Tribunal Regional Eleitoral de São Paulo

Termo de Referência

1. OBJETO

Aquisição de solução redundante de cópia de segurança (backup) composta por hardware (appliance), software de gerenciamento de backup, e serviços de instalação e configuração.

2. JUSTIFICATIVA

O procedimento de cópia de segurança é importante na medida em que permite que este Tribunal Regional Eleitoral retome as suas operações normais na ocorrência de um sinistro que inviabilize o acesso ou a confiabilidade dos dados armazenados em nossos servidores, alinhado à Continuidade de Serviços de TIC, Política de Segurança da Informação, normativos técnicos oriundos de órgãos de controle tais como o Conselho Nacional de Justiça, o Tribunal Superior Eleitoral e o Tribunal de Contas da União os quais deve-se buscar aderência, dentre outros.

Atualmente as cópias de segurança são armazenadas em fitas magnéticas padrão LTO, uma tecnologia que não atende a necessidade de rápida recuperação de dados em razão das particularidades desta tecnologia e volume de dados do TRE-SP. Entretanto, o uso deste recurso é necessário para implementação de cópia off-line e para manter compatibilidade com backups anteriores realizados nesta tecnologia.

A solução de tecnologia da informação necessária para atendimento a essa demanda consiste em dispositivos de hardware denominado “appliance” e uma solução de software de gerenciamento de backup, com possibilidade de utilização de replicação de dados visando redundância e com suporte à desduplicação.

O “appliance” pode ser descrito como um servidor dedicado com armazenamento de dados próprio para manter as cópias de segurança. Por sua vez a solução de software de backup, que pode ser utilizada em conjunto com o appliance ou não, é responsável por gerenciar e realizar os procedimentos de cópia e restauração de dados armazenados em servidores e storages.

Dentre os benefícios da solução escolhida, podemos destacar o custo decrescente de manutenção da solução em disco em comparação com o custo da solução em fita magnética, a agilidade na operação da solução em disco quando comparada com as tecnologias utilizadas atualmente, o que permite uma retomada mais célere dos serviços caso ocorra algum sinistro.

Finalmente a aquisição da solução irá aproximar as tecnologias utilizadas por este Tribunal Regional Eleitoral com as tecnologias utilizadas pelo mercado, facilitando eventuais serviços de suporte, melhorias e ampliações caso necessárias.

3. ESPECIFICAÇÕES DO OBJETO

3.1. Appliance de Backup

3.1.1. O “Appliance” deverá atender integralmente os requisitos especificados, devendo ser fornecido com todas as licenças que forem necessárias para a entrega totalmente funcional da solução;

3.1.2. O “Appliance” deve ser novo, sem uso e constar da linha de produção do fabricante, não sendo aceito gateways e/ ou composições feitas exclusivamente para atendimento ao presente edital;

3.1.3. O “Appliance” deverá constar no site do fabricante, em um documento oficial e público;

3.1.4. O hardware do “Appliance” não poderá ser compartilhado com nenhum outro software;

3.1.5. O “Appliance” deverá ser composto, de processamento e armazenamento integrado, dedicado única e exclusivamente, à execução das atividades de entrada, desduplicação e replicação dos dados enviados pelos servidores de backup;

3.1.6. Deverá vir instalado em rack padrão do Fabricante com todos os acessórios para instalação no Data Center da Contratante.
3.1.7. Deverá obrigatoriamente fazer uso de sistemas inteligentes de armazenamento de backup em disco, baseado em “Appliance”, que se entende como um subsistema com o propósito específico de entrada dos dados de backup, deduplicação e replicação;
3.1.8. O Sistema Operacional do equipamento deverá ser licenciado e nativo do produto. Não serão aceitas as modalidades OEM de sistemas operacionais de propósito geral, tal como Windows ou Unix/Linux;
3.1.9. A desduplicação deve segmentar os dados em blocos de tamanho variável ajustado automaticamente pelo algoritmo do appliance;
3.1.10. A solução deve fazer uso de recursos dedicados para realizar a compressão via hardware dos dados após a desduplicação dos dados, de forma que este processo de compressão não deve impactar o desempenho do equipamento. Será facultada a utilização de soluções que não fazem uso da desduplicação global, desde que a área líquida solicitada seja acrescida em 50% (cinquenta por cento) de forma a compensar a menor eficiência deste tipo de tecnologia.
3.1.11. Possuir tecnologia de desduplicação de dados em linha (inline) ou em paralelo, ou seja, os dados de backup são desduplicados em CPU e memória antes ou concomitantemente com sua gravação em disco. Não serão aceitas soluções que realizem a desduplicação após a gravação do dado no disco (pós-processo) ou mesmo híbridas que realizem parte do processo antes e parte após a gravação do dado no disco;
3.1.12. O sistema inteligente de armazenamento de backup em disco deve permitir realizar a replicação otimizada dos dados (off-host) sem onerar a CPU dos servidores de backup;
3.1.13. O sistema inteligente de armazenamento de backup em disco deve permitir replicar os dados através de rede IP de forma criptografada;
3.1.14. O sistema inteligente de armazenamento de backup em disco deverá ser capaz de suportar falhas de até dois discos, devendo ser fornecido com proteção RAID-6 ou similar;
3.1.15. O sistema inteligente de armazenamento de backup deve ser fornecido com no mínimo um disco “Hot-Spare” para cada RAID group ou gaveta de discos;
3.1.16. Devido ao tempo de reconstrução do RAID em caso de falha do disco, a área de armazenamento da solução deverá ser disponibilizada em conjuntos de discos rígidos com tecnologia SAS com capacidade máxima de 8TB (oito terabytes) brutos cada;
3.1.17. Deve suportar replicação 1 para N, N para 1 (várias origens e 1 destino) e cascata;
3.1.18. Deve ser fornecido licenciamento para funcionalidade de replicação para toda capacidade ofertada;
3.1.19. O(s) disco(s) de “hot spare” devem ser utilizados de forma global dentro do nó de processamento ou do Appliance;
3.1.20. A solução deverá possuir sistema de proteção interno que permita melhorar a segurança dos dados e índices e a recuperação para um momento anterior;
3.1.21. Deverá possuir mecanismos que não permitam a inconsistência dos dados mesmo em casos de interrupção abrupta ou desligamento acidental, por meio de memória não volátil dedicada a operações de escrita ou recurso similar;
3.1.22. Deve possuir mecanismo inteligente que verifique continuamente de forma automática a integridade lógica dos dados, “ponteiros” e índices armazenados (fim-a-fim) no hardware com correção automática das falhas encontradas, de forma a garantir a consistência de todo o conteúdo em sua total capacidade, sem a utilização de scripts e/ ou composições feitas exclusivamente para atendimento a esse item.
3.1.23. Deverá possuir interface de administração gráfica ou GUI (Graphical User Interface) e por linha de comando ou CLI (Command Line Interface);
3.1.24. A solução ofertada deve suportar a integração comprovada por matriz de compatibilidade com o software Oracle RMAN e estar inscrita na matriz do fabricante do appliance ou constar na matriz de fabricantes homologados pelo Oracle Backup Solutions Program (BSP), permitindo que o backup e restore do

banco de dados Oracle possam ser feitos diretamente para o Appliance de maneira desduplicada, sem a utilização de scripts ou software de backup

3.1.25. A solução deverá suportar a criptografia dos dados desduplicados sem necessidade de equipamento adicional;

3.1.26. Permitir o particionamento lógico da área de armazenamento (Mult-Tenant ou Multi-Protocolo), sem prejuízo as características de desduplicação solicitadas;

3.1.27. Deve possuir os recursos de memória necessários para atingir, pelo menos, o desempenho solicitado. Não serão aceitas como memória a utilização de tecnologias Flash, SSD ou qualquer outra tecnologia de extensão de cache;

3.1.28. Deverá possuir no mínimo 75 TB úteis, sem considerar ganhos com desduplicação e compressão de dados;

3.1.29. Deve permitir a expansão da área de armazenamento em, no mínimo, 240TB úteis, em um único pool (área) de armazenamento e deve ser atingida com a adição de gavetas de disco ou nós de processamento sem prejuízo das demais características solicitadas;

3.1.30. Deverá suportar as seguintes interfaces de interconexão com os servidores de backup: interfaces 10Gb Ethernet;

3.1.31. Deverá estar licenciado para suportar simultaneamente as seguintes formas de acesso para backup: CIFS, NFS e OST;

3.1.32. Deverá ser fornecido com no mínimo 04 portas Ethernet 10Gbps (Base-T ou SFP+), com suporte a autonegociação para velocidade de 1 Gbps;

3.1.33. Deverá possuir performance de ingestão de no mínimo 24TB/hora de dados transferidos, considerando somente desduplicação no destino;

3.1.34. Deve suportar no mínimo 100 jobs de gravação simultânea.

3.1.35. Deve ser compatível com os protocolos de rede IPv4 e IPv6;

3.1.36. Deverá ter suporte ao protocolo de monitoramento SNMP v2;

3.1.37. As rotinas internas de manutenção dos dados de backup armazenados tais como: Processo de limpeza (Garbage Collector ou housekeeping) e Validação de integridade (data integrity), devem ser executados em paralelo com as rotinas de backup e recuperação, ou seja, a solução ofertada não deve exigir parada ou interrupção (blackout window) das atividades de backup/restore para tarefas internas do equipamento.

3.1.38. A solução deve possuir no próprio hardware do equipamento função de “call-home” ou email para notificar de forma automática quaisquer problemas para a central do fabricante.

3.1.39. Possuir recurso de imutabilidade de dados utilizando WORM (Write Once Read Many) ou tecnologia equivalente como, por exemplo, secure snapshot, para proteção contra alteração/regravação e exclusão dos dados armazenados, permitindo somente uma única escrita e múltiplas leituras, garantindo integridade e autenticidade, deste modo a solução não deverá permitir que usuários consigam alterar ou apagar dados protegidos, até que o tempo de retenção configurado tenha expirado;

3.1.40. Caso o recurso de imutabilidade WORM dependa de system clock, ele deve possuir certificação Sec 17a-4(f), incluindo proteção (System Clock Hardening Protection) caso o cibercriminoso altere/adiante a data do subsistema para poder alterar/excluir os arquivos protegidos;

3.1.41. Possuir recurso de dupla autenticação (2FA – Two Factor Authentication) para executar atividades administrativas de exclusão no equipamento;

3.1.42. Deve possuir proteção contra Ransomware para os dados de cópia de segurança retidos, e deve ser do dispositivo ofertado, funcionar de maneira automática e transparente, independentemente do software/utilitário de backup, não deve depender do desenvolvimento de scripts de integração, tampouco de ações ou atividades manuais sobre os dados retido e deve garantir a inviolabilidade (imutabilidade) dos dados mesmo se o ambiente operacional onde opera e/ou o software de backup estejam sob controle de um atacante (hacker ou malware). A proteção deve garantir que, independentemente do atacante procurar expirar o conteúdo das cópias de segurança por manipulação do catálogo do software de backup, será possível recuperar os dados retidos no appliance de backup por um período de dias. Para tanto, o appliance deve permitir o particionamento em camadas, com separação lógica de volumes de dados ou air-gap virtual.

3.1.42.1. Caso não possua essas características, deverá fazer a separação física com air-gap e incluir todos os componentes necessários (armazenamento adicional, servidores, software, licenciamento, serviços, etc.) e em quantidade suficiente para proteger todos os dados retidos conforme especificações de volume de dados, retenção, crescimento vegetativo e tamanho mínimo do equipamento deste termo de referência para a proteção dos dados de backup, devendo ser fornecidos em conjunto com a solução e mantendo as condições de escalabilidade e desempenho especificadas nesse projeto;

3.1.42.2. Todos os componentes necessários (hardware, software, licenciamento, serviços, etc.) para a proteção dos dados de backup devem ser fornecidos em conjunto com a solução e devem manter as condições de escalabilidade e desempenho especificadas nesse projeto;

3.1.43. O atendimento de suporte remoto do fabricante deve permitir, sem limite de quantidade, durante a vigência da garantia, que o suporte remoto realize, pelo menos, as seguintes tarefas: instalação de correções e atualizações; revisão das configurações e sugestão de melhores práticas do fabricante; reconfiguração e reinstalação do appliance, quando for necessário;

3.2. Software da solução de Backup

3.2.1. O licenciamento da solução para o ambiente virtualizado de backup/restore deverá ser baseado no modelo de quantidade de VM´s (máquinas virtuais), ou baseado no total de processadores físicos (sockets) do ambiente existente.

3.2.2. O licenciamento da solução para o ambiente físico de backup/restore deverá ser baseado no modelo de quantidades de instancias (servidores) físicas. Por exemplo 1 (um) Sistema Operacional para 1 (um) Servidor Físico.

3.2.2.1. Para cada servidor físico licenciado, deverá ser considerado até 500GB de volumetria.

3.2.3. A solução ofertada deve estar habilitada para permitir a instalação de quantos servidores de mídia e de gerência do backup quanto forem necessários para configuração do ambiente da CONTRATANTE de acordo com as melhores práticas propostas pelo fabricante.

3.2.4. A versão da solução ofertada deve ser a última versão disponível, não será aceita a utilização de versões anteriores para cobrir algum item desse Termo de Referência.

3.2.5. A solução ofertada deverá mostrar a quantidade de licenças adquiridas e utilizadas.

3.2.6. Caso a solução permita o consumo acima do que foi contratado sem nenhuma trava não será cobrado, em hipótese alguma, qualquer diferença seja no licenciamento, seja em renovações futuras ou desistência da utilização do software;

3.2.7. Caso a solução ofertada necessite de algum sistema gerenciador de banco de dados ele deverá ser fornecido devidamente licenciado sem nenhum custo extra para a CONTRATANTE;

3.2.8. Deve ser fornecido licenciamento para funcionalidade de gravação em fita para toda capacidade ofertada;

3.2.9. A solução de backup deve possuir arquitetura em múltiplas camadas, a saber: servidor de gerência do backup, servidores de mídia e clientes / agentes de backup;

3.2.10. O servidor de Gerência de backup deverá ter suporte para instalação, no mínimo, nos sistemas operacionais Microsoft Windows Server 2016 e Microsoft Windows Server 2019;

3.2.11. O servidor deverá possuir um banco de dados ou catálogo interno contendo informações sobre todos os arquivos e mídias onde as cópias de segurança (backups) foram armazenadas;

3.2.12. A infraestrutura de servidores necessária para a instalação do software de Gerenciamento de Backup deverá ser fornecida pela CONTRATANTE, sendo que a CONTRATADA deverá encaminhar a especificação técnica referente a tal infraestrutura;

3.2.13. O servidor de mídia deverá ter suporte para ser instalado, pelo menos, nos sistemas operacionais Microsoft Windows Server 2016, Microsoft Windows Server 2019 e Oracle Linux;
3.2.14. A arquitetura da solução deve ser flexível e escalável, permitindo sua instalação, configuração e uso em sites remotos interligados ao site principal através de WAN. Além disso, a solução deve prover recursos de desduplicação na origem, desduplicação no destino, e compactação tanto no site principal como nos sites remotos na inteireza da capacidade previamente licenciada e sem necessidade de aquisição de qualquer outro tipo de licença ou recurso adicional para execução de tais operações;
3.2.15. Os servidores necessários para a instalação do software de Gerenciamento de Mídias (Media Servers) serão fornecidos pela CONTRATANTE, sendo que o fornecedor vencedor encaminhará a especificação técnica necessária para a Contratante.
3.2.16. A solução ofertada de backup deve ter a funcionalidade para proteger escritórios regionais, assegurando que a transmissão de dados através da WAN seja minimizada, provendo tanto desduplicação quanto replicação, enquanto possibilita recuperação granular de dados. A solução deve prover arquitetura flexível ao ponto de que a recuperação no escritório regional possa ser total (com todos os dados vindos do datacenter) ou parcial (com somente o envio dos dados que não estão em cache local);
3.2.17. A solução ofertada de backup deve implementar a funcionalidade LAN FREE-BACKUP em todo volume licenciado; de forma a prover a cópia e a restauração de dados utilizando a infraestrutura de rede SAN;
3.2.18. A solução de backup deve permitir o controle da banda utilizada durante a operação de backup.
3.2.19. A solução de backup deverá ser capaz de realizar cópia de arquivos abertos sem que a sua consistência seja comprometida;
3.2.20. A solução de backup deverá possuir a opção de priorização de jobs de backup com opção de resumo da cópia caso um job de menor prioridade seja colocado em stand-by para disponibilizar mais recursos para um job de maior prioridade;
3.2.21. A solução de backup deverá possuir a funcionalidade de paralelizar a gravação dos dados em dispositivos de armazenamento (funcionalidade conhecida como multiplexação);
3.2.22. A solução de backup deverá ser capaz de enviar alertas através de e-mail com o objetivo de reportar eventos ocorridos na operação e configuração da solução;
3.2.23. A solução de backup deverá ser capaz de enviar traps SNMP (Simple Network Management Protocol) com o objetivo de reportar eventos ocorridos na operação da solução;
3.2.24. A solução de backup deverá possuir a funcionalidade de agendamento automático de jobs de backup;
3.2.25. Para operações de backup gravadas em disco e fita, a solução de backup deve possuir as seguintes funcionalidades:
3.2.26. Para um mesmo dado armazenado deve ser possível de configurar de diferentes períodos de retenção;
3.2.27. Para um dado armazenado deve permitir a possibilidade de estender o período de retenção.
3.2.28. Permitir a gravação de backups Disk-to-Disk-to-Tape;
3.2.29. A solução ofertada deve permitir backup diretamente para fita magnética (tape) sem a necessidade de armazenar primeiramente em disco;
3.2.30. Ser compatível com bibliotecas auto-carregadoras de cartuchos de fitas magnéticas.
3.2.31. A solução de backup deverá possuir a funcionalidade de criar múltiplas cópias de backups armazenados, com a opção de recuperação dos dados de forma automática através da cópia secundária se a cópia primária não estiver mais disponível.
3.2.32. A solução de backup deverá, a partir de uma única interface, ser capaz de gerenciar e executar operações de backup/restore dos sistemas operacionais Windows, Unix e Linux; ambientes de virtualização (Vmware, Hyper-V, KVM (oVirt), Oracle VM); Microsoft Active Directory e banco de dados Microsoft SQL Server,

Oracle (Windows e Linux), a ser comprovadas por documentação técnica da solução, através de links e manuais do fabricante;

3.2.33. O acesso administrativo ao console do servidor de gerenciamento de backup deverá ser feito com a ferramenta disponibilizada no próprio software (console gráfico) ou por navegador Web;

3.2.34. A solução de backup deverá implementar configuração de servidores em cluster para promover alta-disponibilidade dos serviços de gerenciamento;

3.2.35. A solução de backup deverá implementar distribuição automática de carga entre os media servers, ou seja, os dados oriundos dos clientes de backup deverão ser distribuídos de forma automática entre os servidores de backup, e em caso de falha de um dos servidores, o cliente automaticamente irá encaminhar seus dados para o outro servidor de backup ativo. Esta funcionalidade deverá ser nativa do produto, e não pode ser construída com o uso de soluções baseadas em softwares de cluster de terceiros.

3.2.36. A solução de backup deverá suportar single sign on (SSO), permitindo a integração com o Microsoft Active Directory. A funcionalidade de integração com o Active Directory deverá permitir a definição granular das permissões administrativas aos recursos, objetos e servidores definidos na configuração do software;

3.2.37. A base de dados para armazenamento do catálogo deverá possuir mecanismo de proteção (backup) das informações armazenadas no catálogo e funcionalidades de recuperação rápida do catálogo em caso de desastre;

3.2.38. A solução de backup deverá implementar criptografia de dados na origem (cliente de backup), de uma forma que seja garantido que o dado que trafegará na rede local ou na rede WAN seja criptografado.

3.2.39. A solução de backup deverá implementar criptografia de dados no destino do backup, de uma forma que seja garantido que os dados sejam criptografados

3.2.40. Deverá implementar no mínimo chaves de criptografia de 128 bits e 256 bits

3.2.41. No caso da restauração granular, não há necessidade de se restaurar a Guest VM inteira;

3.2.42. Permitir redirecionar a restauração de uma Guest VM para uma pasta alternativa, outro datastore, host ou rede;

3.2.43. Incluir automaticamente máquinas virtuais novas criadas dentro de seleções de backup anteriores;

3.2.44. Permitir o backup Full, Incremental para os servidores virtuais;

3.2.45. Deverá ser capaz de realizar backups/restore de servidores virtuais Linux e Windows;

3.2.46. Deverá permitir que as tarefas de backup/recovery sejam realizadas via interface gráfica, sem a necessidade de scripts;

3.2.47. O backup dos servidores virtuais deverá ser armazenado de maneira desduplicadas;

3.2.48. A solução deve permitir uso da tecnologia de Desduplicação de dados para toda a capacidade e processadores licenciados, eliminando blocos repetidos, para backups/arquivamento em disco e movimentação de dados desduplicados, independente de quantitativo de dispositivos de armazenamento que compõem a infraestrutura da CONTRATANTE;

3.2.49. A solução deverá permitir a desduplicação em nível de blocos, não sendo aceita a técnica de Single-Instance Storage;

3.2.50. Deverá permitir desduplicação 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;

3.2.51. Deverá permitir desduplicação de dados nos repositórios de Armazenamento (target deduplication), de forma que os blocos repetidos enviados pelos clientes sejam excluídos da gravação, evitando assim o armazenamento de blocos redundantes;

3.2.52. Deverá permitir desduplicação de dados global, efetuando o backup de determinado arquivo apenas uma vez, independente do site e ou localidade originários. A desduplicação global deverá ocorrer em uma única área de armazenamento;

3.2.53. Deverá permitir desduplicação de dados em jobs de backup;

3.2.54. Deverá permitir desduplicação e compressão em um mesmo job;
3.2.55. Deverá permitir o restore granular de arquivos ou sistemas de arquivos a partir de backups em disco ou fita. Em caso de backup armazenado em disco o restore granular poderá ser feito utilizando-se backups que possam estar armazenados de forma desduplicada;
3.2.56. Deverá suportar desduplicação global onde mais de um Media Server acesse e armazene blocos únicos na mesma base de desduplicação;
3.2.57. Cada Media Server deverá gerenciar no mínimo 150 TB de dados desduplicados;
3.2.58. A solução deverá vir disponível com os seguintes relatórios:
3.2.58.1. Quantidade de rotinas de backup concluídos nas últimas 24 horas, nos últimos 30 dias e nos últimos 6 meses;
3.2.58.2. Quantidade de recuperações efetuadas nas últimas 24 horas, nos últimos 30 dias e nos últimos 6 meses;
3.2.58.3. Relatórios de rotinas de backup concluídas com sucesso, com erro ou não concluídos;
3.2.58.4. Taxa de desduplicação por rotina de backup;
3.2.59. Análise e tendência a longo prazo e análise para melhor prever o consumo de armazenamento de backup ao acompanhar as taxas de crescimento ao longo do tempo, incluindo pré e pós-desduplicação, para um acompanhamento de ROI mais fácil e taxas de desduplicação;
3.2.60. Possuir relatórios capaz de classificar arquivos por tipo, tamanho e idade;
3.2.61. Deverá conter reportes onde mostra o total de licenças adquiridas e o total de licenças utilizadas, vigência da licença e caso ocorra uma nova aquisição de licenças as novas licenças deverão constar nesse relatório;
3.2.62. A solução ofertada deverá permitir o envio de alertas por e-mail quando a rotina de backup finalizar com sucesso, finalizar com erro ou tiver encontrado um problema;
3.2.62.1. Falta de recursos para backup – Disco ou fita
3.2.62.2. Alerta para utilização de licenciamento
3.2.62.3. Alerta para utilização de licenciamento acima de um volume pré-determinado;
3.2.63. Deverá permitir desduplicação de dados em jobs de backup;
3.2.64. Deverá permitir desduplicação de dados em jobs de arquivamento;
3.2.65. Deverá permitir desduplicação e compressão em um mesmo job.
3.2.66. Deverá permitir o restore granular de arquivos ou sistemas de arquivos a partir de backups em disco ou fita. Em caso de backup armazenado em disco o restore granular poderá ser feito utilizando-se backups que possam estar desduplicados.
3.2.67. Gerência dos snapshots;
3.2.68. Registro dos snapshots na base relacional de catálogos de forma que possa realizar buscas por snapshots;
3.2.69. 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;
3.2.70. A integração com os snapshots deverá ser feita via API, ou seja, não será aceito implementação de scripts manuais de pré e pós backup para esta funcionalidade.
3.2.71. Deverá efetuar uma cópia dos snapshots criados para disco com desduplicação
3.2.72. O software deverá possuir integração via API para gerência de snapshots com, pelo menos, os seguintes fabricantes: DELL EMC Storage Center (DSM), Dell EMC VNX;
3.2.73. As aplicações e bases de dados elencadas deverão ser suportadas para integração com todos os snapshots acima via API:
3.2.73.1. SQL Server 2012 e versões superiores;
3.2.73.2. VMWare 6.x e superior;
3.2.73.3. Oracle Database 19c
3.2.73.4. Microsoft Windows File System 2008, 2012, 2016 e 2019
3.2.74. A solução deve permitir implantar uma estratégia de gerência de dados que atinja toda a empresa/organização. As funcionalidades que deverão ser incluídas são:
3.2.74.1. Migração de dados e gerenciamento hierárquico de armazenamento;
3.2.74.2. Gerência de recursos de armazenamento;
3.2.74.3. Monitoramento e gerência de nível de serviço;

3.2.75. A console de Gerenciamento da solução de arquivamento deve ser compatível com os sistemas operacionais: Microsoft Windows Server 2008, Microsoft Windows Server 2012 ou superior;
3.2.76. A solução deve implementar configuração de servidores em cluster para promover alta-disponibilidade dos serviços de gerenciamento.
3.2.77. A solução deve contar com um mecanismo de reconstrução de banco de dados de catálogo e índices, de modo a haver uma estratégia contra corrupção de dados.
3.2.78. Para arquivamento de "filesystem" ou "fileshare" o software deve ser capaz de automaticamente arquivar documentos satisfazendo certo critério e substituí-los por "atalhos" que contêm as informações para a recuperação destes. Os usuários podem dar um clique duplo no "atalho" do arquivo numa janela do Windows Explorer para reaver o documento original.
3.2.79. O servidor de arquivos deverá permitir as seguintes regras de arquivamento:
3.2.79.1. Último acesso ao arquivo (em dias);
3.2.79.2. Última modificação de arquivos (em dias);
3.2.79.3. Tamanho de arquivos;
3.2.79.4. Tipo de arquivo.
3.2.80. Além disso, o software deve permitir ao administrador definir regras de arquivamento baseadas nos caminhos dos arquivos de forma a selecionar e excluir arquivos com base na localização do arquivo e características específicas do arquivo (ex.: extensões);
3.2.81. A solução deve prover uma opção para verificação de dados, de forma a assegurar que os dados foram arquivados estão íntegros;
3.2.82. As mensagens arquivadas deverão estar desduplicadas no nível de blocos, caso a solução não desduplique em nível de bloco, a CONTRATADA deverá fornecer uma solução baseada em appliance;
3.2.83. Deverá possuir mecanismos de proteção das aplicações e sistemas operacionais através das melhores práticas de proteção nos padrões do NIST (National Institute of Standards and Technology);
3.2.84. Garantir integridade contra as ameaças de perda de dados através do uso de Autenticação e Autorização;
3.2.85. Deverá possuir monitoração protetiva e Pró-Ativa dos servidores de backup, repositórios e arquivos de produção;
3.2.86. Deverá possuir tecnologia de isolamento dos dados de backup via segmentação de rede para garantir inviolabilidade dos dados secundários e terciários.

3.3. Serviço de instalação, implantação e hands-on da solução
3.3.1. Efetuar a instalação de todos os equipamentos, acessórios e softwares que compõem a solução;
3.3.2. Realizar as configurações iniciais, em conjunto com a Contratante (Hands-on), para uso da solução;
3.3.3. Elaborar documentação técnica do ambiente instalado, incluindo as configurações iniciais e procedimentos para instalação de agentes;
3.3.4. Realizar a devida ativação e configuração da solução (hardware e software) segundo as boas práticas do fabricante, disponibilizando o ambiente de backup em condições de pleno funcionamento.

4. QUANTIDADE

Item	Descrição	Quantidade
1	Appliance de Backup com garantia e suporte pelo período de 36 meses	4
2	Licença da solução de proteção de dados (backup/restore) para aplicações, Banco de dados, File Servers e e-mail contemplando todas as funcionalidades de desduplicação e SnapShot para ambiente virtualizado com	31

	suporte e garantia do fabricante pelo período de 36 meses, contemplando 9 processadores físicos e 300 VMs.	
3	Serviço de instalação, implantação e hands-on da aplicação de backup	1
4	Serviço de instalação, implantação e hands-on da appliance de backup	4

5. LOCAL DE EXECUÇÃO OU ENTREGA DO BEM

5.1. Os equipamentos serão entregues e instalados no prédio do TRE-SP:

Sede I: Rua Francisca Miquelina, 123, Anexo I, 2º andar – Bela Vista - São Paulo – SP – CEP: 01316-900;

5.2. O Serviço de instalação, implantação e hands-on da solução deverá ser realizado nos endereços acima.

6. PRAZO DE ENTREGA OU INÍCIO DA PRESTAÇÃO DO SERVIÇO

6.1. Os equipamentos devem possuir garantia de 36 (trinta e seis) meses a partir do aceite definitivo;
6.2. O prazo de entrega dos equipamentos será de até 60 (noventa) dias corridos, contados a partir da data de assinatura do Instrumento Contratual;
6.3. A contratada deverá instalar, configurar, interconectar, testar e documentar a solução adquirida no prazo máximo de 30 (trinta) dias corridos, contados a partir do recebimento provisório dos bens;
6.4. A CONTRATADA deverá apresentar comprovação formal da aquisição da garantia técnica junto ao fabricante, abrangendo todos os equipamentos e software(s) da solução. A entrega da garantia técnica do fabricante não exclui a responsabilidade da CONTRATADA da prestação de suporte da solução;
6.5. A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA. Não deve haver limite para aberturas de chamados, sejam de dúvidas/configurações e/ou resolução de problemas de hardware ou software;
6.6. A abertura de chamados poderá ser realizada através de telefone 0800 do Fabricante, através da página da WEB do Fabricante ou através de endereço de e-mail do Fabricante. Quando da abertura de chamados através de telefone 0800 o mesmo deverá ser realizado inicialmente em português do Brasil;
6.7. Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto
6.8. A garantia prestada será livre de ônus para a CONTRATANTE**;**
6.9. A CONTRATADA deverá disponibilizar atendimento por técnicos especializados para a solução de problemas, sem limitação para o número de chamadas, durante o período da garantia e assistência técnica;
6.10. O prazo de vigência do contrato será de 36 (trinta e seis) meses, contados a partir da data de sua assinatura, podendo, a critério da Administração, ser prorrogado até o limite de 60 (sessenta) meses, conforme art. 57, inciso II da Lei nº 8.666/93.

7. CONDIÇÕES DE RECEBIMENTO

7.1. Observado o disposto nos artigos 73 a 76 da Lei 8.666/93, o recebimento dos objetos, será realizado da seguinte forma:
7.1.1. Provisoriamente, em até 5 dias úteis após efetuada a entrega, para efeito de posterior verificação da conformidade com as especificações;

7.1.2. Definitivamente, até 10 (dez) dias úteis da entrega, após verificação da qualidade e quantidade do bem e consequente aceitação.

7.2. No caso de consideradas insatisfatórias as condições do objeto recebido provisoriamente, será lavrado Termo de Recusa, no qual se consignarão as desconformidades, devendo o produto ser recolhido e substituído.

7.3. Após a notificação à CONTRATADA, o prazo decorrido até então será desconsiderado, iniciando-se nova contagem tão logo sanada a situação.

7.4. A CONTRATADA terá prazo de 10 (dez) dias úteis para providenciar a substituição do objeto, a partir da comunicação oficial feita pela CONTRATANTE, sem qualquer custo adicional para a CONTRATANTE.

7.5. Caso a substituição não ocorra no prazo determinado, estará a CONTRATADA incorrendo em atraso na entrega e sujeita à aplicação das sanções previstas.

7.6. O recebimento provisório e definitivo do objeto não exclui a responsabilidade civil a ele relativa, nem a ético-profissional, pela sua perfeita execução e dar-se-á se satisfeitas as seguintes condições:

7.6.1. Objeto de acordo com a especificação técnica contidas neste Termo de Referência e na Proposta Comercial vencedora;

7.6.2. Quantidades em conformidade com o estabelecido na Nota de Empenho;

7.6.3. Entrega no prazo, local e horários previsto neste Termo de Referência.

8. FORMA COMO OS SERVIÇOS / COMPRAS SERÃO SOLICITADOS

8.1. O fornecimento do produto será efetuado mediante encaminhamento, pela Seção de Compras e Licitações ou Seção de Logística, de Nota de Empenho, que corresponde à autorização de entrega, devendo constar: especificações do produto, quantitativo, prazo, local de entrega e preços unitário e total.

8.2. A detentora não poderá, sem motivo justo, devidamente comprovado e informado, recusar-se a fornecer os materiais solicitados pela CONTRATANTE.

8.3. O(s) produto(s) será(ão) devolvido(s) na hipótese de apresentar(em) irregularidades, não corresponder(em) às especificações da Nota de Empenho ou estar(em) fora dos padrões determinados, devendo ser substituído(s) pela empresa no prazo indicado no item 7.4.

9. GARANTIA DO PRODUTO

9.1. Especificações aplicáveis para ao item 1:

9.1.1. A garantia e suporte exigidos deverá cobrir todos os equipamentos por, no mínimo, 36 meses;

9.1.2. A garantia e suporte aqui descritos deverão ser prestados pelo fabricante dos produtos;

9.1.3. Durante o período de garantia exigido, a modalidade de atendimento técnico para correção de problemas nos equipamentos deverá ser on-site (no local onde os equipamentos foram instalados);

9.1.4. A garantia deve cobrir os defeitos decorrentes de projeto, fabricação, construção, montagem, acondicionamento, transporte, erros na instalação física e/ou desgaste prematuro, envolvendo, obrigatoriamente, a substituição dos componentes defeituosos, sem qualquer ônus adicional para o CONTRATANTE;

9.1.5. A garantia deverá ser efetuada deixando os equipamentos em perfeitas condições de funcionamento, com suas características originais mantidas;

9.1.6. O fabricante das soluções fornecidas deverá oferecer possibilidade de abrir chamados técnicos por telefone ou Internet;

9.1.7. As novas versões, releases, atualizações e correções dos softwares e firmwares dos hardwares adquiridos, deverão ser disponibilizados à CONTRATANTE sem ônus durante o período de garantia;

9.1.8. O serviço de suporte e assistência técnica deverá ser realizado nos locais onde os equipamentos estiverem instalados (“on-site”), e deve incluir o fornecimento de peças originais para reposição, exceto itens consumíveis, quando aplicável, conforme o manual do fabricante;

9.1.8.1. Os componentes instalados em substituição aos defeituosos e/ou danificados deverão ter, pelo menos, características iguais aos originais do equipamento;

9.1.8.2. Caso os componentes instalados em substituição tenham características superiores, não haverá custo adicional para a CONTRATANTE;

9.1.8.3. Os componentes instalados em substituição aos componentes defeituosos passarão a fazer parte dos equipamentos e, portanto, serão de propriedade da CONTRATANTE;

9.2. Especificações aplicáveis ao item 2:

9.2.1. A CONTRATADA deverá disponibilizar, na vigência do contrato, todas as atualizações dos softwares, concebidas em data posterior ao seu fornecimento, pelo período especificado no termo de referência (36 meses), sem qualquer ônus adicional para o contratante.

9.2.2. As atualizações incluídas devem ser do tipo “minor release” e “major release”, permitindo manter o software atualizado em sua última versão.

10. INDICAÇÃO DE PESSOAL

Serão designados oportunamente pela CONTRATANTE servidores para fiscalizar e acompanhar a execução do presente contrato, nos termos do art. 67 da Lei 8.666/93 e tudo o que dispõe a presente contratação.

11. OBRIGAÇÕES DA CONTRATADA

11.1. Executar fielmente o objeto do presente contrato na mais perfeita conformidade com o estabelecido, comunicando imediatamente à CONTRATANTE, por intermédio da Fiscalização, por escrito, a ocorrência de qualquer fato impeditivo ou relevante à execução do contrato, sem prejuízo de prévia comunicação verbal dos fatos, caso a situação exija imediata providência por parte daquela;

11.2. Indicar novo preposto, informando sua qualificação, no prazo de 24 (vinte e quatro) horas, nas ocasiões em que houver substituição daquele indicado na Proposta Definitiva de Preços (Anexo II) do Edital, por intermédio de carta endereçada a este Tribunal;

11.3. Providenciar, no prazo máximo de 24 (vinte e quatro) horas, a atualização dos números de telefone e fax, bem como o endereço de e-mail, sempre que houver alterações destes;

11.4. Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas para a contratação, comprovando-as, a qualquer tempo, mediante solicitação da CONTRATANTE;

11.5. Não transferir, no todo ou em parte, a execução do serviço objeto do presente contrato, sem prévia e expressa autorização da CONTRATANTE, devendo a subcontratada atender a todas as condições de habilitação, particularmente no que tange à regularidade fiscal, trabalhista e previdenciária, restando vedada, em qualquer hipótese, a subcontratação total do objeto do presente contrato;

11.6. Consentir durante a execução do contrato, que seja realizada Fiscalização, atentando-se para as observações, solicitações e decisões do Fiscal, desde que justificadas, não ficando, contudo, eximida de sua total responsabilidade sobre todos os serviços contratados;

11.7. Responsabilizar-se por danos pessoais ou materiais causados diretamente por seus funcionários na execução deste contrato, decorrentes de sua culpa ou dolo, apurados após regular processo administrativo;

11.8. Aceitar, nas mesmas condições ora avençadas, acréscimo ou supressão de até 25% (vinte e cinco por cento) do valor total atualizado do contrato, conforme disposto na Lei n.º 8.666/93, art. 65, I, “b” e seus §§ 1.º e 2º.”

12. OBRIGAÇÕES DO TRIBUNAL REGIONAL ELEITORAL DE SÃO PAULO

A CONTRATANTE obriga-se a:

12.1. Promover, por intermédio da Fiscalização, o acompanhamento e a fiscalização dos serviços (ou entrega do objeto), sob os aspectos quantitativo e qualitativo, anotando

em registro próprio as falhas detectadas, comunicando à CONTRATADA as ocorrências de quaisquer fatos que exijam medidas corretivas;

12.2. Verificar se durante a vigência do contrato estão sendo mantidas todas as exigências, condições de habilitação e qualificação contratadas;

12.3. Efetuar o pagamento à CONTRATADA, nos termos previstos na cláusula 15."

13. ASSINATURAS

São Paulo, em XX/XX/2022

Robson dos Santos França	Massaichi Maurício Isayama	Nádia Leão Pereira Quadros
José Enrique Canotilho		
Equipe de Planejamento da Contratação		

Aprovo o Termo de Referência.

Paulo Sérgio Furtado Abreu
<Titular da área Demandante>