DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

PROA: 241400-0004618-0
Requerente: Departamento de Tecnologia da Informação e Comunicação
Assunto: Solução de Backup

ANEXO II

TERMO DE REFERÊNCIA - TR

1. OBJETO:

Aquisição de Solução de Backup, incluindo hardware, licenciamento com prazo de 5 anos (podendo ser prorrogável pelo prazo máximo de 10 anos) e serviços de implantação, conforme tabela 1 – Resumo dos itens, no item 3 deste TR.

2. FUNDAMENTAÇÃO / JUSTIFICATIVA:

Conforme o Estudo Técnico Preliminar (ETP), o Departamento de Tecnologia da Informações e comunicações – DETIC – está buscando atingir seus objetivos estratégicos relacionados à segurança da informação, necessita adquirir solução de backup.

Os recentes ataques cibernéticos que assolaram diversas organizações no Brasil evidenciam a urgente necessidade de reforçar a segurança cibernética, tornando-a uma prioridade essencial para todas as instituições. Em conjunto com essa preocupação, a crescente incidência de desastres naturais, como inundações e incêndios, destaca a importância de adotar medidas proativas para proteger os dados e sistemas críticos contra múltiplas formas de ameaças.

Diante desse contexto, este departamento está compelido a fortalecer suas defesas cibernéticas e medidas de continuidade de negócios. A opção por uma solução de backup que ofereça rápida recuperação entre sites e proteção contra-ataques do tipo ransomware torna-se imprescindível para mitigar os riscos de perda de informações e interrupção dos serviços, tanto diante de ataques cibernéticos quanto em face de desastres naturais.

A duplicação dos dados em dois locais distintos proporcionará uma maior segurança e redundância, garantindo que nossos dados estejam protegidos mesmo em caso de falha de hardware, incêndios ou outras situações extremas. Além disso, com um RPO (Recovery Point Objective) igual a zero, os dados estarão sempre atualizados e disponíveis, mesmo em emergências, permitindo uma rápida recuperação das operações.

A aquisição da solução de backup, tem como objetivo:

- **Proteção Abrangente dos Dados**: Garantir a segurança e integridade dos dados contra ameaças cibernéticas, falhas de hardware e desastres naturais.
- **Minimização dos Riscos de Interrupção de Serviços**: Reduzir a probabilidade de interrupção dos serviços essenciais, garantindo a continuidade operacional mesmo diante de incidentes adversos.
- **Rápida Recuperação em Caso de Incidentes**: Capacitar a equipe de TI deste departamento a recuperar rapidamente os dados e sistemas afetados por falhas ou ataques, garantindo a continuidade das operações sem perda significativa de tempo ou produtividade.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

- **Conformidade com as Melhores Práticas de Segurança**: Alinhar as práticas de segurança com as normas e recomendações técnicas mais recentes, garantindo a conformidade e a eficácia das medidas de proteção adotadas.

3. ESPECIFICAÇÃO DO PRODUTO/ SERVIÇO:

Item	Descrição	Quantidade
3.1	**Solução de Hardware**	
3.1.1	Servidor para Solução de Backup	8
3.1.2	Switch topo de Rack	4
3.1.3	Switch de Gerenciamento	2
3.1.4	Rack 19`42U	2
3.2	**Solução de Software**	
3.2.1	Licenciamento de Software para ambiente On-Premises	1
3.2.2	Licenciamento de Software para ambiente Office365	2500 usuários
3.3	**Serviços de Implantação**	
3.3.1	Serviços de Instalação e Configuração	1
3.3.2	Serviços de Treinamento Oficial	1
3.3.3	Serviços de Garantia	1

Tabela 1 – Resumo dos itens

3.1. **SOLUÇÃO DE HARDWARE**

3.1.1.**SERVIDORES PARA SOLUÇÃO DE SOFTWARE DE BACKUP**

3.1.1.1. Deverão ser fornecidos, no mínimo, 4 (quatro) servidores físicos para cada um dos 2 (dois) data centers para rodar o software de backup (servidores de gerenciamento, movimentadores de dados de backup ou outros servidores requeridos). Esses servidores deverão ser dimensionados, no mínimo, conforme as especificações listadas neste ITEM 1, ou em quantidade e recursos de acordo com as melhores práticas de cada fabricante, garantindo o atendimento integral ao aspecto de disponibilidade e agilidade da solução especificada. Caso as melhores práticas definidas pelo fabricante do software sejam inferiores às aqui especificadas, deverão prevalecer as especificações deste termo de referência, sendo elas:

3.1.1.2. **Processador**

3.1.1.2.1. Deve possuir 2 (dois) processadores Intel ou AMD;

3.1.1.2.2. Deve possuir 16 (dezesseis) cores em cada processador;

3.1.1.2.3. Deve ter compatibilidade com a arquitetura x86 com extensões de 64 bits;

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.1.1.2.4. Deve ter índice SPEC CPU2017 Integer Rate Results (Baseline) auditado de no mínimo 339 para 2 (dois) processadores. Os índices SPEC CPU2017 Integer Rate Results (Baseline) utilizados como referência serão validados junto ao site da Internet http://www.spec.org/ Standard Performance Evaluation Corporation. Não serão aceitas estimativas para modelos/famílias de processadores não auditados pelo SPEC, resultados obtidos com a utilização de servidores em cluster, bem como estimativas em resultados inferiores ao mínimo especificado;

3.1.1.2.5. Deve implementar mecanismos de gerenciamento do consumo de energia compatível com o padrão ACPI v4;

3.1.1.2.6. Deve consumir no máximo 205 W;

3.1.1.2.7. Deve possuir tecnologia de no máximo 10 nm;

3.1.1.2.8. Deve possuir frequência de clock interno de no mínimo 2.8 GHz;

3.1.1.2.9. Deve possuir controladora de memória com suporte a DDR4 de no mínimo 3200 MHz, oferecendo no mínimo 8 (oito) canais de memória;

3.1.1.2.10. Deve possuir link de comunicação do processador com o restante do sistema de 16 GT/s;

3.1.1.2.11. Deve possuir memória cache de no mínimo 37 MB – L3;

3.1.1.2.12. Deve suportar o conjunto de instruções SSE4.2, AMX, AVX, AVX-512 e TSX-NI;

3.1.1.3. **Memória RAM:**

3.1.1.3.1. Deve possuir 256 (duzentos e cinquenta e seis) GB de memória RAM através de módulos de memória, os quais:

3.1.1.3.2. Deverão ser do tipo DDR4 RDIMM (Registred DIMM) ou LRDIMM (Load Reduced DIMM);

3.1.1.3.3. Deverão possuir tecnologia de correção ECC (Error Correcting Code);

3.1.1.3.4. Deverão possuir velocidade de, no mínimo, 3200 MHz;

3.1.1.3.5. Deverão ser de 32GB de memória RAM;

3.1.1.3.6. Deve possuir no mínimo 32 (trinta e dois) slots de memória DIMM;

3.1.1.4. **Disco Rígido:**

3.1.1.4.1. Possuir dispositivo otimizado e dedicado para armazenamento para inicialização do sistema operacional:

3.1.1.4.1.1. Ser do tipo PCIe e implementar RAID 1;

3.1.1.4.1.2. Possuir 2 (dois) discos Flash Card do tipo M.2, redundantes (espelhados), para boot com capacidade mínima de 480GB (quatrocentos e oitenta gigabytes) por cada disco;

3.1.1.4.2. Possuir, no mínimo, 4 (quatro) discos 3.0TB SSD com no mínimo 12Gbps, hot plug configuráveis em RAID 6, considerando a implementação de tolerância a falhas.

3.1.1.4.3. A interface controladora de armazenamento deve possuir as seguintes características:

3.1.1.4.4. Taxa de transferência de, no mínimo, 12Gbps por canal e ser totalmente compatível com os discos fornecidos.

3.1.1.4.5. Possuir, no mínimo, 4 GB de cache, suportado por bateria (inclusa) ou ser do tipo flash, com suporte a write-back cache.

3.1.1.4.6. Possuir memória não volátil para backup de configuração ou tecnologia similar.

3.1.1.4.7. Suportar no mínimo RAID 0, 1, 5, 6, 10 por hardware.

3.1.1.4.8. Ser capaz de identificar automaticamente falhas nos discos e refazer o array quando inserido novo disco.

3.1.1.4.9. Possuir suporte à expansão de capacidade do array de discos e à migração de nível de RAID, ambas em modo on-line, isto é, sem indisponibilidade do sistema operacional ou virtualizador.

3.1.1.4.10. Tecnologia de pré-falha SMART (Self Monitor Analysis Report Test) ou equivalente incorporado, atrelado à controladora de disco e a software de gerenciamento.

3.1.1.5. **Adaptador de rede:**

3.1.1.5.1. Deve possuir, no mínimo, 4 (quatro) interfaces de rede Ethernet 100GbE por servidor;

3.1.1.5.2. As interfaces de rede devem ser compatíveis com os conectores QSFP28;

3.1.1.5.3. Deve possuir suporte nativo RDMA (iWARP ou RoCE) e DCBx, SR-IOV;

3.1.1.5.4. As placas de rede ofertadas devem suportar o recurso de NIC Bonding;

3.1.1.5.5. Deve possuir suporte à VLAN, Link Aggregation e Jumbo Frames;

3.1.1.5.6. Deve possuir o recurso PXE (Pre Boot Execution Environment);

3.1.1.5.7. Deve ser compatível com os padrões IPv4 e IPv6;

3.1.1.5.8. Deve possuir interface de gerenciamento, sem necessidade de instalação de sistema operacional ou virtualizador no equipamento, devendo contar com mecanismo de hardware, com software embarcado, com suporte a Console Remota e controle do botão Power/Reset do equipamento;

3.1.1.5.9. Deve fornecer patch cords no padrão CAT6A de pelo menos 2.5 m, em quantidade suficiente para conexão de TODAS as portas de gerenciamento dos equipamentos ofertados.

3.1.1.5.10. Deve fornecer cabos DAC QSFP28 ou superior, de 3m, em quantidade suficiente para atender a TODAS as portas;

3.1.1.6. **Adaptador Fiber Channel:**

3.1.1.6.1. Deve possuir, no mínimo, 2 (duas) interfaces fiber channel com velocidade de 32 Gbps, ou superior, por servidor;

3.1.1.6.2. Deve possuir suporte a especificação plug and play;

3.1.1.6.3. Deve possuir compatibilidade com switches SAN Brocade e Cisco do tipo short wave;

3.1.1.6.4. Deve possuir suporte a serviços fiber channel class 2 e 3;

3.1.1.6.5. Deve possuir suporte a topologia switched fabric;

3.1.1.6.6. Deve possuir conexão ao fabric via F-Port;

3.1.1.6.7. Deve possuir software de diagnóstico e verificação da configuração;

3.1.1.6.8. Deve possuir capacidade de realizar diagnósticos de pré-falha de cabeamento e parte ótica em conjunto com switches Broadcom/Brocade;

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.1.1.6.9. Deve acompanhar 4 (quatro) cordões óticos contendo um par de fibras multímodo cada, com terminações padrão LC e comprimento de, no mínimo, 3 (três) metros;

3.1.1.7. **Configuração de Chassis:**

3.1.1.7.1. Deve ser servidor de rack;

3.1.1.7.2. Deve possuir no mínimo 02 (duas) fontes de alimentação internas ao chassi, redundantes e hot swap, operando automaticamente em tensões de 220 VAC a 240 VAC e em frequência de 60 Hz, cada uma delas configuradas com capacidade para suportar isoladamente a configuração ofertada do chassi e com alimentação através de circuitos elétricos de entrada distintos;

3.1.1.7.3. Deve acompanhar os respectivos cabos e adaptadores para conexão elétrica nos padrões IEC60320 C13-C14.

3.1.1.7.4. Deve suportar e fornecer energia para todos os equipamentos ofertados, em PDU´s distintas para dois circuitos elétricos diferentes.

3.1.1.7.5. Todos os conectores presentes nas PDUs devem estar eletricamente alimentados.

3.1.1.7.6. Cada PDU deve possuir plug para interligação com os circuitos elétricos conforme norma IEC 60309 para interligação com os circuitos elétricos do sistema FFT.

3.1.1.7.7. Deve fornecer conjuntos (kits) para montagem em rack de 19 polegadas;

3.1.1.8. **Sistema Operacional:**

3.1.1.8.1. Deve ser totalmente compatível com o sistema operacional Red Hat Enterprise Linux;

3.1.1.8.2. Deve ser totalmente compatível com o sistema operacional Microsoft Windows;

3.1.1.8.3. O modelo do equipamento ofertado deverá constar como certificado no https://hardware.redhat.com/;

3.1.1.8.4. Deve ser compatível com Windows Server 2019, ou versão superior, devendo o equipamento (marca e modelo) constar no Windows Server Catalog (http://windowsservercatalog.com);

3.1.1.8.5. O equipamento deverá vir acompanhado de uma licença OEM do sistema operacional Windows Server 2019 ou superior, ou Red Hat Enterprise Linux, conforme a recomendação do fabricante do software de backup.

3.1.1.9. **Especificação Complementar:**

3.1.1.9.1. O chipset ofertado deve ser da mesma marca do fabricante dos processadores;

3.1.1.9.2. Deve possuir no mínimo, 2 (dois) slots PCI Express 3.0;

3.1.1.9.3. A solução ofertada deve possuir Placa Mãe da mesma marca do fabricante do equipamento, desenvolvida especificamente para o modelo ofertado não sendo aceitas placas de livre comercialização no mercado;

3.1.1.9.4. Cada servidor deve possuir, no mínimo, 01 (uma) interface VGA ou SVGA e, no mínimo, 02 (duas) portas USB 2.0 ou USB 3.0;

3.1.1.9.5. Deve possuir controladora de vídeo do tipo onboard (integrado na Placa Mãe) ou do tipo Placa de Vídeo PCI;

3.1.1.9.6. Deve suportar resolução gráfica de no mínimo 1280x1024 pixels;

3.1.1.9.7. BIOS desenvolvida pelo mesmo fabricante do equipamento, não sendo aceitas soluções em regime de OEM ou customizadas;

3.1.1.9.8. A BIOS deve possuir o número de série do equipamento e campo editável que permita inserir identificação customizada podendo ser consultada por software de gerenciamento, como número de propriedade e de serviço;

3.1.1.9.9. A BIOS deve possuir opção de criação de senha de acesso, senha de administrador ao sistema de configuração do equipamento;

3.1.1.9.10. A BIOS deve ser atualizável exclusivamente através de softwares;

3.1.1.9.11. As atualizações de BIOS/UEFI deverão possuir (assinatura) autenticação criptográfica segundo as especificações NIST SP800-147B;

3.1.1.9.12. Deve possuir funcionalidade de recuperação de estado da BIOS/UEFI a uma versão anterior gravada em área de memória exclusiva e destinada a este fim, de modo a garantir recuperação em caso de eventuais falhas em atualizações ou incidentes de segurança;

3.1.1.9.13. Deve ser fornecido com Módulo TPM 2.0;

3.1.1.9.14. Possuir painel frontal (Bezel) com travamento por chave para segurança contra remoção dos discos;

3.1.2. **SWITCHES TOPO DE RACK**

3.1.2.1. **Especificação complementar:** Deverá fornecer switch topo de rack com as características mínimas a seguir:

3.1.2.1.1. Deve fornecer switch 100 GbE com no mínimo 32 (trinta e duas) portas QSFP28 operando a 100 Gb/s simultaneamente sem oversubscription.

3.1.2.1.2. A escolha da taxa de transmissão deve ser efetuada pelo tipo de SFP instalado na porta.

3.1.2.1.3. Deve possuir todas as licenças necessárias para sua utilização e versão de software mais recente.

3.1.2.1.4. Deve possuir 1 (uma) interface RJ-45 ou serial para acesso console local e 1 (uma) interface Gigabit Ethernet exclusiva para gerenciamento.

3.1.2.1.5. Deve fornecer 2 (dois) cabos DAC QSFP28 de 3 metros para agregação de portas multi-chassis, através da criação de redundância ativa/ativa livre de loop e sem utilização de protocolo Spanning Tree, conforme as tecnologias MLAG, MC-LAG, M-LAG, Virtual Link Trunking, Multi-Chassis EtherChannel ou equivalentes.

3.1.2.1.6. Deve fornecer cabos DAC QSFP28 e SFP28 ou superior, de 3m, em quantidade suficiente para atender a TODAS as portas da Solução de Backup

3.1.2.1.7. Os cabos DAC fornecidos devem ser completamente compatíveis com o equipamento ofertado e do mesmo FABRICANTE;

3.1.2.1.8. Deverá fornecer 4 (quatro) transceivers óticos QSPF28 100G BiDi por equipamento;

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.1.2.1.9. Para cada switch, devem ser fornecidos, no mínimo, 8 (oito) patch cords óticos LC Duplex de 3 (três) metros ou maior de comprimento;
3.1.2.1.10. Os transceivers fornecidos devem ser completamente compatíveis com o equipamento ofertado e do mesmo FABRICANTE.
3.1.2.1.11. Adicionalmente, deverá fornecer 2 (dois) transceivers óticos QSFP28 100G BiDi compatíveis com o equipamento Aruba 6340 (HPE 100Gb QSFP28 Bidirectional XCVR - PN 845972-B21);
3.1.2.1.12. Deve possuir latência de no máximo 1 µs (micro segundo).
3.1.2.1.13. Deve possuir capacidade de comutação de, no mínimo, 6.4 Tbps.
3.1.2.1.14. Deve possuir capacidade de encaminhamento de, no mínimo, 1.5 Bpps.
3.1.2.1.15. Deve possuir no mínimo 2 (duas) fontes de alimentação internas e redundantes de 220VAC.
3.1.2.1.16. Deve vir equipado com bandejas de ventilação tipo back to front redundante em pelo menos N+1, e deve vir em sua configuração máxima de ventilação possível.
3.1.2.1.17. Deve possuir tabela para no mínimo 64.000 (sessenta e quatro mil) endereços MAC.
3.1.2.1.18. Deve suportar pelo menos 4094 (quatro mil e noventa e quatro) VLANs.
3.1.2.1.19. Deve implementar Jumbo frames.
3.1.2.1.20. Deve implementar Jumbo frames com tamanho de no mínimo 9000 bytes.
3.1.2.1.21. Deve implementar Ethernet link aggregation.
3.1.2.1.22. Deve implementar IEEE 802.1D.
3.1.2.1.23. Deve implementar IEEE 802.1p Priority.
3.1.2.1.24. Deve implementar IEEE 802.1Q VLANs.
3.1.2.1.25. Deve implementar IEEE 802.1w.
3.1.2.1.26. Deve implementar IEEE 802.3ae.
3.1.2.1.27. Deve implementar IEEE 802.1Qbb.
3.1.2.1.28. Deve implementar IEEE 802.3x.
3.1.2.1.29. Deve implementar MSTP IEEE 802.1s com pelo menos 64 (sessenta e quatro) instâncias.
3.1.2.1.30. Deve implementar roteamento estático Ipv4.
3.1.2.1.31. Deve suportar Virtual Router Redundancy Protocol (VRRP).
3.1.2.1.32. Deve implementar roteamento estático Ipv6.
3.1.2.1.33. Deve implementar os seguintes protocolos de roteamento IPv4: OSPF e BGP.
3.1.2.1.34. Deve implementar os seguintes protocolos de roteamento IPv6: BGP.
3.1.2.1.35. Deve implementar SSH e RADIUS.
3.1.2.1.36. Deve permitir no mínimo 16.000 (dezesseis mil) rotas IPv4 e 8000 (oito mil) rotas IPv6.
3.1.2.1.37. Deve prover um controle completo do switch através de CLI (command line interface).
3.1.2.1.38. Deve permitir espelhamento de porta para monitoramento.

3.1.2.1.39. Deve suportar scripting através de REST API.

3.1.2.1.40. Deve possuir no mínimo 02 (dois) ventiladores redundantes e hot swap.

3.1.2.1.41. Deve possuir no mínimo 02 (duas) fontes de alimentação internas ao chassi, redundantes e hot swap, operando automaticamente em tensões de 200 VAC a 240 VAC e em frequência de 60 Hz, cada uma delas configuradas com capacidade para suportar isoladamente a configuração ofertada do chassi e com alimentação através de circuitos elétricos de entrada distintos.

3.1.2.1.42. Deve fornecer cabos para todas as fontes de alimentação de energia elétrica no padrão especificado no rack para servidores.

3.1.2.1.43. Deve fornecer conjuntos (kits) para montagem em rack de 19 polegadas.

3.1.3.**SWITCH DE GERENCIAMENTO**

3.1.3.1. Deverá fornecer um switch, com no mínimo, 24 portas 1GbE, por site, para as portas de gerenciamento da solução de hardware ofertada e com as seguintes características mínimas:

3.1.3.1.1. Deve permitir a sua instalação em rack padrão de 19”, devendo estar acompanhado de todos os adaptadores, suportes e guias necessários para a instalação;

3.1.3.1.2. Deve possuir fonte de alimentação interna ao equipamento com ajuste automático de tensão 110 e 220 Volts;

3.1.3.1.3. Deve possuir capacidade mínima de 52 Gbps por unidade;Deve possuir um throughput mínimo de 38 Mpps;Deve possuir no mínimo 24 (vinte e quatro) portas 10/100/1000BaseT “auto-sensing” e com seleção automática do modo de operação (halfduplex/full-duplex) em conectores do tipo RJ45 diretamente conectados ao equipamento;

3.1.3.1.4. Deve possuir no mínimo 2 (duas) portas para uplink 10GbE SFP+ ou superior.

3.1.3.1.5. Devem ser fornecidos transceivers compatíveis com o switch topo de rack para interconexão;

3.1.3.1.6. Deve fornecer 24 (vinte e quatro) patch cords no padrão CAT6A de pelo menos 2.5 m;

3.1.3.1.7. Todas as licenças necessárias para as funcionalidades exigidas neste Termo de Referência deverão estar inclusas no equipamento;

3.1.3.1.8. Deve permitir agregação de links conforme o padrão IEEE802.3ad, suportando a criação de no mínimo 6 grupos “LAG” por unidade;

3.1.3.1.9. Deve implementar espelhamento de tráfego para análise de rede, funcionalidade SPAN, port mirror ou similar;

3.1.3.1.10. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada;

3.1.3.1.11. Deve implementar controle de acesso por porta (IEEE 802.1x);

3.1.3.1.12. Deve implementar o protocolo de autenticação IEEE802.1x com atribuição dinâmica de VLAN;

3.1.3.1.13. Deve implementar IEEE 802.1p ¬ Classe de Serviços;

3.1.3.1.14. Deve implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
3.1.3.1.15. Deve implementar IEEE 802.3x;
3.1.3.1.16. Deve permitir no mínimo 16.000 entradas de endereços MAC em sua tabela de endereçamentos;
3.1.3.1.17. Deve permitir no mínimo 512 VLANs ativas por unidade conforme o padrão IEEE 802.1Q;
3.1.3.1.18. Deve possuir no mínimo 4 filas de classificação de prioridade por porta, conforme protocolo 802.1p;
3.1.3.1.19. Deve suportar o standard IEEE 802.3az (Energy Efficient Ethernet - EEE);Deve implementar IEEE 802.1Q;
3.1.3.1.20. Deve implementar, no mínimo, 30 (trinta) sessões IEEE 802.1X ou Web ou autenticação por MAC simultaneamente por porta;
3.1.3.1.21. Deve suportar controle de acesso baseado em perfis (Role Based Access Control);
3.1.3.1.22. Deve suportar a criação de um conjunto de políticas de acesso, segurança e QoS que pode ser atrelada a um usuário ou dispositivo da rede;
3.1.3.1.23. Deve implementar RADIUS Client;
3.1.3.1.24. Deve implementar LANs Virtuais (VLANs) conforme definições do padrão IEEE 802.1Q;Deve suportar VLANs dinâmicas;
3.1.3.1.25. Deve implementar "VLAN Trunking" conforme padrão IEEE 802.1Q nas portas Gigabit Ethernet. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos 802.1Q configurados;Deve implementar a funcionalidade de "Port Trunking" conforme padrão IEEE 802.1Q;
3.1.3.1.26. Deve implementar o Protocolo Spanning-Tree conforme padrão IEEE 802.1d;
3.1.3.1.27. A instalação e configuração dos equipamentos serão de responsabilidade da CONTRATADA.
3.1.3.1.28. Deve ser novo, sem uso, estar na linha atual de produção do fabricante e ser fornecido com a versão de firmware mais atual disponível para o equipamento;

3.1.4.**RACK 19'' 42U**

3.1.4.1. Especificação complementar:

3.1.4.1.1. Deve ser fornecido um rack para servidores no padrão 19' polegadas e altura máxima de 42 U.
3.1.4.1.2. Os racks devem ser fornecidos em quantidade suficiente para abarcar toda solução de hardware para backup seguindo as recomendações de melhores práticas de todos os fabricantes da solução de backup.
3.1.4.1.3. Deve acompanhar os respectivos cabos e adaptadores para conexão elétrica nos padrões IEC60320 C13-C14.
3.1.4.1.4. Deve acompanhar PDU's padrão IEC60320 C13-C14 para instalação em rack de 19 polegadas, conforme a quantidade de equipamentos ofertados.
3.1.4.1.5. Deve suportar e fornecer energia para todos os equipamentos ofertados, em PDU´s distintas para dois circuitos elétricos diferentes.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.1.4.1.6. Todos os conectores presentes nas PDU's devem estar eletricamente alimentados.

3.1.4.1.7. Cada PDU deve possuir plug para interligação com os circuitos elétricos conforme norma IEC 60309 para interligação com os circuitos elétricos do sistema FFT.

3.2. **SOLUÇÃO DE SOFTWARE**

O software de backup (backup e recovery) ofertado deve atender integralmente os requisitos para a coordenação e o gerenciamento das tarefas e operações de backup e recovery dos dados e arquivos, devendo ser fornecido com todas as licenças que forem necessárias para entrega funcional da solução.

As licenças do software de backup deverão ser ofertadas na modalidade de licenciamento perpétuo, de modo a garantir que a solução não venha a perder qualquer funcionalidade operacional e que não sejam cobrados quaisquer valores adicionais pelo uso das referidas licenças do software de backup durante e após o término do CONTRATO.

O licenciamento de software de backup poderá adotar o modelo por subscrição desde que o acesso aos dados e todas as funcionalidades operacionais de restauração de dados sejam mantidos mesmo após o término do CONTRATO.

3.2.1. **Licenciamento de Software para ambiente On-Premises**

3.2.1.1. A solução deverá estar licenciada para a quantidade de pelo menos quinhentas (500) máquinas virtuais. Para os ambientes físicos, a proteção deve ser feita através do uso de agentes para até duzentos (200) servidores físicos com sistemas operacionais Windows Server e Linux;

3.2.1.2. O software de backup deve possuir catálogo ou banco de dados centralizado contendo as informações sobre todos os dados e mídias onde os backups estão armazenados, esse banco de dados ou catálogo deve ser próprio e fornecido em conjunto com o produto;

3.2.1.3. O software de backup deve possuir mecanismo de verificação e checagem de consistência da base de dados ou da cadeia de bakup, no intuito de garantir a integridade dos dados;

3.2.1.4. O software de backup deve possuir mecanismo de reconstrução do catálogo ou banco de dados centralizado em caso de perda do mesmo, sem a necessidade de recatalogar as imagens de backup;

3.2.1.5. O software de backup deve fazer uso de um sistema gerencial do banco de dados para guardar o catálogo de Jobs, arquivos e mídias dos backups;

3.2.1.6. O software de backup 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;

3.2.1.7. Caso o software de backup dependa de catálogo, o mesmo 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 nas plataformas Red Hat Enterprise Linux e Microsoft Windows Server;

3.2.1.8. O software de backup deve ser implementado na plataforma Red Hat Enterprise Linux ou Microsoft Windows Server 2022;

3.2.1.9. O software de backup deve suportar servidores movimentadores de dados (servidores de backup) em pelo menos uma das seguintes plataformas: Linux ou Windows;

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.2.1.10. Os servidores movimentadores de dados (proxies, media agentes, media servers) devem suportar balanceamento de carga para distribuir a carga entre os mesmos de forma automática.

3.2.1.11. Os servidores movimentadores de dados (proxies, media agentes, media servers) 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;

3.2.1.12. O software de backup deverá suportar o backup e o restore de diferentes sistemas operacionais e versões superiores tais como Windows (2012/2012R2/2016/2019/2022), Oracle Linux (7/8), Red Hat Enterprise Linux (6/78), CentOS (7/8), Ubuntu (18.04), em ambientes virtuais como VMware VSphere 7.0 e superiores e Hyper-V (2012/2016/2019/2022);

3.2.1.13. Poderá ser feito uso de versões de agentes backlevel, para versões antigas de Aplicações e Sistemas Operacionais;

3.2.1.14. O software de backup deve permitir o backup e restore de arquivos abertos, garantindo a integridade do backup;

3.2.1.15. O software de backup deve ser capaz de gerenciar múltiplos e diferentes dispositivos de backup , 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);

3.2.1.16. O software de backup deve 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;

3.2.1.17. Caso o software de backup dependa de backup a nível de arquivos (file level), o mesmo deverá possuir a capacidade de dividir o fluxo de dados proveniente de um servidor em vários dispositivos de gravação (multiple streams);

3.2.1.18. O software de backup deve possuir a capacidade de reiniciar backups a partir do ponto de falha, após a ocorrência da mesma;

3.2.1.19. O software de backup deve possuir mecanismo de atualização de clientes e agentes de backup de forma remota, através da interface de gerenciamento, permitindo a instalação de múltiplos clientes de backup simultaneamente;

3.2.1.20. O software de backup deve possuir a capacidade de realizar download e instalação de atualizações em clientes, de forma automática, e para o servidor de backup deve ao menos notificar sobre novas versões, incluindo o link para download da versão citada;

3.2.1.21. O software de backup deve possuir ambiente de gerenciamento, monitoramento de criação de políticas de backup e restore via interface gráfica e linha de comando;

3.2.1.22. O software de backup deve possuir função de agendamento do backup através de calendário;

3.2.1.23. O software de backup deve possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades de administração e operação do software de backup;

3.2.1.24. O software de backup deve possuir função para definição de prioridades de execução de Jobs de backup;

3.2.1.25. O software de backup deve permitir o agendamento de trabalhos (jobs) de backup, sem utilização de utilitários de agendamento dos hosts;

3.2.1.26. O software de backup deverá permitir a programação de trabalhos (jobs) de backup automatizadas em que sejam definidos prazos de retenção dos arquivos e imagens;

3.2.1.27. O software de backup deve 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;

3.2.1.28. O software de backup deve 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;

3.2.1.29. O software de backup deve permitir a realização do backup completo de servidor para recuperação de desastres;

3.2.1.30. O software de backup deve permitir restaurar o backup de recuperação de desastres para hardware diferente do original;

3.2.1.31. O software de backup deve permitir o controle da banda de tráfego de rede ou oferecer técnicas que proporcionem a redução na utilização de rede durante a execução do backup e/ou do restore;

3.2.1.32. O software de backup deve ser capaz de recuperar dados para servidores diferentes do equipamento de origem;

3.2.1.33. O software de backup deve 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;

3.2.1.34. O software de backup deve 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;

3.2.1.35. O software de backup deve permitir que Logical Unit Numbers (LUNs) sejam apresentadas aos servidores da camada de mídia como destino para realização de backups;

3.2.1.36. O software de backup deverá permitir integração do controle de acesso com sistemas de diretório Active Directory;

3.2.1.37. Deverá possuir e implementar o fator duplo de autenticação para o console de administração gráfica por meio do provedor de identidade baseado em SAML ou (T)OTP ou cartões inteligentes ou certificados de usuário Criptografia;

3.2.1.38. O software de backup deve possuir interface única para gerenciamento de todos os servidores independente do Sistema Operacional que hospeda esse serviço (Windows, Linux);

3.2.1.39. O software de backup deve implementar monitoramento e administração remotos da solução de backup a partir de qualquer servidor ou estação de trabalho Windows;

3.2.1.40. O software de backup deverá permitir operações de Backup e Restore através de rede local (LAN e SAN);

3.2.1.41. O Software 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;

3.2.1.42. O Software de backup 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, isto é, sem a utilização de software de terceiros);

3.2.1.43. Deve suportar criptografia dos dados na origem, suportando o tráfego de dados via rede já criptografado.

3.2.1.44. Deverá suportar o armazenamento dos backups criptografados no repositório de backups;

3.2.1.45. O software de backup 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;

3.2.1.46. O software de backup deve possuir a funcionalidade de orquestração e execução de cópias tipo clone e snapshot e restaurações, a partir de sua indexação;

3.2.1.47. Para esta funcionalidade, considerar que as cópias (clones e snapshots) serão executadas na camada do(s) subsistema(s) de discos e/ou virtualizador(es) de discos existentes nas instalações da CONTRATANTE.

3.2.1.48. A solução deverá prover funcionalidade de gerenciamento e orquestração de cópias de volumes (Clone / snapshots) junto aos sistemas de armazenamento (storage arrays) da CONTRATANTE, conforme relação no Anexo I, sendo de responsabilidade da CONTRATANTE o provisionamento de recursos e licenças requeridos por cada sistema de armazenamento envolvido nesse tipo de operação.

3.2.1.49. A CONTRATADA deverá comprovar a compatibilidade entre a solução proposta para execução dos requerimentos deste item junto aos sistemas de armazenamento da CONTRATANTE envolvidos com esse tipo de operação.

3.2.1.50. O software de backup deverá permitir a criação e gerenciamento de Snapshots através da ferramenta de administração;

3.2.1.51. O software de backup deverá possibilitar o registro dos Snapshots na base relacional de catálogos de forma a possibilitar a realização de buscas;

3.2.1.52. O software de backup deve 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;

3.2.1.53. O software de backup deve possibilitar enviar notificações, quando configurado, dos eventos por e-mail;

3.2.1.54. O software de backup deve possuir mecanismo de auditoria, permitindo a emissão de relatórios onde constem, no mínimo, as seguintes informações:

3.2.1.54.1. 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);

3.2.1.54.2. Auditoria e controle de acesso devem ser funcionais para operações realizadas via interface gráfica e linha de comando;

3.2.1.55. O software de backup deve prover monitoramento via interface gráfica e em tempo real dos Jobs sendo executados, incluindo visão de nível hierárquico dos Jobs;

3.2.1.56. O software de backup deve suportar operações de backup e restore em paralelo;

3.2.1.57. O software de backup deve permitir encadear Jobs para que um só comece após outro ter terminado;

3.2.1.58. O software de backup deve suportar armazenamento nos cloud storages: Amazon S3, Microsoft Azure e Google Cloud Storage;

3.2.1.59. Utilizando desduplicação, criptografia e imutabilidade para segurança contra Ransomware dos dados enviados para nuvem, ao menos, Amazon S3 e Microsoft Azure.

3.2.1.60. O software de backup deve prover relatórios gerenciais de backup com no mínimo as seguintes informações:

3.2.1.60.1. Backups com sucesso;

3.2.1.60.2. Backups com falha;

3.2.1.60.3. Volume de backup realizado;

3.2.1.60.4. Restores com sucesso;

3.2.1.60.5. Restores com falha;

3.2.1.60.6. Volume de restore realizado;

3.2.1.60.7. Clientes de backup configurados;

3.2.1.60.8. Ocupação no destino de backup;

3.2.1.60.9. Licenciamento e capacidade;

3.2.1.61. O software de backup deve possuir interface web para gerenciamento, monitoramento, emissão de alertas, emissão de relatórios sobre operações de backup e restore e emissão de relatórios sobre capacidade e tendência de crescimento do ambiente;

3.2.1.62. Se houver múltiplos ambientes de backup, uma única interface web deverá ser capaz de monitorar e agregar informações de diversos Servidores da Camada de

3.2.1.63. Gerenciamento para emissão dos relatórios;

3.2.1.64. Relatórios para verificar o nível de serviço, ou seja, visualização de que aplicações estão com políticas de backup ativadas e executadas periodicamente;

3.2.1.65. Deve permitir exportar relatórios no formato pdf e adicionalmente em pelo menos um dos formatos (html, doc, xlsx) ;

3.2.1.66. O software de backup deve ter Base de dados de relatórios para suportar armazenamento de dados históricos de no mínimo 12 (doze) meses;

3.2.1.67. O software de backup deve suportar as seguintes tecnologias de virtualização:

3.2.1.68. VMware vSphere: Ser comprovadamente compatível com o VADP (vStorage API for Data Protection) para realizar operações de Backup e Restore de ambientes VMware versão 6.7 e superior;

3.2.1.69. Suporte a VMware vCenter/vSphere possibilitando backup automático das máquinas virtuais e recuperação completa; Microsoft Hyper-V: Suporte a Microsoft Hyper-V Server 2012/R2, Microsoft Hyper-V Server 2016, Microsoft Hyper-V Server 2019, Microsoft Hyper-V Server 2022;

3.2.1.70. O software de backup deve possuir suporte a backup e restore de máquinas virtuais Microsoft Hyper-V e VMware 6.7 e versões superiores através de vStorage API com as seguintes características:

3.2.1.71. 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), e também arquivos de maneira granular sem a necessidade de scripts, área temporária ou montagem dos arquivos VMDK;

3.2.1.72. Deve suportar o uso da funcionalidade CBT (Change Block Tracking) para as operações de backup;

3.2.1.73. Deve permitir a recuperação granular de arquivos/aplicações através da execução de um único backup;

3.2.1.74. Permitir o descobrimento automático das máquinas virtuais nos ambientes VMware, com capacidade de realizar filtros avançados com critérios como:

3.2.1.74.1. Nome da máquina virtual;
3.2.1.74.2. Sistema Operacional;
3.2.1.74.3. Serão aceitas soluções que possuam o recurso de criação de Tags de forma dinâmica para atender tal funcionalidade;
3.2.1.74.4. DataStore (Vmware);
3.2.1.74.5. vApp;
3.2.1.74.6. VM Folder;
3.2.1.74.7. DataCenter;
3.2.1.74.8. Host/Cluster;
3.2.1.74.9. Resource Pool

3.2.1.75. Deve possuir a capacidade de balanceamento de carga automático dos backups através de múltiplos backups hosts;

3.2.1.76. 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 da VM de origem disponíveis para o processo de recuperação instantânea;

3.2.1.77. Deve prover otimização do backup e recursos, permitindo que somente blocos utilizados sejam copiados no processo de backup;

3.2.1.78. Deve permitir a realização de backups e monitoração do backup de máquinas virtuais através de plug-in integrado ao vCenter ou vSphere 6.7 Web Client;

3.2.1.79. Deve possuir capacidade de realizar backup de maneira off-host, sem a necessidade de instalação de agentes nas máquinas virtuais;

3.2.1.80. Deve possuir capacidade de realizar backup de máquinas virtuais em estado online ou offline;

3.2.1.81. Deve possuir a capacidade de realizar backup de máquinas virtuais existentes em um vApp;

3.2.1.82. Deve possuir a capacidade de recuperação da imagem da máquina virtual, para máquinas que possuam discos VMFS ou RDM;

3.2.1.83. O software de backup deve possuir a capacidade de realizar backup de maneira Full, incremental ou Diferencial sem a necessidade de instalação de agentes nas máquinas virtuais;

3.2.1.84. O software de backup deve suportar ambientes configurados com Cluster Shared Volumes;

3.2.1.85. O software de backup 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 ou vmdk), e também arquivos de maneira granular para VMs Windows;

3.2.1.86. O software de backup deve possuir a capacidade de recuperação das máquinas virtuais para uma área temporária de disco;

3.2.1.87. O licenciamento do software de backup deve abranger os dois sites da CONTRATANTE, permitindo a proteção de uma quantidade ilimitada de agentes por servidor (físico ou virtual) para, no mínimo, as seguintes aplicações e banco de dados:
3.2.1.87.1. Microsoft SQL Server versões 2012, 2014, 2016, 2017 e 2019;
3.2.1.87.2. Microsoft Exchange 2013 e 2016;
3.2.1.87.3. PostgreSQL 12 e superiores;
3.2.1.87.4. Será permitido o uso de pré-script caso a versão esteja fora da matriz de compatibilidade do software de backup;

3.2.1.87.5. MySQL 5.7 e superiores;

3.2.1.87.6. Será permitido o uso de pré-script caso a versão esteja fora da matriz de compatibilidade do software de backup;

3.2.1.87.7. Microsoft Active Directory

3.2.1.87.8. O software de backup deve suportar DAG (DataBase Availability Groups) do MS Exchange;

3.2.1.88. O software de backup 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;

3.2.1.89. O software de backup 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;

3.2.1.90. Caso o software de backup dependa de catálogo, deverá possibilitar a distribuição automática de carga entre os servidores que executarão o serviço de Proteção da Informação, 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 terceiros;

3.2.1.91. O software de backup deverá fazer uso de tecnologia de replicação dos dados (não somente os dados protegidos – imagens de backup – mas também do catálogo do software de backup necessários para a recuperação do site principal para o site de desastre, de forma que em um evento de desastre, os sites sejam independentes no processo de recuperação;

3.2.1.91.1. Caso a solução de backup dependa de catálogo, as credenciais de acesso a console de gerenciamento e catálogo de cada site devem ser independentes para isolamento em caso de ataque de Ransomware;

3.2.1.91.2. As soluções que não dependam de catálogo devem possuir mecanismo que permita criptografar o backup armazenado com chave AES 256 e deverá exigir tal chave para importar os backups em outro servidor de backup;

3.2.1.92. A solução ofertada deverá possuir, de forma nativa e/ou integrada, mecanismos e funcionalidades de proteção (que deverão estar 100% licenciados) para atuar, e eventualmente bloquear ataques cibernéticos (tipo “ransomware” – sequestro de dados), prevenindo a perda e/ou indisponibilidade de dados por remoção ou criptografia, considerando as seguintes características:

3.2.1.93. Os dados armazenados nos repositórios de backup devem estar protegidos contra alterações indesejadas, e ser imutáveis, ou seja, não podem ser modificados por agentes externos ao backup, de modo que eles só possam ser alterados ou removidos mediante expiração do backup e respeitar o período estabelecido para remoção;

3.2.1.94. Possuir mecanismos que previnam que hackers ou mesmo administradores maliciosos tenham acesso a senhas de administração do backup e sejam capazes de remover dados utilizando a própria ferramenta de backup;

3.2.1.95. Possuir mecanismos que impeçam a deleção de backups do armazenamento do backup (funcionalidades do tipo “Ramsomware Protection”) que garantam o bloqueio do repositório de armazenamento de backup.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.2.1.96. O software de backup deve possuir o recurso de dupla autenticação (2FA – Two Factor Authentication) ou (Four Eyes Principle) para executar atividades administrativas de exclusão no equipamento;
3.2.1.97. Deverá exigir a autenticação e autorização de um segundo usuário (escalação) para concluir a alteração de parâmetros críticos, como, por exemplo, a deleção de uma imagem de backup;
3.2.1.98. O software de backup deve suportar e estar licenciado com a funcionalidade de criptografia do tipo DARE (Data At Rest Encryption) de no mínimo 256 bits com certificação FIPS 140-2;
3.2.1.99. A solução ofertada deve garantir o Reforço da infraestrutura (Infrastructure hardening);
3.2.1.100. O software de backup deve permitir o uso das melhores práticas de provisionamento de sistemas operacionais certificadas e aprovadas por estes organismos;
3.2.1.101. O software de backup deve possuir mecanismos de controles dos binários dos aplicativos que compõem a solução através do uso de assinatura digital;
3.2.1.102. Caso o software de backup e proteção de dados demande de licenciamento para replicação de dados “Air Gap”, deverão ser ofertadas as licenças para toda a capacidade de 1.5 Petabytes por site.
3.2.1.103. Para atender os princípios de Isolamento dos Dados por meio de segmentação da rede de dados de backup, a solução deve prover os seguintes pontos:
3.2.1.104. Deve suportar criptografia in Flight visando proteger o conteúdo do backup durante o transporte de dados;
3.2.1.105. Uso de gateway ou proxy entre suas zonas públicas e seguras;
3.2.1.106. A comunicação entre recursos de backup deve permitir o uso de certificados de autorização;
3.2.1.107. Validação dos Dados (Data Validation) – Testes de Integridade dos dados armazenados:
3.2.1.107.1. A solução deve prover recursos de validação dos dados armazenados nos repositórios de backup para verificar e garantir a integridade dos mesmos;
3.2.1.107.2. A solução deve utilizar métodos de análise física de validação dos dados como: verificação de redundância cíclica (CRC), que realiza validação dos dados a nível de blocos, permitindo a identificação de blocos corrompidos e ações de correção;
3.2.1.107.3. A rotina de validação dos dados deve permitir o agendamento e ser executada periodicamente para garantir a integridade dos dados armazenados;
3.2.1.107.4. No caso de identificação de blocos corrompidos, a solução deve enviar alertas e notificações aos responsáveis;
3.2.1.107.5. A solução deve prover monitoramento de Ameaças (Threat Monitoring), permitindo assim a visibilidade de anomalias e falhas de backup, bem como uma visualização única de alertas atuais, histórico e tendências;
3.2.1.108. Monitoramento Ativo: A solução deverá monitorar continuamente as métricas para atividades anômalas do sistema de arquivos, como modificações e exclusões. Quando alterações anômalas no sistema de arquivos forem detectadas, alertas deverão ser acionados para fornecer motivo para ação. A solução deverá possuir mecanismos que permitam que alertas sejam integrados a informações de

segurança e gerenciamento de eventos (SIEM), outros sistemas de resposta a incidentes ou iniciar fluxos de trabalho.

3.2.2. **Licenciamento de Software para ambiente Office365**

3.2.2.1. O licenciamento deverá prover proteção para 1000 (mil) usuários de Microsoft Office365. A solução proposta deverá ser capaz de fazer backup e recuperar dados no Microsoft Office365, com base em um licenciamento único, tendo como métrica a quantidade de 1000 usuários, com atendimento 24x7 pelo período de 60 (sessenta) meses.

3.2.2.2. A solução ofertada deverá possuir integração com Microsoft Office 365:

3.2.2.2.1. Deverá suportar minimamente a proteção dos seguintes itens:

3.2.2.2.1.1. Calendário;

3.2.2.2.1.2. OneDrive (pasta e arquivos individuais);

3.2.2.2.1.3. Sites;

3.2.2.2.1.4. Contatos;

3.2.2.2.1.5. Tarefas;

3.2.2.2.1.6. E-mail

3.2.2.2.1.7. Caixas de e-mail compartilhadas

3.2.2.2.1.8. Grupos do Teams (arquivos postados e conversas)

3.2.2.2.1.9. SharePoint sites (site inteiro e arquivos individuais)

3.2.2.3. Operação de recuperação dos dados, no mínimo, nos seguintes níveis:

3.2.2.3.1. Microsoft Exchange: Caixa postal completa e Itens individuais (arquivos, e-mail, contatos, calendário);

3.2.2.3.2. OneDrive: Pasta completa e arquivos individuais, inclusive anotações do OneNote;

3.2.2.3.3. Grupos do Teams: Conversas e arquivos;

3.2.2.3.4. SharePoint: site completo e arquivos individuais;

3.2.2.3.5. Usuário;

3.2.2.4. Operação de recuperação versões anteriores, devendo disponibilizar, no mínimo, as seguintes formas de recuperação dos dados:

3.2.2.4.1. Recuperação para o local de origem;

3.2.2.4.2. Fazer download do arquivo;

3.2.2.5. Deverá permitir enviar notificações sobre os resultados das tarefas de backup por e-mail ou disponibilizadas em uma central de notificações.

3.2.2.6. A solução deve criptografar a comunicação entre o Office 365 e a infraestrutura de backup usando SSL.

3.2.2.7. Deve permitir a adição de contas de backup auxiliares da organização, por meio de grupos de segurança pré-configurados do Office 365;

3.2.2.8. Deverá oferecer a capacidade de ajuste do uso da largura de banda durante as tarefas de backup;

3.2.2.9. A solução deve ter a opção de executar a criptografia AES de 256 bits dos dados armazenados, de forma nativa ou através de criptografia a nível de disco.

3.2.2.10. A implementação deve permitir a configuração ou geração de políticas de retenção.

3.2.2.11. Deverá suportar o armazenamento dos dados localmente, seja em volumes locais ou apresentados via SAN, além de suportar o armazenamento em ambiente On-Premises (Local) e Cloud gravando em Object Storage compatível com S3.

3.2.2.12. A solução deverá criar várias tarefas de backup na mesma organização do Office 365, permitindo a inclusão ou exclusão de tipos de objetos de acordo com as

necessidades da organização. Para tarefas de backup configuradas, deve ser possível configurar a seguinte opção de agendamento:

3.2.2.12.1. Execução diária em horários e dias específicos;

3.2.2.13. A solução deverá fornecer uma interface para exibir as estatísticas dos objetos processados em cada sessão de backup.

3.2.2.14. A solução deverá ter a capacidade de procurar itens do Exchange a partir de uma interface guiada sem a necessidade de processos de recuperações anteriores.

3.2.2.15. A solução deve ter a capacidade de recuperar uma caixa de correio inteira ou selecionar individualmente quaisquer itens e recuperá-los para qualquer caixa de correio existente, ou exportá-los para arquivos .PST ou .EML.

3.2.2.16. Oferecer suporte a utilização de usuários com autenticação multi-fator (MFA) habilitada para execução segura dos processos de backup e restauração. Suportar mecanismos de autenticação moderna para operações de backup.

3.2.2.17. Disponibilizar logs de auditoria para as operações dos usuários realizadas na plataforma com, no mínimo, as seguintes informações:

3.2.2.17.1. Logon na console;

3.2.2.17.2. Arquivos baixados (download);

3.2.2.17.3. Arquivos pré-visualizados;

3.2.2.17.4. Tenant adicionado ou/e removido;

3.2.2.17.5. Arquivos recuperados;

3.2.2.18. Deve incluir relatórios para identificar estado da proteção de caixas de correio do Office 365, gerenciar o uso de licenças e obter visibilidade sobre o consumo de armazenamento.

3.2.2.19. A solução deve oferecer opções de retenção com base na data de criação dos itens em seu local original, ou baseadas na data de execução dos backups.

3.2.2.20. Permitir exportar o conteúdo de backup, possibilitando o transporte físico de dados.

3.3. **SERVIÇOS DE IMPLANTAÇÃO**

3.3.1. **SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO**

3.3.1.1. Deve contemplar a montagem de todos os componentes conforme orientação técnica da CONTRATANTE, incluindo conexões e organizações dos cabos da melhor forma.

3.3.1.2. Deve entregar o cabeamento organizado de forma a minimizar a visualização dos mesmos pela parte frontal ou traseira do rack, com distinção de cores dos cabos conforme o circuito de rede.

3.3.1.3. A CONTRATADA deve realizar a montagem, instalação e configuração nos dois (2) data centers, incluindo o material, mão de obra, insumos e ferramentas, sem ônus adicional para a CONTRATANTE.

3.3.1.4. Deve incluir assessoria de implantação e acompanhamento para a instalação física e lógica da solução, sua ativação, configuração e testes para garantir o pleno funcionamento de toda a solução.

3.3.1.5. Deve ser fornecido, após a instalação física do equipamento, documentação da instalação na qual inclua as identificações dos cabos, conectores e interligações elétricas e de rede, com diagramas (bayface) e também registros fotográficos da montagem.

3.3.1.6. Deve fornecer na documentação da instalação informações suficientes para que seja possível correlacionar os dispositivos lógicos com as interligações físicas de todos os componentes da solução.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.3.1.7. A definição de instalação e configuração da solução de salvamento e recuperação é entendida como a montagem dos componentes físicos, sua conexão na rede da CONTRATANTE e a configuração lógica de todos os produtos, testes de todas as capacidades, validação dos procedimentos necessários, validação da operação das funcionalidades contratadas e verificação dos critérios de qualidade definidos nesta aquisição.

3.3.1.8. A CONTRATADA deverá apresentar um documento com as melhores práticas do respectivo fabricante validando as configurações frente a oferta da solução proposta.

3.3.1.9. A CONTRADADA deverá fornecer os equipamentos com todos os itens acessórios de hardware e software necessários à sua perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, suportes, trilhos, drivers de controle e softwares.

3.3.1.10. A CONTRATADA deve garantir a plena compatibilidade de operação dos dois (2) conjuntos de repositórios de armazenamento implantados em harmonia com os demais equipamentos da infraestrutura computacional da CONTRATANTE em que estarão interligados, atendendo às regras e regulamentos estabelecidos em ambos os data centers.

3.3.1.11. A replicação de dados do data center principal para o secundário deve ser configurada pela CONTRATADA.

3.3.1.12. Não haverá serviço de migração do ambiente antigo de backup para a nova solução.

3.3.1.13. A CONTRATADA será responsável pelo transporte, desembalarem, instalação física, configuração e ativação dos softwares e equipamentos da solução.

3.3.1.14. Deverão ser configuradas todas as funcionalidades disponíveis no licenciamento do software de salvamento e recuperação de dados, bem como aquelas apontadas pelo CONTRATANTE conforme previsto na especificação técnica deste termo de referência.

3.3.1.15. Configuração do software de salvamento e recuperação de dados e dos repositórios de armazenamento em disco das estratégias de salvamento e recuperação e da replicação de dados definido pelo CONTRATANTE.

3.3.1.16. Configuração de alertas e relatórios disponíveis no software de salvamento e recuperação de dados e repositório de armazenamento em disco.

3.3.1.17. A atividades mínimas que devem estar cobertas pelos serviços de instalação e configuração da solução, compreendem, entre outros, os seguintes procedimentos:

3.3.1.17.1. Reuniões de alinhamento para criação do escopo do projeto de instalação;

3.3.1.17.2. Cronograma de execução;

3.3.1.17.3. Análise da topologia e arquitetura da solução, considerando todos os equipamentos já existentes e instalados;

3.3.1.17.4. Levantamento de informações sobre o ambiente;

3.3.1.17.5. Planejamento de funcionalidades a implementar;

3.3.1.17.6. Projeto de instalação;

3.3.1.17.7. Definição dos parâmetros de configuração a serem implementados;

3.3.1.17.8. Procedimentos de implementação;

3.3.1.17.9. Análise dos sistemas e ambientes dos dados protegidos pela solução;

3.3.1.17.10. Integração com a estrutura de rede local (LAN Local Área Network) e a rede de dispositivos de armazenamento (SAN Storage Area Network) e outros

ativos já existentes, com as devidas configurações de tolerância a falhas (failover) e balanceamento de carga (load balance);

3.3.1.17.11. Definição dos procedimentos de roll back;

3.3.1.17.12. Instalação física de todos os equipamentos (hardware) e softwares necessárias para atender os requisitos da solução fornecida;

3.3.1.17.13. Configurações das funcionalidades contratadas, incluindo os agentes nos datacenters principal e secundário, e localidades remotas;

3.3.1.17.14. Migração ou reconfiguração das regras e políticas de salvamento e recuperação de dados aplicáveis à solução ofertada;

3.3.1.17.15. Configuração do sistema de gerência e monitoramento da solução de salvamento e recuperação;

3.3.1.17.16. Transferência de conhecimento (Hands On);

3.3.1.17.17. Integração da solução com ferramenta de monitoramento externa da CONTRATANTE;

3.3.1.17.18. Testes e validações;

3.3.1.17.19. Homologação;

3.3.1.17.20. Documentação final da solução implantada.

3.3.1.18. Após a homologação da instalação e operação da solução em regime produtivo (ongoing), deve ser disponibilizado, de forma presencial na CONTRATANTE, um técnico especializado para acompanhar a equipe técnica de sustentação na execução das principais tarefas administrativas da operação diária, atuando em esclarecimentos, ajustes e eventuais correções, durante 5 (cinco) dias úteis (operação assistida).

3.3.1.19. Deve haver repasse de conhecimento para a equipe técnica da CONTRATANTE do ambiente implantado suficientes para supervisão e gestão do projeto de implementação, instalação e configuração.

3.3.1.20. Durante a implantação da solução a equipe da Contratada deverá repassar informações para a equipe da CONTRATANTE, e a quem ela definir a seu critério, apresentando as configurações realizadas nos equipamentos, a arquitetura final da solução e procedimentos executados.

3.3.1.21. Deve ser realizada a transferência de conhecimento sobre a solução durante o período de operação assistida sobre a solução no ambiente da CONTRATANTE, para no mínimo para 3 (três) profissionais a critério da CONTRATANTE (Hands On).

3.3.1.22. Os serviços de instalação e configuração e operação assistida serão iniciados em um prazo máximo de 60 (sessenta) dias corridos contados da data indicada na ordem de início de serviços.

3.3.1.23. Os serviços devem ser planejados em conjunto com a CONTRATANTE, prevendo o menor tempo de parada possível (downtime) dos serviços durante sua execução. A critério da CONTRATANTE este tempo de parada pode exigir tarefas e ações de mitigação deste tempo.

3.3.1.24. A critério da CONTRATANTE, os serviços (totalmente ou em parte) poderão ser executados fora do horário comercial ou em finais de semana e feriados, sem quaisquer custos adicionais de modo a minimizar os transtornos aos usuários pela eventual indisponibilidade dos serviços.

3.3.1.25. Devem ser realizadas as configurações de todas as funcionalidades presentes na solução, mesmo que não constem explicitamente neste documento.

3.3.1.26. Na realização dos serviços de implementação e repasse tecnológico, em nenhuma hipótese, haverá custos adicionais para a CONTRATANTE. O fornecedor é

responsável por todas as despesas, tais como transporte, hospedagem, alimentação e outras necessárias para execução dos serviços.

3.3.1.27. Os serviços de instalação e configuração deverão ser prestados por técnicos certificados pelos fabricantes da solução.

3.3.1.28. Durante todo o período de instalação e configuração, a fabricante deverá disponibilizar, mesmo que remotamente, equipe técnica para esclarecimento de dúvidas, validação das configurações pretendidas e aplicadas, além de resolução de problemas.

3.3.1.29. Sempre que for possível deve ser considerada a opção de instalação e configuração em modo de alta disponibilidade.

3.3.1.30. Toda a implantação e configurações da solução (políticas gerais, objetos, itens de administração) deve ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada.

3.3.1.31. O processo de implantação deve ser devidamente documentado. Esta documentação deve compor o relatório final da implantação com o detalhamento do processo realizado contendo todas as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado.

3.3.1.32. Prazo máximo para Instalação e configuração (implementação) da solução será de 90 (noventa) dias corridos contados a partir da entrega dos equipamentos, devendo preferencialmente, ser realizada em horário não comercial, conforme agendamento da contratante.

3.3.1.32.1. Deve ser fornecido juntamente com os produtos e licenças os manuais técnicos de referência, contendo todas as informações sobre os produtos com as instruções para instalação, configuração e operação, preferencialmente em português (Brasil), ou ser escritos em língua inglesa.

3.3.2. **SERVIÇOS DE TREINAMENTO OFICIAL**

3.3.2.1. O treinamento deverá ser ministrado abrangendo teoria e prática de implantação, configuração, administração, estratégias de backup e recovery, replicação de dados, solução de problemas e assuntos teóricos relacionados ao software de salvamento e recuperação de dados e repositórios de armazenamento em disco.

3.3.2.2. Caso a avaliação da qualidade do treinamento, realizada pelos participantes, não atingir uma aceitação mínima de setenta (70%) a CONTRATANTE poderá solicitar repetição do treinamento, com os ajustes necessários, sem quaisquer ônus adicional.

3.3.2.3. O treinamento deve ser composto por curso oficial da FABRICANTE da solução de software de backup, abrangendo conteúdo teórico e prático, abordando todas as funcionalidades da ferramenta e deve tratar, no mínimo, as seguintes abordagens:

3.3.2.3.1. Apresentação da arquitetura da solução e dos conceitos fundamentais;
3.3.2.3.2. Instalação da solução;
3.3.2.3.3. Configuração inicial;
3.3.2.3.4. Configuração de interface;
3.3.2.3.5. Funcionalidade de criptografia;
3.3.2.3.6. Perfil de acesso;
3.3.2.3.7. Políticas de segurança de dados aplicadas;
3.3.2.3.8. Configuração de alta disponibilidade (redundância, high availability);
3.3.2.3.9. Geração de relatórios;

3.3.2.3.10. Customização de relatórios existentes na solução adquirida, cujos casos aplicáveis a CONTRATANTE;
3.3.2.3.11. Configuração e gerenciamento da solução;
3.3.2.3.12. Operação completa da solução;
3.3.2.3.13. Análise e resolução de problemas (troubleshooting);
3.3.2.3.14. Alertas e ações;
3.3.2.3.15. Monitoramento;
3.3.2.3.16. Demais assuntos pertinentes a solução ofertada.

3.3.2.4. O treinamento deve ser ministrado com instrutores certificados na solução ofertada pelo fabricante.

3.3.2.5. O treinamento deve ser realizado no período de segunda a sexta-feira, em dias úteis, entre 8 (oito) horas e 18 (dezoito) horas, sendo que não poderá exceder o máximo de 8 (oito) horas diárias.

3.3.2.6. Na realização do treinamento, em nenhuma hipótese, haverá custos adicionais para a para realização do treinamento para a CONTRATANTE. O fornecedor deve fornecer toda a infraestrutura necessária para realização do treinamento. Recursos tais como instrutor, lanche, material, equipamentos, entre outros não terão ônus adicional para a CONTRATANTE.

3.3.2.7. O treinamento da solução adquirida será ministrado, preferencialmente, nas dependências da CONTRATANTE. A critério da CONTRATANTE, o fornecedor poderá fornecer vouchers para realização de treinamento na solução adquirida a ser realizado, de forma presencial, nas instalações do fabricante ou de parceiro autorizado. Nesta hipótese, todas as despesas de deslocamento, hospedagem e alimentação dos alunos serão de responsabilidade do fornecedor.

3.3.2.8. O treinamento deve ser ofertado em português e o material didático, preferencialmente, deve ser em português.

3.3.2.9. O treinamento deverá possuir carga horária adequada de forma a abranger todo o conhecimento necessário para operar a solução fornecida a CONTRATANTE, e em quantos módulos forem necessários, de acordo com o treinamento oficial.

3.3.2.10. O material didático deve ser oficial, sendo uma unidade para cada dos participantes.

3.3.2.11. Deve ser fornecido certificado de participação para cada participante a critério da CONTRATANTE. O certificado de conclusão do curso deve descrever ao menos o título do curso, ter o nome completo do participante, informar a carga horária, o nome do instrutor, local e data da realização do curso.

3.3.2.12. O treinamento deverá ser ministrado para no mínimo 6 (seis) integrantes da equipe da CONTRATANTE ou de seus subcontratados a seu critério.

3.3.2.13. O conteúdo teórico dos treinamentos deve ficar disponível para os participantes para pesquisas futuras, após a conclusão do curso.

3.3.3.**SERVIÇO DE GARANTIA**

3.3.3.1. A Garantia abrange TODOS os equipamentos do item 3.1 e iniciará somente após a emissão emitir o aceite definitivo. Este período de garantia será de 5(cinco) anos.

3.3.3.2. Deverá possuir suporte técnico e garantia on-site de 5 (cinco) anos para a solução de hardware, com atendimento 24x7 e tempo de resolução/reparo em até 8 (oito) horas para casos críticos de indisponibilidade da solução, podendo a reposição de peças ser no próximo dia útil (NBD - Next Business Day) nos casos em que não houver indisponibilidade;

3.3.3.3. Deve possibilitar a abertura dos chamados diretamente com o fabricante do componente;

3.3.3.4. Os chamados devem ser abertos através de telefone e através do website de suporte do fabricante da solução;

3.3.3.5. Os chamados abertos por telefone devem ser abertos através de um número 0800;

3.3.3.6. Deve permitir atualização para a versão mais recente de toda parte composta por software da solução durante todo o período de garantia;

3.3.3.7. A proposta deve conter declaração do fabricante da solução sobre a sua responsabilidade referente a garantia e SLA dos equipamentos bem como a lista de equipamentos e seus números de série deverão constar no site do fabricante;

3.3.3.8. Todos os equipamentos desse item deverão ser iguais, sem qualquer diferença de subcomponentes;

3.4. **LOCAIS DA ENTREGA E PRESTAÇÃO DOS SERVIÇOS**

3.4.1. A entrega e a prestação dos serviços serão realizadas em dois (2) datacenters localizados em Porto Alegre, RS, a serem definidos pela CONTRATANTE.

3.5. **HORÁRIOS DA PRESTAÇÃO DOS SERVIÇOS:**

3.5.1. Fica definido o horário das 09:00 às 17:00 nos locais para prestação de serviços.

3.5.2. A CONTRATANTE poderá considerar alterar os horários previamente definido através de estabelecimento de acordo com a CONTRATADA

4. DESCRIÇÃO DA SOLUÇÃO

4.1. A solução de Backup é um conjunto de ferramentas projetadas para garantir a segurança e disponibilidade dos dados críticos da SEFAZ oferecendo proteção contra uma variedade de ameaças cibernéticas e desastres naturais.

4.2. A solução deverá operar em alta disponibilidade, com os seguintes componentes principais:

4.2.1. Software de Backup com Recuperação Rápida: Um software robusto dedicado à realização de backups regulares dos dados críticos da SEFAZ, permitindo uma rápida recuperação em caso de perda de dados ou corrupção de arquivos. A solução também oferecerá proteção avançada contra-ataques ransomware, detectando e impedindo atividades maliciosas que possam comprometer a integridade dos dados.

4.2.2. As licenças do software de backup deverão ser ofertadas na modalidade de licenciamento perpétuo, de modo a garantir que a solução não venha a perder qualquer funcionalidade operacional e que não sejam cobrados quaisquer valores adicionais pelo uso das referidas licenças do software de backup durante e após o término do CONTRATO. O licenciamento de software de backup poderá adotar o modelo por subscrição desde que o acesso aos dados e todas as funcionalidades operacionais de restauração de dados sejam mantidos mesmo após o término do CONTRATO.

4.2.3. Serviço de Treinamento e Implantação: O serviço de treinamento e implantação da solução de backup fornecerá suporte especializado para garantir uma implementação eficiente da solução na infraestrutura existente da SEFAZ. Isso incluirá treinamento para a equipe de TI sobre as melhores práticas de configuração, operação e manutenção da solução de backup.

4.2.4. Compatibilidade com o Ambiente Existente e Integração com Soluções de Segurança: A solução de backup será totalmente compatível com o ambiente de TI atual da SEFAZ,

integrando-se perfeitamente aos ambientes de produção e desenvolvimento da SEFAZ. Além disso, será totalmente integrada às soluções de segurança existentes.

5. MODELO DE GESTÃO DO CONTRATO

5.1. Solução de Backup, com fornecimento de Licenças, pelo período de 60 meses: O contratado é obrigado a submeter, mensalmente, um relatório detalhado de todas as ordens de serviço geradas durante o período. Este documento deve incluir informações essenciais como data de abertura, fechamento, grau de criticidade, e o nome do responsável pela abertura de cada ordem.

5.2. Serviço de Implantação da Solução Backup:

5.2.1. Treinamento: Após a conclusão do treinamento, será necessário apresentar um relatório de encerramento que detalhe as datas de realização, carga horária total, identificação do responsável pelo treinamento, cópia do material didático utilizado, e a lista de participantes. Este documento visa documentar o cumprimento e a eficácia do treinamento oferecido.

5.2.2. Instalação e Configuração: Deve-se entregar um relatório resumido que destaque os principais marcos alcançados durante a fase de implantação, incluindo o cronograma de execução, os desafios encontrados e as soluções adotadas, culminando com o relatório final de implantação. Este relatório deve alinhar-se com os requisitos especificados no item 3.3.1.31, garantindo que todos os aspectos da implantação foram devidamente executados e documentados

6. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

6.1. O processo de medição e pagamento será estruturado em duas fases principais:

6.1.1. Na primeira fase, um Atestado de Recebimento Provisório será emitido. Esta etapa assegura que todos os equipamentos foram entregues no prazo estabelecido no edital.

6.1.2. A segunda fase, um atestado de recebimento definitivo será emitido, condicionado a finalização dos serviços de implantação e ativação das licenças.

6.2. O pagamento, por sua vez, será efetuado em uma parcela única, subsequente à emissão do Atestado de Recebimento Definitivo.

7. ADEQUAÇÃO ORÇAMENTÁRIA:

7.1. Esta aquisição será custeada com o Recurso 0377, Projeto 5735 – PROFISCO II.