacidade;
 - 1.5.9.1.1.10. Quantidade de dados sendo protegidos e dados expirados;
 - 1.5.9.1.1.11. Descrição do conteúdo de cada fita;

CLÁUSULA SEGUNDA – DA GARANTIA DA SOLUÇÃO

- 2.1. Durante o período de garantia a CONTRATADA executará, sem ônus adicionais, correções de falhas (bugs) de software;
- 2.2. 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.
- 2.3. Canais de Atendimento:
 - 2.3.1. Será disponibilizado canal de atendimento e chamado técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de site na Internet e/ou canal telefônico gratuito 0800;
 - 2.3.2. Em caso de indisponibilidade do canal de atendimento disponibilizado, os chamados técnicos poderão ser abertos via e-mail, "website" do fabricante, telefone, etc.;
 - 2.3.3. A CONTRATADA deverá possuir e informar página da Internet onde estejam disponíveis drivers atualizados, últimas versões do software, sem restrições de acesso público ou via cadastramento de pessoas autorizadas pelo CONTRATANTE para o acesso.
- 2.4. A CONTRATADA concederá ao CONTRATANTE garantia integral durante 12 (doze) meses, 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, mesmo ocorrida sua aceitação/aprovação pelo contratante;
- 2.5. A CONTRATADA deverá garantir por, no mínimo, 12 (doze) meses o fornecimento dos componentes de software, para manutenções, suporte técnico ou ampliações, de forma que possam ser mantidas todas as funcionalidades inicialmente contratadas. Caso haja neste período a descontinuidade de fabricação dos componentes, deve ser também garantida a total compatibilidade dos itens substitutos com os originalmente fornecidos;
- 2.6. Manutenção corretiva será efetuada sempre que a solução apresente falhas que impeçam o seu funcionamento normal e/ou requeiram a intervenção de técnico especializado.

CLÁUSULA TERCEIRA – DA ESPECIFICAÇÃO DO SUPORTE TÉCNICO

- 3.1. Os serviços de suporte técnico deverão contemplar as manutenções corretivas e evolutivas para a solução contratada e não poderão acarretar custos adicionais ao CONTRATANTE, além do contratado.
- 3.2. Entende-se por “manutenção corretiva” uma série de procedimentos destinados a recolocar a solução em pleno estado de funcionamento, removendo definitivamente os defeitos apresentados.
- 3.3. Entende-se por “manutenção evolutiva” o fornecimento de novas versões e/ ou releases corretivas e/ou evolutivas de softwares que compõem a solução corporativa do software, lançadas durante a vigência deste contrato.
- 3.4. Durante o período de vigência do contrato o CONTRATANTE terá direito, sem ônus adicional, a todas as atualizações de versão e releases dos softwares e firmwares que fazem parte da solução ofertada.
- 3.5. A CONTRATADA deverá manter o serviço de suporte técnico, disponível para a abertura e acompanhamento de chamados em tempo integral, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados, com início de atendimento e prazo de solução de acordo com o nível de severidade exigido para o caso, conforme os índices de criticidade abaixo:

Nível	Classificação	Diagnóstico
01	Crítico: Serviço parado ou que possa tornar inoperante o ambiente de produção do SESC por inteiro ou uma parte majoritária desta que é essencial aos negócios diários.	A CONTRATADA deverá iniciar o atendimento do incidente no prazo máximo de 01 (uma) hora , contadas a partir da abertura do chamado de suporte corretivo pelo SESC. No prazo máximo de 4 (quatro) horas subsequentes ao início do atendimento do incidente, o serviço deverá estar totalmente operacional , estando a solução em perfeito funcionamento, de acordo com as melhores práticas recomendadas pelo fabricante
02	Urgente: Representa um incidente que está causando ou irá causar uma degradação que impacta o ambiente de produção do SESC ou um grupo majoritário de usuários.	A CONTRATADA deverá iniciar o atendimento do incidente no prazo máximo de 2 (duas) horas , contadas a partir da abertura do chamado de suporte corretivo pelo SESC. No prazo máximo de 5 (cinco) horas subsequentes ao início do atendimento do incidente, o serviço deverá estar totalmente operacional e sem nenhuma degradação , estando a solução em perfeito funcionamento, de acordo com as melhores práticas recomendadas pelo fabricante.

03	<p>Rotina: Representam falhas mínimas no ambiente do SESC não afetando o desempenho, serviço ou operação ou ainda a função afetada só e usada eventualmente ou temporariamente.</p>	<p>A CONTRATADA deverá iniciar o atendimento do incidente no prazo máximo de 4 (quatro horas) horas contadas a partir da abertura do chamado de suporte corretivo pelo SESC.</p> <p>No prazo máximo de 24 (vinte e quatro) horas subsequentes ao início do atendimento do incidente, o serviço deverá estar totalmente operacional, sem nenhuma degradação ou falhas, estando a solução em perfeito funcionamento, de acordo com as melhores práticas recomendadas pelo fabricante.</p>
----	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3.6. O suporte poderá ser realizado à distância (atendimento remoto), por quaisquer meios seguros de comunicação, incluindo, telefone (0800), internet, e-mail ou “on site” (presencial).

3.7. Será disponibilizado canal de atendimento e chamado técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de site na Internet e/ou canal telefônico gratuito 0800.

CLÁUSULA QUARTA – DO TREINAMENTO

4.1.A CONTRATADA deverá fornecer treinamento oficial do fabricante sobre a solução ofertada, abrangendo todos os tópicos necessários para a configuração da solução.

4.2.O treinamento deverá ser ministrado em Goiânia ou de forma remota respeitando os decretos estaduais e municipais referentes a pandemia da COVID-19 que vigorarem na época do treinamento, em caso de treinamento presencial, as instalações serão fornecidas pela CONTRATANTE, para um número de 4 (quatro) participantes, em horário que será estabelecido pelo CONTRATANTE, com carga horária mínima de 24 horas, sempre respeitando os protocolos sanitários do COVID-19.

4.3. As despesas com o ambiente de treinamento (sala, computadores, projetores e servidores) será de responsabilidade da CONTRATANTE, devendo ser observado o protocolo de segurança do Covid-19.

4.4. Deverá ser fornecido material didático e o mesmo deverá ser preparado pela CONTRATADA e entregue 02 (dois) dias antes do início do treinamento.

4.5. No momento do fechamento da turma a Contratada deverá encaminhar a documentação comprovando que o instrutor é certificado pelo fabricante da solução proposta.

4.6. As despesas com o instrutor, inclusive as relativas a transporte, estadia e alimentação, serão de responsabilidade da CONTRATADA.

4.7. A empresa contratada deverá fornecer certificados para os participantes.

CLÁUSULA QUINTA – DA VIGÊNCIA

5.1. O prazo de vigência deste de Contrato é ___ (___) ____, com início na data de ___/___/___ e encerramento em ___/___/___, prorrogável mediante aditivo contratual, em acordo com o Art. 26, Parágrafo único da Resolução Sesc nº 1.252/2012-CN.

5.2.A **CONTRATADA** deverá manter durante toda a relação contratual, todas as condições de habilitação e qualificação exigidas no **Pregão Eletrônico nº. 21/01.00009-PG**.

CLÁUSULA SEXTA – DO PREÇO

6.1.O valor total do presente Contrato é de R\$
(.....) que será pago de

acordo com a entrega e execução, desde que os materiais ou serviços tenham sido entregues e aceitos pelo Sesc Goiás, de acordo com a tabela abaixo:

ITEM	DESCRIÇÃO	QTD	UND	Valor unitário	Valor total
1	EQUIPAMENTO - APPLIANCE FISICO PARA PROTECAO DE DADOS LOCAL	1	UND	R\$	R\$
2	EQUIPAMENTO - APPLIANCE FISICO DE REDUNDÂNCIA PARA PROTECAO DE DADOS LOCAL	1	UND	R\$	R\$
3	SERVICO - GARANTIA E SUPORTE POR 12 MESES PARA APPLIANCE FISICO PARA PROTECAO DE DADOS LOCAL.	1	SVÇ	R\$	R\$
4	SERVICO - GARANTIA E SUPORTE POR 12 MESES PARA APPLIANCE FISICO DE REDUNDÂNCIA PARA PROTECAO DE DADOS LOCAL.	1	SVÇ	R\$	R\$
5	SERVICO - SERVICO DE PROTECAO DE DADOS COM LICENCIAMENTO PARA NO MINIMO 1TB.	12	SVÇ	R\$	R\$
6	SOLUÇÃO DE PROTEÇÃO DE DADOS COM LICENCIAMENTO PARA NO MÍNIMO 1 TB.	12	SVÇ	R\$	R\$
7	SERVIÇO - INSTALACAO E CONFIGURACAO DA SOLUCAO	1	SVÇ	R\$	R\$
8	TREINAMENTO DA SOLUÇÃO	4	SVÇ	R\$	R\$

6.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução contratual, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

CLÁUSULA SETIMA – DA ENTREGA DO OBJETO E REALIZAÇÃO DO SERVIÇO

7.1. As entregas deverão ser realizadas da seguinte forma:

7.1.1. A entrega das licenças deverá ser realizada em no máximo 15 (quinze) dias após a assinatura do contrato, podendo ser realizada de forma eletrônica.

7.1.2. O prazo para instalação e configuração da solução será de até 45 (quarenta e cinco) dias a contar da data de entrega das licenças.

7.2. Produtos e serviços em desacordo com o solicitado ou com problemas serão devolvidos ou não recebidos, devendo a contratada repor os produtos e serviços, na mesma quantidade e especificações descritas neste Contrato, sem ônus adicional, no prazo máximo de 10 (dez) dia após a notificação de desacordo.

7.3. A confirmação de recebimento ocorrerá após a conferência dos mesmos e das demais condições estabelecidas neste Contrato.

CLÁUSULA OITAVA – DO PAGAMENTO, FATURAMENTO E LOCAL DE ENTREGA

8.1. Os pagamentos serão realizados em até 15 (quinze) dias subsequentes à entrega da nota fiscal, desde que os serviços tenham sido conferidos e aceitos pelo Sesc-GO, e será feito preferencialmente através de boleto bancário, não sendo possível sua emissão o pagamento poderá ser feito através de crédito em conta corrente da empresa CONTRATADA.

8.1.1. A empresa deverá indicar em sua Nota Fiscal ou Fatura o banco, agência e conta corrente, onde será efetuado o crédito bancário referente à execução do objeto desta Licitação, desde que o mesmo tenha sido executado e aceito pelo Sesc-GO.

8.2. Os dados de faturamento da empresa contratada constantes na nota fiscal deverão estar vinculados à Ata de Registro de Preços, Contrato ou instrumento equivalente.

8.2.1. Se, durante a vigência dos documentos citados anteriormente, houver alterações no contrato social da empresa tais como, CNPJ, razão social, endereço, elas deverão ser informadas por meio formal à Seção de Gestão de Contratos do Sesc-GO.

8.3. O faturamento e local de entrega deverá ocorrer conforme dados abaixo:

8.3.1. DO FATURAMENTO:

Administração Regional em Goiás.

Razão Social: SERVIÇO SOCIAL DO COMÉRCIO - SESC

CNPJ: 03.671.444/0001-47 I.E: Imune.

Endereço: Rua 19 nº 260, Setor Central, Goiânia – GO. CEP: 74.030-090.

8.3.2. DA ENTREGA:

Administração Regional em Goiás.

Endereço: Rua 31-A, nº 43, Setor Aeroporto, Goiânia-Goiás, SENAC-GO.

CLÁUSULA NONA – REAJUSTE

O preço proposto, não poderá ser reajustado antes de decorrido 12 (doze) meses de contrato. No caso de as prorrogações ultrapassarem os 12 (doze) meses, o reajuste poderá ser feito com base na variação acumulada do ICTI - Ipea (Índice de Custos de Tecnologia da Informação), dos últimos 12 (doze) meses anteriores ao penúltimo mês de vencimento do contrato em vigor, mediante aditivo e acordo entre as partes.

CLÁUSULA DECIMA – OBRIGAÇÕES DA CONTRATANTE

10.1. Realizar os pagamentos em até 15 (quinze) dias subsequentes à entrega da nota fiscal, desde que os materiais ou serviços tenham sido conferidos e aceitos pelo Sesc/GO.

10.2. A contratante realizará a conferência e a fiscalização na entrega do produto, assegurando-se da qualidade, quantidade e especificações do item solicitado.

10.3. Comunicar a contratada, por escrito, sobre imperfeições, falhas, ou irregularidades verificadas no objeto fornecido, para que seja substituído.

10.4. Acompanhar e fiscalizar o cumprimento das obrigações da contratada, através de comissão/servidor especialmente designado, conforme CLÁUSULA DÉCIMA SEXTA, item 17.2, deste contrato.

10.5. O Sesc/GO reserva o direito de não receber os produtos em desacordo com as especificações e condições constantes neste Contrato.

CLÁUSULA DÉCIMA PRIMEIRA – OBRIGAÇÕES DA CONTRATADA

11.1. A contratada deverá manter em seu corpo funcional um profissional com certificação PMP (Project Management Professional) durante o período de validade do contrato.

11.2. A contratada deverá emitir um relatório referente a Lei Geral de Proteção de Dados (LGPD) de toda a solução ofertada, evidenciando quais aspectos da lei a solução está aderente. Esse relatório deve ser emitido por profissional com certificação de mercado específica para proteção de dados;

11.3. A contratada cumprirá fielmente com as obrigações assumidas por meio deste Contrato, podendo a contratante aplicar ao vencedor as penalidades previstas, em caso de não cumprimento do estabelecido.

11.4. Correrá por conta da contratada qualquer prejuízo causado ao produto em decorrência do transporte.

11.5. Cabe à contratada o cumprimento dos prazos de entrega, nas datas, condições e local definido, nas quantidades contratadas.

11.6. Em nenhuma hipótese a contratada poderá alegar desconhecimento, incompreensão, dúvidas ou esquecimento de qualquer detalhe especificado neste Contrato.

11.7. Substituir sem custos adicionais para o Sesc todo o produto inadequado para o uso ou em desacordo com o padrão exigido neste Contrato.

11.8. Enquanto não ocorrer a substituição ou troca do objeto desta licitação, a empresa será considerada em atraso e, em consequência, sujeita as penalidades.

11.9. Atender prontamente a quaisquer exigências do Sesc, inerentes ao objeto do presente Contrato;

11.10. Cabe à contratada consultar com antecedência os seus fornecedores quanto aos prazos de entrega do produto especificado, não cabendo, portanto, a justificativa de atraso do fornecimento devido ao não cumprimento da entrega por parte do fornecedor.

11.11. Cabe contratada responsabilizar-se por despesas, tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução do contrato.

CLÁUSULA DÉCIMA SEGUNDA - DA SUBCONTRATAÇÃO

A contratada não poderá transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada.

CLÁUSULA DÉCIMA TERCEIRA – DAS PENALIDADES

13.1. Em caso de inadimplemento total, parcial, sem motivo de força maior, na execução do objeto deste contrato, a CONTRATADA estará sujeita, no que couber, e garantida a prévia defesa, às seguintes penalidades:

I - Por atraso injustificado ou por inexecução parcial:

a) Advertência;

b) Multa de 0,3% (zero virgula três por cento) ao dia incidente sobre o valor correspondente ao material ou serviço objeto desta licitação; e

c) Suspensão temporária de participar em licitação e impedimento de contratar com o Sesc-GO, por um prazo de até 2 (dois) anos.

II - Por inexecução total do objeto desta licitação:

a) Advertência;

b) Multa de 10% (dez por cento) sobre o valor total do Contrato; e

c) Suspensão temporária de participar em licitação e impedimento de contratar com o Sesc-GO, por um prazo de até 2 (dois) anos.

13.2. As multas estabelecidas nesta cláusula são independentes e terão aplicação cumulativa e consecutivamente, de acordo com as normas que regeram a licitação, mas somente serão definitivas depois de exaurida a fase de defesa prévia da CONTRATADA.

13.3. Quando não pagos em dinheiro pela CONTRATADA, os valores das multas eventualmente aplicadas serão deduzidos pela CONTRATANTE, dos pagamentos devidos e, quando for o caso, cobrado judicialmente.

13.4. Quando se tratar de inexecução parcial, o valor da multa será proporcional ao serviço que deixou de ser executado.

13.5. Em caso de reincidência por atraso injustificado será a CONTRATADA penalizada nos termos do art. 32, da Resolução Sesc nº 1.252/2012-CN.

CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO

14.1. O CONTRATANTE poderá rescindir o presente contrato, sem que assista à CONTRATADA qualquer direito de indenização, nos seguintes casos:

a) Conveniência administrativa, mediante comunicação, por escrito, à CONTRATADA, com 30 (trinta) dias de antecedência;

b) Não cumprimento ou o cumprimento irregular de cláusulas contratuais, especificações ou prazos;

c) A decretação de falência ou a instauração de insolvência, dissolução da CONTRATADA;

d) A ocorrência de caso fortuito ou força maior, regularmente comprovada, impeditiva da execução do contrato.

14.2. Os casos de rescisão contratual serão formalmente motivados pela CONTRATANTE.

14.3. O termo de rescisão será precedido por Relatório indicativo dos seguintes aspectos, conforme o caso:

14.3.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

14.3.2. Relação dos pagamentos já efetuados e ainda devidos;

14.3.3. Indenizações e multas, se houver.

CLÁUSULA DÉCIMA QUINTA – DAS ALTERAÇÕES

15.1. Eventuais alterações contratuais reger-se-ão por meio de aditivo contratual, nos termos do Art. 29 da Resolução Sesc nº 1.252/2012-CN.

15.2. A CONTRATANTE poderá a qualquer momento, determinar a supressão ou acréscimo do objeto contratado, até o limite de 25% (vinte e cinco por cento).

15.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, mediante acordo das partes.

CLÁUSULA DÉCIMA SEXTA - DOS CASOS OMISSOS.

Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Resolução Sesc nº 1.252/2012-CN bem como por normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SETIMA – DA GESTÃO E FISCALIZAÇÃO DO CONTRATO

17.1. A gestão, o controle, bem como todos os atos preparatórios para formalização dos procedimentos que envolvam a prorrogação, alteração, reequilíbrio, extinção do contrato e demais comunicações relativas a este ajuste deverão ser efetuadas, protocoladas ou transmitidas para a Seção de Gestão de Contratos localizada na Rua 31 - A, nº 43, Qd. 26A, Lt. 27-E, Setor Aeroporto, Goiânia-GO, telefone (62) 3221-0607 / 3219-5199.

17.2. A fiscalização do presente instrumento será exercida conforme abaixo:

- a) Fiscal: Saúle Tassara Bortolani, Matrícula: 7224 CPF: 706.932.421-91. Analista de Infraestrutura.
- b) Suplente: Plinio Marcos Mendes Carneiro, Matrícula: 1382 CPF: 001.517.821-80. Chefe da Seção de Infraestrutura e Suporte.

CLÁUSULA DÉCIMA OITAVA – FORO

Fica eleito pelas partes o Foro da cidade de Goiânia/GO para dirimir as questões oriundas deste contrato.

E, por estarem assim justos e contratados, firmam o presente instrumento em 02 (duas) vias de igual teor e forma, na presença das testemunhas abaixo, para que produza os seus efeitos legais.

....., de..... de

CONTRATANTE
Representante legal –

CONTRATADA
Representante legal -

TESTEMUNHAS:

1- _____

CPF:

2- _____

CPF: