



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

ANEXO II – REQUISITOS TÉCNICOS DA SOLUÇÃO

Pregão Eletrônico nº ____/2022 – Processo Administrativo nº 11512/2021

1. ITEM 1 - SERVIDOR DE PROPÓSITO GERAL PARA BACKUP COM 60 (SESSENTA) TB DE CAPACIDADE ÚTIL E GARANTIA ON-SITE DE 60 (SESSENTA) MESES

1.1. CARACTERÍSTICAS GERAIS

- 1.1.1. 1 (um) Servidor biprocessado de arquitetura x64 com processador de tecnologia multi-core;
- 1.1.2. Compatível com rack padrão 19’;
- 1.1.3. Ocupar, no máximo, 2U de espaço no rack;
- 1.1.4. Possuir botão liga/desliga na parte frontal do equipamento;
- 1.1.5. Vir acompanhado dos acessórios necessários para montagem em rack padrão 19’.
- 1.1.6. 2 (dois) processadores, originalmente concebido para servidores por equipamento. O padrão de arquitetura do processador deverá ser x64;
- 1.1.7. 8 (oito) núcleos físicos por processador;
- 1.1.8. Frequência base de clock de no mínimo 2,1 GHz;
- 1.1.9. Processadores devem incorporar a tecnologia HT, de forma a apresentar 16 vCPUs virtuais por processador ao sistema operacional;
- 1.1.10. Recurso second-level address translation (SLAT);
- 1.1.11. Deve possuir, no mínimo, 11 MB de memória cache por processador;
- 1.1.12. Processadores devem implementar mecanismos de redução de consumo de energia e controle automático para evitar superaquecimento que possa danificá-lo, e deve também implementar tecnologia para aumentar de maneira automática a frequência do clock dos processadores caso seja demandada maior capacidade de processamento pelo sistema;
- 1.1.13. Ter sido fabricados com tecnologia de litografia de, no máximo, 14nm.

1.2. MEMÓRIA RAM

- 1.2.1. No mínimo, 64 GB de memória RAM;
- 1.2.2. Memória do tipo DDR4 ECC padrão RDIMM Dual Rank x4;
- 1.2.3. Cada módulo de memória RAM deve ter, no mínimo, 2.933 MHz de velocidade;

1.3. SISTEMA

- 1.3.1. No caso de falha de qualquer um dos processadores, o servidor deverá executar automaticamente a reinicialização, sem necessidade de intervenção manual;
- 1.3.2. Suporte a tecnologia de virtualização VT-d (Virtualization Technology for Directed I/O), IOMMU (input/output memory management unit), ou equivalente;
- 1.3.3. Suporte a Hardware-enforced Data Execution Prevention (DEP);
- 1.3.4. Suporte a DMA remapping;



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

1.3.5. Suporte a Access control services (ACS);

1.3.6. O BIOS deverá ser do tipo Flash Memory, utilizando memória não volátil e eletricamente reprogramável;

1.3.7. A inicialização do servidor deverá ser realizada na seqüência definida pelo usuário, via cartão de memória e/ou CD-ROM e/ou disco rígido, bem como pela placa de rede;

1.3.8. Deverão possuir recursos de controle de permissão através de senhas, uma para inicializar o servidor e outra para acesso e alterações das configurações do BIOS;

1.3.9. Suporte a TPM na versão 2.0.

1.4. PORTAS DE COMUNICAÇÃO

1.4.1. Mínimo de 2 portas USB 3.0 Traseira;

1.4.2. Mínimo de 1 porta USB 3.0 Frontal;

1.4.3. Mínimo de 1 porta USB 2.0 Frontal;

1.4.4. Entrada para cartão SDcard;

1.4.5. Interface HBA FC 16Gb com 2 portas ou interface SAS 12Gb a depender da interface da biblioteca de fitas (item 3).

1.5. INTERFACE DE REDE

1.5.1. Interface de rede com 2 portas do tipo 10Gb SFP+ (10GBASE-SR) com respectivos mini-GBICs LC;

1.5.2. Interface de rede com 2 portas do tipo 1Gb RJ45 (podendo ser onboard);

1.5.3. Caso o módulo mini-GBIC não acompanhe a interface de rede este deverá ser fornecido junto com a interface;

1.5.4. Full Duplex;

1.5.5. Recursos de Wake on LAN (WOL);

1.5.6. Suporte a Jumbo Frames (MTU ate 9k);

1.5.7. Múltiplas filas;

1.5.8. TCP Segmentation Offload ;

1.5.9. Virtual Machine Device Queues (VMDq);

1.5.10. Suporte a VLAN e inserção de TAG Vlan;

1.5.11. Todas as placas off-board devem ser preferencialmente do mesmo fabricante e mesmo quando não houver essa possibilidade deverão estar sempre cobertas pela garantia geral do servidor;

1.5.12. Todos os gbics das placas óticas devem ser preferencialmente do mesmo fabricante e mesmo quando não houver essa possibilidade deverão estar sempre cobertos pela garantia geral do servidor;

1.5.13. Virtual Machine Device Queues (VMDq) ou RDMA (Remote Direct Memory Access). Outras tecnologias de otimização de tráfego para ambientes virtualizados serão aceitas, desde que o fornecedor comprove através de documentação do fabricante que a referida tecnologia é capaz



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

de otimizar o tratamento de pacotes de rede em servidores virtualizados com os hypervisores ESXi (VMware) e Hyper-V (Microsoft), em no mínimo 20%;

1.5.14. A interface deverá vir completa, todos os itens deverão ser compatíveis entre si, de maneira que permita o seu perfeito funcionamento.

1.6. VÍDEO

1.6.1. 1 saída de vídeo VGA traseira;

1.6.2. Saída de vídeo adicional frontal.

1.7. CONTROLADORA RAID

1.7.1. Conexão dos discos rígidos com suporte a tecnologia hotswap;

1.7.2. Suporte aos padrões SAS 12Gb/s e SATA 6Gb/s;

1.7.3. Controladora RAID dedicada com suporte a RAID 0/1/10/5/6. Se for necessário algum licenciamento para habilitar os modos RAID especificados, tal licenciamento deve acompanhar a controladora;

1.7.4. Memória cache de no mínimo 4 GB, independente da memória RAM do servidor, e está deve vir devidamente instalada;

1.7.5. Controladora com bateria para proteção dos dados em caso de falta de energia;

1.7.6. A configuração de RAID deve abranger todos os slots para discos rígidos fornecidos;

1.7.7. Recursos de hot swap (troca de disco sem a necessidade de reinicializar o servidor) para as unidades de disco rígido, permitindo a detecção e recuperação automática de falhas e reconstrução de discos dos volumes de RAID, de forma automática, sem impacto para as aplicações e sem necessidade de reiniciar o equipamento;

1.7.8. Tecnologia SMART para detecção de problemas potenciais.

1.8. ARMAZENAMENTO PRIMÁRIO

1.8.1. Mínimo de 2 discos SSD SAS;

1.8.2. 2,5 polegadas de tamanho;

1.8.3. Capacidade mínima de armazenamento por disco de 400 GB;

1.9. ARMAZENAMENTO SECUNDÁRIO

1.9.1. Discos HDD SAS, totalizando 60 TB líquidos após o uso de pelo menos raid 6;

1.9.2. Não serão aceitos discos em gabinetes externos ao servidor;

1.10. UNIDADE DE LEITURA E GRAVAÇÃO – DVD-RW

1.10.1. 1 (um) unidade de leitura e gravação DVD-RW por servidor interna ao gabinete.

1.11. ALIMENTAÇÃO

1.11.1. Fontes redundantes, de 100 a 240 VAC, e 50 a 60 Hz, com a potência adequada ao pleno funcionamento do equipamento;

1.11.2. Fontes hot-pluggable permitindo a substituição de qualquer uma das fontes em caso de falha sem parada ou comprometimento do funcionamento do equipamento;



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

1.11.3. Certificação 80Plus, no mínimo, categoria PLATINUM;

1.11.4. Tomadas 2P+T, conforme norma brasileira NBR 14136.

1.12. GERENCIAMENTO

1.12.1. Deverá haver interface ethernet exclusiva para gerenciamento remoto e também possibilitar o uso desse recurso através de interface ethernet compartilhada usando o recurso de vlan;

1.12.2. Gerenciamento remoto com, no mínimo, as funções de ligar, desligar, reinicializar e acessar o console do servidor remotamente;

1.12.3. Console Virtual;

1.12.4. Interface de linha de comando;

1.12.5. Interface de gerenciamento deve ser baseada em HTML5;

1.12.6. Acesso via SSH;

1.12.7. Suporte aos protocolos SNMP v2c/3 e IPMI.

2. ITEM 2 - LICENCIAMENTO PERPÉTUO DE WINDOWS SERVER STANDARD (ÚLTIMA VERSÃO CORRENTE)

2.1. CARACTERÍSTICAS GERAIS

2.1.1. O Sistema operacional Windows Server deverá ser instalado no servidor especificado no item 1 acima.

2.1.2. Cada unidade deste item deverá ser capaz de licenciar 01 (um) servidor com 02 (dois) processadores de até 8 núcleos físicos cada, totalizando 16 núcleos por servidor;

2.1.3. Deverá permitir o uso da versão mais atual do Windows Server Standard de forma perpétua e as suas atualizações/suporte oficial do FABRICANTE;

2.1.4. A CONTRATADA deverá prover meios de conferir ou requisitar, a qualquer tempo, as licenças adquiridas;

2.1.5. Enviar por e-mail ou informar o link para download do sistema operacional e licenças;

2.1.6. Permitir a consulta no site da fabricante, a qualquer tempo, pelas chaves de licenças adquiridas;

2.1.7. A CONTRATADA deverá fornecer sem custo adicional todos os softwares, documentação e manuais, drivers, e outros necessários para a instalação e interligação, configuração e o perfeito funcionamento dos Sistemas Operacionais Licenciados, garantindo assim a entrega e perfeito funcionamento da solução, mesmo que não especificados.

3. ITEM 3 - SUBSCRIÇÃO DE SOFTWARE DE BACKUP PARA 8 HOSTS (OU EQUIVALENTE A 128 NÚCLEOS OU 80 MÁQUINAS VIRTUAIS) - PERÍODO DE 60 (SESSENTA) MESES

3.1. CARACTERÍSTICAS GERAIS

3.1.1. A solução ofertada deverá, obrigatoriamente, atender às especificações mínimas previstas, quanto às funcionalidades, integrações e compatibilidades com o ambiente virtualizado da CONTRATANTE para criação de backups e recuperação desses ambientes com o mínimo de indisponibilidade e reestruturação da parte física necessária, de forma que recupere, total e/ou



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

granular, qualquer item assegurado por sua funcionalidade de backup e restauração;

3.1.2. Deverá ser fornecido licenciamento perpétuo do software, de propriedade e registrado para a CONTRATANTE, na modalidade de capacidade por quantidade de processadores (sockets) para o ambiente virtualizado, com suporte para backup e restore de dados, em sua versão acadêmica (quando houver).

3.1.3. Cada licença de software licenciará um processador físico (CPU Socket) do servidor hypervisor, do ambiente virtualizado (provedor/host das máquinas virtuais), e não deverá estar limitado à quantidade de máquinas virtuais ou quantidade de dados geridas e movimentadas por essa estrutura;

3.1.4. A CONTRATADA deve fornecer sem custo adicional todos os softwares, documentação e manuais, drivers, e outros necessários para a instalação e interligação, configuração e o perfeito funcionamento dos Sistemas Operacionais Licenciados, garantindo assim a entrega e perfeito funcionamento da solução de backup, mesmo que não especificados.

3.2. CARACTERÍSTICAS ESPECÍFICAS

3.2.1. Deverá incluir funcionalidades de proteção (backup) e replicação integradas em uma única solução;

3.2.2. Não deverá necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais;

3.2.3. Deverá garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através das soluções de virtualização VMware ou Hyper-V;

3.2.4. Ser compatível nativamente com todos os ambientes de virtualização abaixo:

3.2.4.1. VMWare VCenter Server Appliance (VCSA) e VSphere Esxi versões 5.5 e superiores;

3.2.4.2. Microsoft Hyper-V 2012 R2 Standalone e versões superiores;

3.2.4.3. Nuvem da Amazon Web Service;

3.2.4.4. Nuvem da Microsoft Azure;

3.2.4.5. Nuvem da Google Cloud;

3.2.5. Ser compatível nativamente com todas as aplicações abaixo:

3.2.5.1. Microsoft Active Directory 2012 R2 e superiores;

3.2.5.2. Microsoft Exchange 2016 e versões superiores;

3.2.5.3. Microsoft FileServer, FailoverCluster 2012 e superiores;

3.2.5.4. Microsoft SQL Server 2012 e superiores;

3.2.5.5. PostgreSQL 11.6 e superiores;

3.2.5.6. MariaDB 10.2.13 e superiores;

3.2.5.7. Microsoft 365.

3.2.6. Deverá ter a capacidade de replicação de dados armazenados entre storages e/ou máquinas de configuração e de fabricantes diferentes;

3.2.7. Possuir a capacidade de efetuar backup para disco e fita com retenções, através de



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

políticas predefinidas e agendadas;

- 3.2.8.** Para um dado armazenado deve haver a possibilidade de alterar o período de retenção;
- 3.2.9.** 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;
- 3.2.10.** Deverá prover a desduplicação e compressão durante a operação de qualquer backup sem a necessidade de hardware de terceiros (appliance duplicadora);
- 3.2.11.** Deverá possibilitar a cópia de uma máquina virtual completa ou discos virtuais específicos;
- 3.2.12.** Deverá ser fornecida com ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador (vCenter);
- 3.2.13.** Deverá ter a capacidade de integração através de API's dos fabricantes de infraestrutura virtualizada para a proteção de dados;
- 3.2.14.** 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);
- 3.2.15.** Suportar qualquer tecnologia utilizada na infraestrutura de armazenamento como destino do backup – DAS, NAS e SAN, sem prejuízos das demais funcionalidades suportadas pelo software;
- 3.2.16.** Deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (backup), a saber:
 - 3.2.16.1.** Diretamente através de Storage Area Network (SAN);
 - 3.2.16.2.** Diretamente do storage, através do hypervisor I/O (Virtual Appliance);
 - 3.2.16.3.** Mediante uso da rede local (LAN);
 - 3.2.16.4.** Diretamente do snapshot do storage onde os dados das VMs estejam armazenados.
- 3.2.17.** Deverá manter um backup sintético, eliminando assim a necessidade de realizar backups completos (full) periódicos, incremental permanente, o que permitirá economizar tempo e espaço;
- 3.2.18.** Deverá possibilitar a inicialização de uma máquina virtual diretamente do arquivo de backup, inclusive sem necessidade de "hidratação" dos dados "desduplicados e "comprimidos";
- 3.2.19.** 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;
- 3.2.20.** 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 uma máquina virtual;
- 3.2.21.** Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows;
- 3.2.22.** Deverá permitir realizar a truncagem de logs transacionais (transaction logs) para máquinas virtuais com SQL Server e PostgreSQL;
- 3.2.23.** Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

máquina virtual do resultado da execução de seus trabalhos;

3.2.24. Deverá permitir recuperar no nível de objetos e arquivos de qualquer aplicação virtualizada, em qualquer sistema operacional, utilizando as ferramentas de gestão das aplicações existentes;

3.2.25. Deverá incluir ferramentas de recuperação sem a necessidade de agentes adicionais para o ambiente virtualizado, sem a necessidade de recuperar os arquivos da máquina virtual como um todo ou reiniciar a mesma (recuperação granular), principalmente para os seguintes serviços:

3.2.25.1. Microsoft Active Directory 2012 R2, possibilitando recuperar objetos individuais, tais como usuários, recuperação de senhas de usuários e computadores, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory entre outros sem a necessidade de usar o agente tanto para backup e restauração;

3.2.25.2. Microsoft SQL Server 2012 e superior, possibilitando recuperar objetos individuais, tais como bases, tabelas, registros, entre outros;

3.2.25.3. Microsoft Sharepoint 2013;

3.2.25.4. PostgreSQL 11 e superior;

3.2.25.5. Microsoft 365, possibilitando recuperar objetos individuais, tais como arquivos, mensagens, etc.

3.2.26. Permitir a integração com o Microsoft SQL Server 2012 e versões superiores:

3.2.26.1. Executar backup/recovery de bases de dados do SQL Server de forma “online”, ou seja, sem a parada do banco;

3.2.26.2. Executar backup de logs transacionais, possibilitando a criação de rotina de backup para que ocorra em intervalos mínimos de 1 (uma) hora;

3.2.26.3. Permitir a configuração de forma que após o backup dos logs transacionais, os mesmos sejam mantidos ou deletados;

3.2.26.4. Permitir a recuperação granular a nível individual de banco de dados, no mesmo servidor e em servidor remoto.

3.2.27. Permitir a integração com o PostgreSQL 11 e versões superiores:

3.2.27.1. Executar backup/recovery de bases de dados do SQL de forma “online”, ou seja, sem a parada do banco;

3.2.27.2. Executar backup de logs transacionais, possibilitando a criação de rotina de backup para que ocorra em intervalos mínimos de 1 (uma) hora;

3.2.27.3. Permitir a configuração de forma que, após o backup dos logs transacionais os mesmos sejam mantidos ou deletados;

3.2.27.4. Permitir a recuperação granular a nível individual de banco de dados, no mesmo servidor e em servidor remoto.

3.2.28. Permitir a recuperação do banco de dados em um momento de tempo específico;

3.2.29. Permitir a integração com Microsoft Active Directory 2012 R2 e versões superiores:

3.2.30. Permitir a integração com ambiente virtual VMWare VCenter Server Appliance 5.5 e



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

superiores e deverá executar backup/recovery com as seguintes características:

- 3.2.30.1.** Permitir a conexão com o VCenter e a exploração (descoberta) automática das máquinas virtuais;
- 3.2.30.2.** Realizar o backup/recovery de Máquinas Virtual sem a necessidade de instalação de agente;
- 3.2.30.3.** Realizar o armazenamento de backup das Máquinas Virtuais de maneira deduplicada;
- 3.2.30.4.** Ser compatível com a funcionalidade VMWare VSphere CBT (Changed Block Tracking), ou seja, em vez de verificar todo o arquivo VMFS (Virtual Machine File System) deverá consultar a API (Application Programming Interface) do VMWare para descobrir somente os blocos que foram alterados desde do último backup.
- 3.2.30.5.** Permitir a inclusão automática de máquinas virtuais sem backup em seleções de backup anteriores;
- 3.2.30.6.** Permitir o backup das máquinas virtuais através de Snapshot executados diretamente nos Storages;
- 3.2.30.7.** Realizar a restauração da imagem completa da máquina virtual dentro do VMWare;
- 3.2.30.8.** Permitir redirecionar a restauração de uma da máquina virtual para uma pasta, datastore, hospedeiro ou rede alternativos;
- 3.2.30.9.** Ser capaz e iniciar a execução da máquina virtual diretamente a partir do seu arquivo de backup, sem a necessidade de esperar o término do processo de restauração.
- 3.2.31.** Deverá ser possível executar uma ou várias máquinas virtuais a partir do arquivo de backup, em um ambiente isolado de forma automática através de schedule, sem a necessidade de espaço de armazenamento adicional e sem modificar os arquivos de backup (read-only), para criação de ambiente de homologação, teste, etc.;
- 3.2.32.** Permitir a comunicação de rede entre as Máquinas Virtuais dentro deste ambiente isolado;
- 3.2.33.** Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção;
- 3.2.34.** Deverá possuir integração com o ambiente VMware vSphere Client e Hyper-V, a fim de permitir o monitoramento da infraestrutura de backup diretamente da console de gerência do ambiente VMware, com visibilidade detalhada e geral do estado dos trabalhos e recursos de backup;
- 3.2.35.** Deverá operar em ambientes virtualizados através das soluções de virtualização, incluindo: VMware vSphere 5.5, Hyper-V 2012 R2 e superiores;
- 3.2.36.** Deverá ter a capacidade de monitoramento em tempo real, sem a necessidade de agentes, da infraestrutura virtual e de backup, inclusive máquinas virtuais, para VMware ou Hyper-V, com notificação de problemas de backup e desempenho, com geração de alertas e base de conhecimento embutida para resolução dos mesmos;
- 3.2.37.** Deverá ter a capacidade de monitoramento e análise de capacidade do ambiente para crescimento, ajustes e planejamentos de crescimento;



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

3.2.38. Deverá regular de forma dinâmica e parametrizável, o uso de recursos computacionais, de forma que se possa diminuir o impacto na infraestrutura de produção, durante as atividades de backup;

3.2.39. Deverá permitir um método de fácil recuperação, desde ambientes de contingência, com as ações pré-configuradas para evitar ações manuais em caso de desastre, similar a um botão de emergência;

3.2.40. A solução deverá estar configurada para recuperação de desastres com os mecanismos de exportação do catálogo implementados e a procedimentos de recuperação documentados;

3.2.41. 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;

3.2.42. 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;

3.2.43. Deverá integrar uma solução unificada de monitoração de ambientes virtualizados, com fornecimento de relatórios capazes de apresentar informações do tipo:

3.2.43.1. Relatórios que permitam o planejamento de capacidade;

3.2.43.2. Relatórios que permitam determinar a ineficiência dos recursos em uso;

3.2.43.3. Relatórios que facilitem a visibilidade de tendências negativas e anomalias;

3.2.43.4. Quadros de controle claros, apresentáveis e integráveis em sites web.

3.2.44. A licença de software de backup deverá, nativamente, ser capaz de emitir relatórios com informações completas, conforme subitens:

3.2.44.1. Permitir acesso aos relatórios através de interface gráfica ou web;

3.2.44.2. Suportar a geração de relatórios gráficos customizáveis de atividades de backups/restores, contendo: Horário de início e término dos jobs; Tempo de duração dos jobs; Todos os jobs em execução; Status (situação) de execução dos jobs; Relação e porcentagem de jobs executados por status, como por exemplo: com sucesso e com erros; Logs dos jobs; Volume de dados na origem e no destino, total e por job, por período de tempo, por localidade e por host (físico ou virtual); Tendência de crescimento; Dados históricos de, no mínimo, 24 (vinte e quatro) meses.

3.2.44.3. Suportar a geração de relatórios gráficos customizáveis de atividades de backups, contendo: Identificação da ocupação nos destinos de backups: uso de disco e fita; Porcentagem de dados desduplicados; Taxa de desduplicação e compressão;

3.2.44.4. Permitir a geração de relatórios baseados na utilização de recursos, identificando restrições associadas a aplicativos específicos;

3.2.44.5. Permitir a geração de relatórios baseados em alertas pré-definidos, com o objetivo de reportar eventos ocorridos do ambiente operacional de backup e restore.

3.3. GERENCIAMENTO E CONFIGURAÇÃO

3.3.1. O software de backup/recovery deverá:

3.3.1.1. Possuir módulo de gerenciamento central com interface gráfica (ou web) e linha



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

de comando (interface CLI) responsáveis pela administração de todas as operações de backup/recovery, configurações, gerenciamento, monitoração, criação/atualização de políticas do ambiente e rotinas associadas à proteção de dados de todos os sites;

3.3.1.2. Suportar a instalação do módulo de gerenciamento e da base de dados do catálogo de metadados nos sistemas operacionais: Microsoft Windows Server 2012 R2 e versões superiores ou Linux;

3.3.1.3. Possuir gerenciamento das operações da infraestrutura de backup em modo gráfico, que permita o monitoramento em tempo real das rotinas de backup/recovery e status dos dispositivos e clientes de todo o ambiente ;

3.3.1.4. Possuir dashboards com suporte a visualização de todas as rotinas de backup/recovery, com opções de gerar relatórios on-line e envio por e-mail;

3.3.1.5. Permitir que as tarefas abaixo sejam realizadas pela interface gráfica central, sem a necessidade de scripts e sem a necessidade de acessar a interface do cliente:

3.3.1.5.1. Instalar e aplicar patches/upgrades de agentes remotamente;

3.3.1.5.2. Configurar backup de clientes de forma remota, ou seja, toda a configuração do backup que o cliente irá executar deve ser feita na própria console central, sem a necessidade de ter que configurar localmente o cliente;

3.3.1.5.3. Executar a restauração de backup de forma remota, ou seja, na console central seleciona-se o backup, com as integrações descritas e para onde será realizada a restauração remota.

3.3.1.6. Correlacionar a execução de trabalhos de backup e réplica com os objetos do ambiente virtual;

3.3.1.7. Oferecer a capacidade de relatar o cumprimento das políticas de proteção de dados e disponibilidade de acordo com parâmetros definidos;

3.3.1.8. Suportar múltiplas operações dos componentes/servidores participantes da estrutura de backup, permitindo atividades de backup e recuperação simultâneas;

3.3.1.9. Suportar repositório de backup com aumento de escala ilimitado para o armazenamento de dados com suporte aos seguintes sistemas de armazenamento:

3.3.1.9.1. Microsoft Windows;

3.3.1.9.2. Linux;

3.3.1.9.3. Pastas compartilhadas (SMB, NFS);

3.3.1.9.4. Appliances desduplicadoras;

3.3.1.9.5. Storages do tipo SAN e NAS;

3.3.1.9.6. Nuvem (Amazon AWS, Microsoft Azure, Google Cloud).

3.3.1.10. Permitir a seleção de um destino de armazenamento do backup em um provedor de serviços em nuvem (BaaS – Backup as a Service);

3.3.1.11. Permitir a seleção de um destino para a réplica dos dados que poderá ser em um provedor de serviços em nuvem (DRaaS – DR as a Service);

3.3.1.12. Possuir integração com armazenamento de objetos em nuvem compatíveis com



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

Amazon S3, Azure Blob Storage, Google Cloud Backup e qualquer outro dispositivo de armazenamento local compatível com S3;

3.3.1.13. Realizar arquivamento dos dados de backup nos dispositivos e locais de armazenamento de objetos compatíveis com S3;

3.3.1.14. Em caso de desastre, deverá ser possível realizar a recuperação dos dados diretamente do arquivamento em nuvem;

3.3.1.15. Possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem;

3.3.1.16. Ser ofertada a versão mais atual do software de backup, liberada oficialmente pelo fabricante do software;

3.3.1.17. 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 e com direito a upgrade futuro para versão mais atual, sem nenhum ônus adicional;

3.3.1.18. O prazo de cobertura da manutenção de software, com licença por subscrição, deverá ser de, no mínimo, 60 (sessenta) meses com suporte técnico de 24 x 7, contados a partir da data do recebimento definitivo das licenças de software.

4. ITEM 4 - BIBLIOTECA DE FITA (DE TECNOLOGIA NO MÍNIMO LTO 7) COM GARANTIA ON-SITE DE 60 (SESENTA) MESES

4.1. CARACTERÍSTICAS GERAIS

4.1.1. Possuir 01 (um) drive padrão Ultrium LTO-7;

4.1.2. Os drives devem possuir conectividade no padrão SAS (Serial Attached SCSI), com velocidade mínima de 6 Gbps (seis gigabits por segundo) ou FC (Fibre Channel), com velocidade mínima de 8 Gbps (oito gigabits por segundo);

4.1.3. Cada drive deverá permitir taxa de transferência mínima de dados nativa (sem compressão) de 300MB/s (trezentos megabytes por segundo), considerando cartuchos de fita tipo LTO-7;

4.1.4. Deve possuir pelo menos 8 (oito) slots para cartuchos de fita internos em um mesmo gabinete;

4.1.5. Deve suportar cartuchos de fita no padrão Ultrium LTO-7 com capacidade de 6 TB (seis terabytes), sem compressão, e 15 TB (quinze terabytes), com compressão;

4.1.6. Suportar protocolo LTFs;

4.1.7. Deve estar incluso todo o licenciamento de uso perpétuo necessário para a utilização dos drives, slots para cartuchos e software de gerenciamento do equipamento ofertado.

4.1.8. Possuir biblioteca interna única de cartuchos de fita, ou seja, um único chassi, com mecanismo robotizado para a montagem automática das fitas nos tape drives sem a intervenção do operador;

4.1.9. Deverão ser capazes de efetuar as montagens tanto de cartuchos de fita de dados quanto de cartuchos de fita de limpeza (tape cleaner cartridge);

4.1.10. Deve possuir painel frontal para operações de configuração, diagnóstico e visualização de



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

status;

4.1.11. Deve realizar o inventário de todas as fitas da fitoteca e o carregamento das fitas existentes na estação de entrada/saída (I/O Station ou Magazine) de fitas – sem a interrupção do funcionamento e na condição ativa ou online;

4.1.12. Deve possuir leitor de código de barras (bar code reader) para reconhecimento dos cartuchos de fita através da leitura do código de barras nas etiquetas (labels) padrão de mercado.

4.1.13. Deve possuir interface de rede dedicada para gerenciamento remoto de no mínimo 100 Mbps (100BASE-TX);

4.1.14. Deve ser compatível e instalável em rack padrão 19” e deve vir acompanhado de todos os acessórios necessários à sua instalação (trilhos, parafusos, etc.), assim como cabos elétricos e lógicos apropriados;

4.1.15. Possuir 02 (duas) fontes de alimentação elétrica independentes e redundantes, capazes de operar entre 100 a 240 VAC por reconhecimento automático do nível de tensão;

4.1.16. Possuir tamanho máximo de 2U;

4.1.17. O fabricante deverá, obrigatoriamente, constar na lista de *compliance verified license* do site <http://www.lto.org/participants/>.

4.2. Cartuchos e acessórios

4.2.1. Devem ser fornecidos 2 (dois) cabos para realizar a conexão ponto-a-ponto dos tape drives com equipamento servidor (adaptador tipo HBA SAS ou FC com conector apropriado).

5. ITEM 5 - CARTUCHO DE FITA PARA LIMPEZA COM GARANTIA DE 12 (DOZE) MESES

5.1.1. Devem ser fornecidos 02 (dois) cartuchos de fita de limpeza LTO (tape cleaner cartridge), compatíveis com os drives LTO-7, incluindo as respectivas etiquetas;

5.1.2. Devem ser do tipo universal e compatível, obrigatoriamente, com a limpeza de drives de gravação ultrium lto-7;

5.1.3. Devem estar identificadas conforme padrão de código de barras lto;

5.1.4. Todos os produtos ofertados deverão ser novos e sem uso, entregues em embalagem original, sem vícios ou marca de violação;

5.1.5. Não serão aceitos produtos reconicionados, ou que tenham origem desconhecida, ou que sejam comercializados sem as devidas conformidades dos órgãos de fiscalização brasileiros, ou com restrições de comercialização;

5.1.6. Em caso de produto substituído, o mesmo deverá ser novo e de primeiro uso, não podendo ser reconicionado;

5.1.7. A garantia compreende a cobertura de todo e qualquer defeito, avaria, desgaste ou disfunção ocorrida no objeto, independentemente de ser ou não decorrente de falha na fabricação;

5.1.8. Durante o período da garantia concedida pelo fabricante, eventuais defeitos, falhas ou vícios nos produtos adquiridos serão de responsabilidade do fornecedor, que se incumbirá de:



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

substituir o produto que, dentro do prazo de garantia, apresentar defeito, no prazo máximo de 72 (setenta e duas) horas, por produto novo, sem uso, com qualidade, desempenho e padrões iguais ou superiores. O fornecedor se responsabilizará por eventuais acertos e tratativas com o fabricante que eventualmente se fizerem necessários.

6. ITEM 6 - CARTUCHO DE FITA PARA GRAVAÇÃO DE DADOS, COM TAMANHO MÍNIMO DE 6 TB E GARANTIA DE 12 (DOZE) MESES

- 6.1.1.** Devem ser fornecidos 10 (dez) cartuchos de fita LTO-7, incluindo as respectivas etiquetas;
- 6.1.2.** As etiquetas de identificação devem ter as seguintes características:
 - 6.1.2.1.** Possibilitar impressão em impressoras laser;
 - 6.1.2.2.** Possuir código de barras;
 - 6.1.2.3.** Ser fabricado para uso em cartuchos de fita backup do tipo LTO-7, trazendo compatibilidade com características como dimensões, contraste para leitura adequada pela biblioteca de fitas, etc.
- 6.1.3.** Possibilitar a gravação e leitura de dados;
- 6.1.4.** Tecnologia LTO-7;
- 6.1.5.** Possuir capacidade de armazenamento de 6 TB (sem compressão) / 15 TB (compressão);
- 6.1.6.** Suportar LTFS;
- 6.1.7.** Velocidade de transferência: 750 MB/segundo (compactado); 300 MB/segundo (nativo);
- 6.1.8.** Ter durabilidade de no mínimo 1.000.000 de leituras;
- 6.1.9.** Proporcionar durabilidade de arquivamento de, no mínimo, 30 anos;
- 6.1.10.** Ter compatibilidade com o item 4;
- 6.1.11.** Todos os produtos ofertados deverão ser novos e sem uso, entregues em embalagem original, sem vícios ou marca de violação;
- 6.1.12.** Não serão aceitos produtos reconicionados, ou que tenham origem desconhecida, ou que sejam comercializados sem as devidas conformidades dos órgãos de fiscalização brasileiros, ou com restrições de comercialização;
- 6.1.13.** Em caso de produto substituído, o mesmo deverá ser novo e de primeiro uso, não podendo ser reconicionado;
- 6.1.14.** A garantia compreende a cobertura de todo e qualquer defeito, avaria, desgaste ou disfunção ocorrida no objeto, independentemente de ser ou não decorrente de falha na fabricação;
- 6.1.15.** Durante o período da garantia concedida pelo fabricante, eventuais defeitos, falhas ou vícios nos produtos adquiridos serão de responsabilidade do fornecedor, que se incumbirá de: substituir o produto que, dentro do prazo de garantia, apresentar defeito, no prazo máximo de 72 (setenta e duas) horas, por produto novo, sem uso, com qualidade, desempenho e padrões iguais ou superiores. O fornecedor se responsabilizará por eventuais acertos e tratativas com o fabricante que eventualmente se fizerem necessários;



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

6.1.16. Por se tratar de produto que poderá conter dados sensíveis o produto substituído não será devolvido ao fornecedor.

7. ITEM 7 - INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE BACKUP

7.1. A Contratada deverá enviar à Contratante, no prazo de até 10 (dez) dias corridos, o Plano de Implantação, o qual deverá conter, minimamente:

7.1.1. Cronograma de Instalação e Configuração da Solução de Backup;

7.1.2. Listagem com os nomes e cópias dos respectivos documentos válidos dos técnicos que entrarão nas dependências do Coren-SP para realizarem os serviços necessários;

7.1.3. Lista com os procedimentos a serem adotados pelos fiscais de Contrato do Coren-SP para a Conferência dos equipamentos físicos a serem recebidos, com suas respectivas Notas Fiscais de Remessa;

7.1.4. Procedimento de instalação e de testes a serem realizados para o pleno funcionamento da Solução, em perfeitas condições e de forma totalmente integrada ao ambiente de infraestrutura tecnológica do Coren-SP.

7.2. A Contratante realizará, no prazo de até 02 (dois) dias úteis, o Aceite ou Não do Plano de Implantação, podendo pedir esclarecimentos sobre determinados pontos.

7.2.1. No caso do Não Aceite, a Contratada deverá, no prazo de até 05 (cinco) dias corridos, apresentar plano corrigido, sendo que a Contratante terá mesmo prazo para Aprovar ou Não.

7.3. Após a entrega da versão final do Plano de Implantação, o Coren-SP emitirá Ordem de Serviço da Instalação – OSI (de acordo com o modelo do Anexo IV – Ordem de Serviço);

7.4. Modo e prazos para realização da implantação:

7.4.1. Será realizada no *data center* da Gerência de Tecnologia da Informação do Coren-SP, localizada no Edifício Sede do órgão, sito à Alameda Ribeirão Preto, nº 82, Bela Vista, São Paulo/SP, CEP 01331-001;

7.4.2. A instalação e procedimentos de configuração deverão ser antecedidos por agendamento prévio junto à Contratante e executadas, em regra, em dias úteis, no período das 07h00 às 19h00;

7.4.3. Em caráter excepcional e a critério do Coren-SP, as atividades poderão ser realizadas em dia e horários distintos do estabelecido, definidos em acordo com a Contratada;

7.5. A Contratada se obriga a se certificar de todas as condições físicas, elétricas e ambientais de instalação dos equipamentos, de acordo com padrões estabelecidos pelos fabricantes;

7.6. A instalação, configuração e ativação dos *softwares* serão realizadas por equipe(s) certificada(s) pela(s) respectiva(s) fabricante(s), para esse fim;

7.7. As atividades serão acompanhadas e supervisionadas pela equipe técnica do Setor de Infraestrutura da Gerência de Tecnologia da Informação do Coren-SP;

7.8. Todos componentes da solução deverão ser fornecidos com a versão mais atualizada dos softwares considerando-se a data de implantação;



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

7.9. O conjunto de procedimentos de instalação, configuração e ativação da solução fornecida, consistirá nas etapas a seguir, sendo previstas no Plano de Implantação discriminado acima e, que, deverão ser realizadas em conformidade com as diretrizes estabelecidas na reunião Preparatória a ter prazo indicado na Reunião Inicial:

- 7.9.1.** Instalação dos softwares em suas respectivas últimas versões estáveis;
- 7.9.2.** Instalação dos itens de hardware;
- 7.9.3.** Instalação e aplicação de todas as licenças ofertadas, caso necessário;
- 7.9.4.** Configuração de rede;
- 7.9.5.** Configuração de Alta Disponibilidade, caso necessário;
- 7.9.6.** Configuração de identificação de usuário;
- 7.9.7.** Configuração de armazenamento;
- 7.9.8.** Configuração das políticas de segurança e políticas de backup da informação;
- 7.9.9.** Testes de validação da instalação e configuração.

7.10. Caso seja necessário realizar paradas ou interrupções de acesso ao ambiente, tais eventos deverão ser planejados com a máxima mitigação de riscos e deverão ocorrer fora do horário de expediente administrativo do Coren-SP (isto é, a partir das 18h00);

7.11. A Contratada será responsável por prover todo e qualquer ferramental necessário para a execução das atividades, não devendo incorrer à Contratante qualquer ônus adicional para a realização dessas atividades.

7.11.1. A ocorrência de impactos no ambiente, não planejados, estará sujeita à aplicação de multas e/ou glosas em cima do objeto do contrato;

7.12. A Solução contratada deverá ser instalada, configurada e disponibilizada para uso em regime de produção em até 10 (dez) dias corridos, contados da data de recebimento da OSI pela Contratada.

7.13. Após a completa instalação, configuração e ativação da Solução, a Contratada deverá produzir documentação relativa a todo trabalho realizado, isto é, o RELATÓRIO FINAL DE IMPLANTAÇÃO, correspondente ao *'as built'* do projeto. Neste documento deverão constar todas as informações geradas pela CONTRATADA abordando os aspectos de arquitetura implantada, configuração, testes e integração ao ambiente.

7.13.1. A apresentação do Relatório Final de Implantação será considerada como requisito para os procedimentos de recebimento provisório e definitivo dos itens da Solução.

8. ITEM 8 - REPASSE DE CONHECIMENTO

8.1. A Contratante solicitará a realização do Repasse de Conhecimento por intermédio de Ordem de Serviço de Treinamento (OST) e deverá **ser realizado em até 15 (quinze) dias úteis contados a partir da emissão da respectiva OST e finalizado em até 30 (trinta) dias corridos após o início da ação de treinamento.**

8.2. O treinamento deverá ser o oficial do(s) fabricante(s);

8.3. O treinamento poderá ser presencial, em instalações indicadas pela Contratada na Região Metropolitana de São Paulo, na Sede do Coren-SP ou on-line, a critério da Contratante e deverá atender à



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

carga horária mínima recomendada pela fabricante;

8.4. O treinamento deverá ser ministrado para 1 (uma) turma, composta por até 5 (cinco) alunos oficiais;

8.5. Na hipótese de o treinamento ser realizado em instalações indicadas pela Contratada, o local de treinamento deverá possuir toda a infraestrutura necessária para o perfeito desempenho das atividades de aprendizado, possuindo recursos materiais e tecnológicos necessário para tal, sem ônus algum para a Contratante;

8.6. O local do treinamento, horários de realização, conteúdo programático, bem como o material didático a ser utilizado pelos treinandos deverá ser previamente aprovado pela Contratante;

8.7. O conteúdo programático deverá ser voltado para a instalação, configuração, administração, manutenção e solução de problemas dos componentes ofertados na Solução contratada, devendo abordar, minimamente:

8.7.1. Apresentação da arquitetura da Solução completa (software de backup e hardware) e dos conceitos fundamentais;

8.7.2. Instalação;

8.7.3. Configuração e gerenciamento da Solução;

8.7.4. Operação completa;

8.7.5. Análise de problemas;

8.7.6. Alertas e ações;

8.8. O treinamento será do tipo teórico-prático e contemplará o conteúdo programático necessário ao perfeito funcionamento e utilização das funcionalidades da Solução;

8.9. Toda a documentação e material didático necessária ao repasse de conhecimento deverá ser disponibilizada em mídia digital, preferencialmente na língua portuguesa (Português do Brasil) ou, na inviabilidade, em inglês;

8.10. São produtos esperados do treinamento:

8.10.1. Material didático contratado e aprovado pela Contratante;

8.10.2. Certificados de conclusão do treinamento, emitidos pela Contratada e destinados aos participantes indicados pela Contratante.

8.11. O(s) instrutor(es) indicado(s) para a execução do treinamento deverá(ão) ser certificado(s) na Solução;

8.12. Ao final do treinamento:

8.12.1. A Contratante emitirá um Termo de Aceite da Qualidade – TAQ, cuja emissão estará vinculada à obtenção da média mínima de 60% (sessenta) por cento das fichas de avaliação do treinamento respondeicas pelos treinandos;

8.12.2. A Contratada fornecerá certificado de conclusão do treinamento aos participantes que atenderem a, no mínimo, 70% do total da c/h definida;

8.12.3. Os certificados deverão ser encaminhados à Contratante no prazo de até 5 (cinco) dias corridos contados da conclusão do treinamento;



CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

8.13. Caso o treinamento seja reprovado na avaliação dos treinandos, a Contratada ficará obrigada a refazê-lo, após as adequações necessárias, sem qualquer custo à Contratante, sendo que o novo treinamento também será submetido aos mesmos critérios de avaliação.