

Introdução

A PROCEMPA encontra-se atualmente com uma infraestrutura tecnológica extremamente precária e desatualizada, resultado de um longo período sem investimentos significativos em renovação de equipamentos e sistemas. Essa defasagem tem elevado consideravelmente o risco operacional, tornando o ambiente suscetível a falhas críticas e a uma eventual interrupção total de serviços essenciais prestados à administração pública municipal.

Atualmente, a infraestrutura existente opera próxima ao seu limite técnico, o que implica em alto risco de indisponibilidade a qualquer momento. O cenário é de **manutenção emergencial constante**, com falhas recorrentes em equipamentos de missão crítica e limitações de capacidade em praticamente todos os sistemas corporativos.

Em 2024, a área técnica responsável realizou um extenso diagnóstico da situação atual e elaborou um **planejamento estratégico de investimentos em infraestrutura de TI** com horizonte até **2030**, contemplando as necessidades mínimas e obrigatórias para assegurar a continuidade, a segurança e a modernização dos serviços. Esse planejamento foi construído de forma criteriosa, com base em projeções de crescimento, obsolescência tecnológica e requisitos de disponibilidade compatíveis com as demandas atuais e futuras.

O conjunto de investimentos propostos visa garantir **a sustentabilidade tecnológica da PROCEMPA pelos próximos 5 a 7 anos**, estabelecendo uma base moderna, resiliente e escalável para suportar o crescimento das demandas de processamento, armazenamento e segurança da informação, conforme demonstrado em planilha anexa.

O presente documento, portanto, apresenta as justificativas técnicas que fundamentam os principais itens do termo de referência da Solução de Armazenamento de Dados e Backup.

(STORAGE) - CLASSE I VOLUMETRIA

5.1.1. Setecentos e Cinquenta (750) TiB de capacidade efetiva. Para o fornecimento da capacidade efetiva serão considerados ganhos de redução de dados obtidos através de compactação e deduplicação;

6.1.1. Quatro (4) PiB de capacidade efetiva. Para o fornecimento da capacidade efetiva serão considerados ganhos de redução de dados obtidos através de compactação e deduplicação.

Justificativa itens 5.1.1 e 6.1.1:

O espaço atualmente utilizado (novembro de 2025) nos ambientes de virtualização e de bancos de dados físicos é de aproximadamente 550 TB. Considerando um crescimento projetado de 50% nos próximos anos, justifica-se a capacidade solicitada para garantir a continuidade das operações e evitar esgotamento prematuro do espaço de armazenamento.

Para o ambiente de backup, foi considerado o volume atual de dados (arquivos de usuários, bancos de dados e ambiente de virtualização) somado às respectivas retenções (diária, mensal e anual), totalizando aproximadamente 2 PiB.

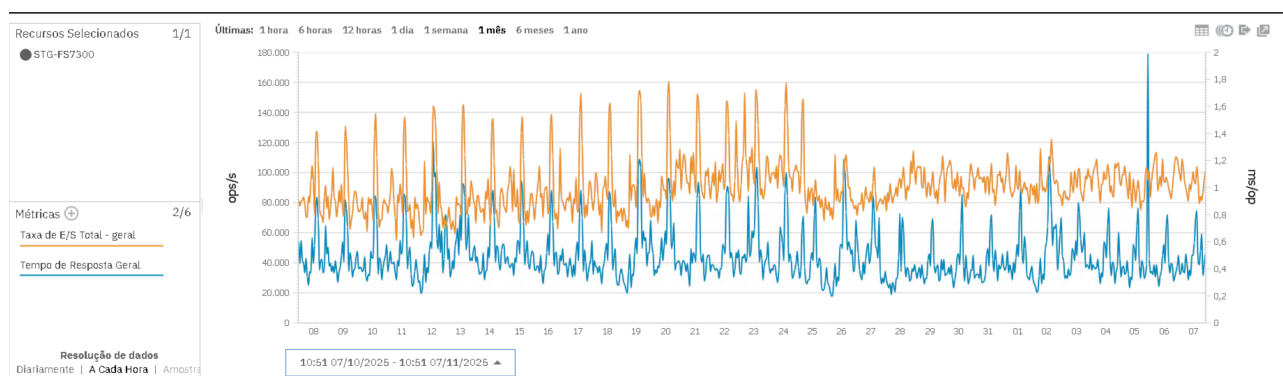
5.1.3. Deverá suportar uma taxa sustentada de 180.000 (cento e oitenta mil) IOPS (operações de I/O por segundo), de acesso exclusivamente randômico, sendo 70% leitura e 30% de escrita, sem a utilização de cache read hit, com as funcionalidades de criptografia, compressão e deduplicação

habilitadas, bem como replicação metro-cluster ativa-ativa habilitada para toda a capacidade armazenada, com blocos de tamanho mínimo de 48KiB, operando com 50% de suas capacidades totais de processamento e ocupação de módulos de armazenamento, com tempo de resposta para gravação de no máximo 1ms e tempo de resposta para leitura de no máximo 4ms;

6.1.3. Deverá suportar uma taxa sustentada de 120.000 (cento e vinte mil) IOPS (operações de I/O por segundo), de acesso exclusivamente randômico, sendo 50% leitura e 50% de escrita, sem a utilização de cache read hit, com as funcionalidades de compressão e deduplicação habilitadas, com blocos de tamanho mínimo de 48KB, operando com 50% de suas capacidades totais de processamento e ocupação de módulos de armazenamento, com tempo de resposta para gravação de no máximo 1ms e tempo de resposta para leitura de no máximo 4ms;

Justificativa itens 5.1.3 e 6.1.3:

Atualmente o Storage faz em média entre 80k e 100k IOPS com picos de 160k, notando que o Storage não faz deduplicação e nem criptografia. Considerando um aumento de utilização de 50% para os próximos anos, justifica-se o desempenho solicitado.



ESCALABILIDADE

5.2.1. Cada equipamento ofertado na solução de armazenamento deverá permitir a expansão de sua capacidade efetiva para no mínimo 1,5 PiB, mantendo o desempenho descrito neste termo de referência, sem que exista a necessidade de reconfiguração de parâmetros de endereçamento lógico ou de volumes apresentados aos hosts;

6.2.1. Cada equipamento ofertado na solução de armazenamento deverá permitir a expansão de sua capacidade efetiva para no mínimo 8 PiB (oito pebibytes), mantendo o desempenho descrito neste termo de referência, sem que exista a necessidade de reconfiguração de parâmetros de endereçamento lógico ou de volumes apresentados aos hosts.

Justificativa itens 5.2.1 e 6.2.1:

Levando em consideração o crescimento do ambiente em no mínimo 50% em pelo menos 5 anos, justifica-se a capacidade de escalabilidade solicitada.

CONECTIVIDADE FRONT-END

5.4.3. Possuir, no mínimo, 6 (seis) interfaces de "front-end" FC SAN de 32/64 Gbps, por controladora, com conectores para fibra ótica multimodo do tipo LC para fins de conectividade de hosts contidos no fabric FC SAN.

6.4.3. Possuir, no mínimo, 6 (seis) interfaces de "front-end" FC SAN de 32/64 Gbps, por controladora, com conectores para fibra ótica multimodo do tipo LC para fins de conectividade de hosts contidos no fabric FC SAN.

Justificativa itens 5.4.3 e 6.4.3:

Este item justifica-se visando a evolução tecnologica (refresh da rede SAN da PROCempa para 64 Gbps para o próximo ano) para os próximos anos, além de melhorar o desempenho do tráfego de dados entre servidores e solução de armazenamento.

FUNCIONALIDADES

5.8.2. A solução de armazenamento deverá prover de forma nativa a funcionalidade de criptografia, deduplicação e compressão de dados inline;

5.8.3. A solução de armazenamento de dados deverá suportar de forma simultânea inline, em 100% do tempo de operação, as funcionalidades de criptografia, deduplicação e compressão de dados.

6.8.2. A solução de armazenamento deverá prover de forma nativa a funcionalidade de deduplicação e compressão de dados inline;

6.8.3. A solução de armazenamento de dados deverá prover de forma nativa a funcionalidade de compressão e deduplicação de dados de forma inline;

Justificativa itens 5.8.2, 5.8.2, 6.8.2 e 6.8.3:

Estes itens abordam questões relacionadas a segurança de dados (criptografia) e melhor aproveitamento da área de armazenamento solicitada através das tecnologias de deduplicação e compressão de dados.

5.8.7. A solução de armazenamento deverá suportar no mínimo 350000 (trezentos e cinquenta mil)0 snapshots por equipamento.

6.8.8. A solução de armazenamento deverá suportar no mínimo **350000** (trezentos e cinquenta mil)0 snapshots por equipamento.

Justificativa itens 5.8.7 e 6.8.8:

O cálculo para o número de snapshots solicitado foi realizado da seguinte forma:

-----Storage Classe 1-----

Total de LUNs atualmente (nLuns): 150

Tempo de retenção (tRet): 5 dias

RPO (tRPO): 5 minutos

$N_{snaps} = nLuns \times (1440(1dia \text{ em minutos}) / tRPO) \times tRet$

$N_{snaps} = 150 \times 288 \times 5$

$N_{snaps} = 216.000$

Percentual de crescimento: 50%

Total de snapshots: 324.000

-----Storage Classe 2-----

Total de LUNs atualmente (nLuns): 150

Tempo de retenção (tRet): 30 dias

RPO (tRPO): 1 hora

$N_{snaps} = nLuns \times (1440(1dia \text{ em minutos}) / tRPO) \times tRet$

$N_{snaps} = 150 \times 24 \times 30$

$N_{snaps} = 108.000$

Percentual de crescimento: 30%

Total de snapshots: 140.400

5.8.8. A solução de armazenamento deverá suportar snapshots com consistência de aplicativos para bancos de dados Oracle, Microsoft Sql Server e PostgreSQL.

6.8.9. A solução de armazenamento deverá suportar snapshots com consistência de aplicativos para bancos de dados Oracle, Microsoft Sql Server e Postgress.

Justificativa itens 5.8.8 e 6.8.9:

Esta exigência visa assegurar integridade transacional e consistência lógica dos bancos de dados durante a criação de snapshots, evitando corrupção ou inconsistência em cópias de segurança. O suporte nativo a snapshots consistentes com os principais SGBDs garante recuperação confiável e rápida em cenários de falha ou restauração planejada, reduzindo o tempo de indisponibilidade dos serviços.

5.8.22. A solução de armazenamento de dados deverá suportar a replicação entre dois sites(metro cluster), de forma síncrona, no formato ativo-ativo, para leitura e escrita simultânea nos dois sites, permitindo desta forma que os volumes estejam acessíveis para os hosts sob um único endereço lógico, independente de site onde estiver o referido host. Esta funcionalidade deverá ser nativa dos equipamentos ofertados, não sendo aceito o uso de equipamentos externos para tal.

6.8.23. A solução de armazenamento de dados deverá suportar a replicação entre dois sites(metro cluster), de forma síncrona, no formato ativo-ativo, para leitura e escrita simultânea nos dois sites, permitindo desta forma que os volumes estejam acessíveis para os hosts sob um único endereço lógico, independente de site onde estiver o referido host. Esta funcionalidade deverá ser nativa dos equipamentos ofertados, não sendo aceito o uso de equipamentos externos para tal.

Justificativa itens 5.8.22 e 6.8.23:

A replicação síncrona em formato ativo-ativo garante alta disponibilidade e continuidade operacional entre dois datacenters. Em caso de falha em um dos sites, o outro continua operando de forma imediata e transparente para as aplicações, sem necessidade de intervenção manual. Essa arquitetura elimina pontos únicos de falha, reduz o RPO e RTO praticamente a zero.

5.8.25. A solução de armazenamento, além da replicação metro cluster, ativo-ativo, deverá suportar de forma nativa replicação assíncrona ou síncrona para um terceiro site (datacenter físico ou data center em nuvem). Caso seja necessário licenciamento para este requisito, o mesmo deverá ser contemplado para a volumetria máxima suportada pelo equipamento ofertado, de acordo com o exigido neste edital.

***6.8.26.** A solução de armazenamento, além da replicação metro cluster, ativo-ativo, deverá suportar de forma nativa replicação assíncrona ou síncrona para um terceiro site (datacenter físico ou data center em nuvem). Caso seja necessário licenciamento para este requisito, o mesmo deverá ser contemplado para a volumetria máxima suportada pelo equipamento ofertado, de acordo com o exigido neste edital.

Justificativa itens 5.8.25 e 6.8.26*:

A replicação para um terceiro site amplia a resiliência e a proteção contra desastres de larga escala, permitindo manter cópias de dados fora da localidade principal. Essa topologia de replicação 3-site (ativa-ativa-assíncrona) é essencial para políticas de Disaster Recovery (DR) e conformidade com boas práticas de continuidade de serviços críticos.

***Item 6.8.26 faltou quebra de linha. Item 5.8.26 ilustra como deveria estar.**

5.8.26. A solução de armazenamento deverá fornecer funcionalidade de mitigação de ataques de criptografia de dados (RANSOWARE) ou deleção intencional de dados, possibilitando a contratante a restauração de forma rápida dos dados criptografados ou deletados, observando um RPO (Recover Point Objective) de até 5 (cinco) minutos e RTO (Recover time objective) de até 30(trinta) minutos, através de uma das alternativas abaixo:

5.8.27. Isolamento de cópias protegidas por meio lógico, através de imutabilidade de snapshots, que impeça a criptografia ou deleção de dados e acordo com política de retenção pré-definida;

5.8.28. Isolamento de cópias protegidas por meio físico, através armazenamento de dados em nuvem assíncrono ou “air gap” local.

***Continuação do item 6.8.26 ...**A solução de armazenamento deverá fornecer funcionalidade de mitigação de ataques de criptografia de dados (RANSOWARE) ou deleção intencional de dados, possibilitando a contratante a restauração de forma rápida dos dados criptografados ou deletados, observando um RPO (Recover Point Objective) de até 5 (cinco) minutos e RTO (Recover time objective) de até 30(trinta) minutos, através de uma das alternativas abaixo:

6.8.27. Isolamento de cópias protegidas por meio lógico, através de imutabilidade de snapshots, que impeça a criptografia ou deleção de dados e acordo com política de retenção pré-definida;

6.8.28. Isolamento de cópias protegidas por meio físico, através armazenamento de dados em nuvem assíncrono ou “air gap” local.

Justificativa itens 5.8.26, 5.8.27, 5.8.28, 6.8.26*, 6.8.27 e 6.8.28:

Os ataques de ransomware e deleção intencional de dados representam uma das principais ameaças à operação de TI. A exigência dessas funcionalidades visa garantir proteção e recuperação rápida de dados críticos, permitindo o retorno operacional em até 30 minutos e perda máxima de 5 minutos de dados (RPO). As abordagens de imutabilidade de snapshots e/ou isolamento físico (air gap) proporcionam camadas adicionais de defesa, garantindo que cópias protegidas não possam ser alteradas nem mesmo por administradores com privilégios elevados.

5.8.31. Caso seja utilizado o mecanismo de isolamento de cópias protegidas logicamente (snapshots), este deve assegurar que nem mesmo usuários com privilégios de administrador/root seja capaz de desativá-lo ou excluir os dados.

5.8.32. O período de retenção de snapshots, após aplicado a determinado conjunto de cópias (snapshots) somente poderá ter sua retenção alterada (de forma a diminuir o tempo de retenção) através do fabricante do equipamento, mediante abertura de chamado e validação de identidade e veracidade da contratante, sendo necessário, no mínimo, duas pessoas atribuídas para este fim, pelo contratante.

6.8.31. Caso seja utilizado o mecanismo de isolamento de cópias protegidas logicamente (snapshots), este deve assegurar que nem mesmo usuários com privilégios de administrador/root seja capaz de desativá-lo ou excluir os dados.

6.8.32. O período de retenção de snapshots, após aplicado a determinado conjunto de cópias (snapshots) somente poderá ter sua retenção alterada (de forma a diminuir o tempo de retenção) através do fabricante do equipamento, mediante abertura de chamado e validação de identidade e veracidade da contratante, sendo necessário, no mínimo, duas pessoas atribuídas para este fim, pelo contratante.

Justificativa itens 5.8.31, 5.8.32, 6.8.31 e 6.8.32:

Esses requisitos complementam a política de proteção imutável de dados, impedindo que cópias protegidas sejam excluídas ou alteradas indevidamente, inclusive por administradores.

A exigência de dupla autenticação e validação junto ao fabricante garante rastreabilidade e segurança em processos de alteração de políticas de retenção, mitigando riscos internos e reforçando as práticas de segurança corporativa e compliance.

5.8.34. Deve possuir suporte nativo a docker/kubernetes, Container Storage Integration (CSI) Plugins ou equivalente.

5.8.35. O sistema de armazenamento deverá possuir suporte aos protocolos SMB/CIFs, NFSv3, NFSv4 ou NFSv4.1.

6.8.34. Deve possuir suporte nativo a docker/kubernetes, Container Storage Integration (CSI) Plugins ou equivalente.

6.8.35. O sistema de armazenamento deverá possuir suporte aos protocolos SMB/CIFs, NFSv3, NFSv4 ou NFSv4.1 e S3.

Justificativa itens 5.8.34, 5.8.35, 6.8.34 e 6.8.35:

Essas funcionalidades são fundamentais para garantir integração com ambientes modernos de virtualização e containers, permitindo a orquestração de volumes de forma dinâmica via Kubernetes ou Docker. O suporte simultâneo aos protocolos SMB, NFS e S3 amplia a flexibilidade de acesso e interoperabilidade, viabilizando a utilização da mesma infraestrutura de armazenamento para múltiplos tipos de aplicações — desde workloads tradicionais até serviços nativos em nuvem.

NAS SCALE-OUT

8.1.2. O sistema de armazenamento de arquivos NAS deverá ser composto por no mínimo, 4 (quatro) nodos;

Justificativa item 8.1.2:

A exigência mínima de quatro nós visa assegurar distribuição de carga, paralelismo e resiliência do sistema NAS. Essa configuração permite balanceamento eficiente do tráfego, alta disponibilidade e continuidade operacional mesmo em caso de falha de um dos nós, mantendo o desempenho e a integridade dos dados.

8.1.4. Ficam vedadas soluções de armazenamento que dependam de gateways ou que exijam a instalação de agentes, clientes ou qualquer outro software adicional nos hosts para viabilizar o acesso aos protocolos especificados.

Justificativa item 8.1.4:

O objetivo deste requisito é garantir simplicidade de integração e interoperabilidade nativa com os protocolos de rede padrão (NFS, SMB/CIFS), eliminando dependências de software proprietário ou intermediário. Essa abordagem reduz complexidade operacional, aumenta a estabilidade do ambiente e assegura independência tecnológica em longo prazo.

VOLUMETRIA

8.3.1. A solução deverá disponibilizar, no mínimo, 800 TB (oitocentos terabytes) de capacidade efetiva, prontos para uso, após a aplicação das configurações de proteção de dados (como RAID ou equivalente), bem como os ganhos obtidos por técnicas de deduplicação e compressão de dados.

Justificativa item 8.3.1:

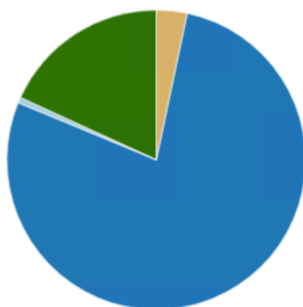
O dimensionamento de 800 TB efetivos considera o volume atual de armazenamento de arquivos corporativos, o crescimento anual histórico e as necessidades de projetos estratégicos previstos. A aplicação de compressão e deduplicação otimiza a eficiência do uso do espaço, garantindo longevidade e margem para expansão sem comprometer desempenho.

Cluster: **isilon-nas-sa**

Current Estimated Usable Capacity

Legend:

- Total Capacity
- Unprovisioned Capacity
- Reserved for Virtual Hot Spares
- User Data including Protection
- Snapshots Usage
- Estimated Additional Protection Overhead
- Estimated Usable Capacity



Total Capacity **528 TiB**

– **0 B** Unprovisioned Capacity

Provisioned Capacity **528 TiB**

– **17.5 TiB** Reserved for Virtual Hot Spares

Writeable Capacity **510 TiB**

– **411 TiB** User Data including Protection

– **3.19 TiB** Snapshots Usage

Remaining Capacity **95.9 TiB**

– **0*** Estimated Additional Protection Overhead

Overhead estimation based on FSA report:

Jan 17 2025, 12:43 pm (BST)

Estimated **95.9 TiB** of Usable Capacity Remaining

ESCALABILIDADE

8.4.1. Deverá suportar a expansão para no mínimo para 3Pb efetivos;

8.4.2. Deverá suportar a expansão de no mínimo 16 nodos ao cluster;

Justificativa itens 8.4.1 e 8.4.2:

A possibilidade de expansão para 3 PiB e até 16 nodos assegura que o sistema NAS poderá acompanhar o crescimento progressivo da demanda corporativa por armazenamento, tanto em capacidade quanto em desempenho. Essa escalabilidade horizontal (scale-out) permite que novos nós sejam adicionados sem interrupção do serviço, preservando o investimento inicial e garantindo longevidade à solução, com crescimento linear de performance e capacidade.

8.4.3. O sistema de armazenamento de arquivos scale-out NAS deverá suportar no mínimo 20.000 (vinte mil) compartilhamentos de rede ou pontos de montagem, utilizando o protocolo CIFS;

8.4.4. O sistema de armazenamento de arquivos scale-out NAS deverá suportar no mínimo 20.000 (vinte mil) compartilhamentos de rede ou pontos de montagem, utilizando o protocolo NFS;

8.4.5. O sistema de armazenamento de arquivos scale-out NAS deverá suportar no mínimo de 100 (cem) servidores cifs;

8.4.6. O sistema de armazenamento de arquivos scale-out NAS deverá suportar o mínimo de 100 (cem) sistemas de arquivos;

8.4.7. O sistema de armazenamento de arquivos scale-out NAS deverá suportar o número mínimo de 30.000 (trinta mil) cotas de diretórios;

8.4.8. O sistema de armazenamento de arquivos scale-out NAS deverá suportar o número mínimo de 30.000 (trinta mil) arquivos abertos;

8.4.9. O sistema de armazenamento de arquivos scale-out NAS deverá suportar número mínimo de 12.000 (doze mil) conexões CIFS ativas;

8.4.10. O sistema de armazenamento de arquivos deverá suportar, no mínimo, 1 (um) bilhão de arquivos;

8.4.11. O sistema de armazenamento de arquivos deverá suportar, no mínimo, 200 (duzentos) milhões de diretórios;

8.4.12. O sistema de armazenamento de arquivos deverá suportar, no mínimo, arquivos com tamanho de até 16Tb;

8.4.13. O sistema de armazenamento de arquivos scale-out NAS deverá sustentar o mínimo de 5GB/s de throughput de rede;

8.4.14. O sistema de armazenamento de arquivos scale-out NAS deverá sustentar o mínimo de 5 Gbps de throughput no sistema de arquivos;

Justificativa itens 8.4.3 até 8.4.14:

Atualmente temos a seguinte utilização do NAS:

- **20 Mil usuários**
- **15 Filesystem**
- **3000 Shares**
- **3500 Quotas**
- **50 Milhões de diretórios**
- **350 Milhões de Arquivos**

Essas especificações visam garantir que o ambiente NAS corporativo suporte com folga o volume de acessos simultâneos, a grande quantidade de arquivos e diretórios e as demandas de desempenho e throughput exigidas por aplicações críticas e múltiplos usuários concorrentes.

Os valores solicitados refletem o perfil atual de utilização da PROCempa, acrescido de uma margem de crescimento projetada para os próximos anos, assegurando alta escalabilidade e desempenho sustentado mesmo com o aumento do número de usuários, volumes e conexões ativas.

FUNCIONALIDADES

8.7.1. O sistema de armazenamento de arquivos scale-out NAS deverá suportar o gerenciamento de cotas a serem aplicadas no sistema de arquivos distribuído, por usuários, grupos de usuários, diretórios e por sistemas de arquivos;

Justificativa item 8.7.1:

O gerenciamento de cotas por usuário, grupo e diretório é essencial para controle e governança do espaço de armazenamento, evitando uso indevido de recursos e garantindo distribuição justa entre os diversos departamentos e sistemas corporativos. Essa funcionalidade permite também otimizar a gestão de capacidade e prever expansões futuras de forma planejada.

8.7.2. O sistema de armazenamento de arquivos scale-out NAS deverá prover de forma nativa a funcionalidade de deduplicação e compressão de dados inline;

Justificativa item 8.7.2:

A deduplicação e compressão inline proporcionam ganhos significativos de eficiência no uso do espaço físico, reduzindo custos de armazenamento sem comprometer o desempenho. A execução dessas funções de forma nativa e em tempo real assegura que os ganhos de otimização sejam aplicados continuamente, contribuindo para a sustentabilidade e a performance do ambiente.

8.7.3. O sistema de armazenamento de arquivos scale-out NAS deverá permitir a gravação de arquivos no modo WORM (Write Once Read Many);

8.7.5. O sistema de armazenamento de arquivos "Scale-out" NAS deverá suportar a utilização de cloud storage (nuvem pública, privada ou híbrida) como um tier de dados para movimentação de dados de forma automática, baseada em políticas de armazenamento;

Justificativa itens 8.7.3 e 8.7.5:

A funcionalidade WORM (Write Once Read Many) é necessária para atendimento a requisitos de conformidade e integridade de dados, especialmente em sistemas que demandam proteção contra alteração ou exclusão de informações, como registros contábeis e jurídicos. Já a integração com cloud storage como tier de dados permite movimentar automaticamente informações menos acessadas para camadas de armazenamento mais econômicas, otimizando custos e aumentando a eficiência operacional da infraestrutura.

8.7.6. O sistema de armazenamento de arquivos deverá suportar a replicação entre dois sites(metrocluster), de forma síncrona e assíncrona, no formato ativo-ativo, para leitura e escrita simultânea nos dois sites, permitindo desta forma que arquivos e objetos estejam acessíveis para clientes e aplicações sob um único endereço lógico. Esta funcionalidade deverá ser nativa dos equipamentos ofertados, não sendo aceito o uso de equipamentos externos para tal.

Justificativa item 8.7.6:

A replicação ativo-ativo síncrona e assíncrona entre sites garante continuidade de serviço e proteção contra falhas de datacenter, mantendo a integridade e a disponibilidade dos dados em múltiplas localidades. Essa funcionalidade é fundamental para alta disponibilidade (HA) e recuperação de desastres (DR), permitindo que o ambiente permaneça acessível mesmo em cenários de falha total de um dos sites.

8.7.10. A funcionalidade de snapshot deverá proporcionar o agendamento automático de snapshots com proteção para sistema de arquivos e objetos ;

8.7.11. A solução de armazenamento deverá suportar no mínimo 150 (cento e cinquenta) mil snapshots;

Justificativa itens 8.7.10 e 8.7.11:

O cálculo para o número de snapshots solicitado foi realizado da seguinte forma:

-----Storage NAS-----

Total de Filesystem atualmente (nFileS): 100

Tempo de retenção (tRet): 30 dias

RPO (tRPO): 30 minutos

$N_{snaps} = nFileS \times (1440(1dia \text{ em minutos}) / tRPO) \times tRet$

$N_{snaps} = 100 \times 48 \times 30$

$N_{snaps} = 144.000$

O suporte a snapshots agendados e automatizados é essencial para a proteção contínua de dados e rápida recuperação de versões anteriores em caso de exclusão acidental ou corrupção. O número mínimo de 150 mil snapshots garante ampla capacidade para múltiplas políticas de retenção e pontos de restauração distribuídos entre diferentes volumes, sistemas de arquivos e períodos de retenção, cobrindo cenários de backup local e proteção lógica.

8.7.12. A solução de armazenamento deverá fornecer funcionalidade de mitigação de ataques de criptografia de dados (RANSOWARE) ou deleção intencional de dados, possibilitando a contratante a restauração de forma rápida dos dados criptografados ou deletados, observando um RPO (Recover Point Objective) de até 15 (quinze) minutos e RTO (Recover time objective) de até 30(trinta) minutos, através de uma das alternativas abaixo:

8.7.12.1. Isolamento de cópias protegidas por meio lógico, através de imutabilidade de snapshots, que impeça a criptografia ou deleção de dados e acordo com política de retenção pré-definida;
8.7.12.2. Isolamento de cópias protegidas por meio físico, através armazenamento de dados em nuvem assíncrono ou “airgap” local;
8.7.15. O período de retenção de snapshots, após aplicado a determinado conjunto de cópias (snapshots) somente poderá ter sua retenção alterada através do fabricante do equipamento, mediante abertura de chamado e validação de identidade e veracidade da contratante, sendo necessário, no mínimo, duas pessoas atribuídas para este fim, pelo contratante.

Justificativa itens 8.7.12, 8.7.12.1, 8.7.12.2 e 8.7.15:

Os ataques de ransomware e deleção intencional de dados representam uma das principais ameaças à operação de TI. A exigência dessas funcionalidades visa garantir proteção e recuperação rápida de dados críticos, permitindo o retorno operacional em até 30 minutos e perda máxima de 5 minutos de dados (RPO). As abordagens de imutabilidade de snapshots e/ou isolamento físico (air gap) proporcionam camadas adicionais de defesa, garantindo que cópias protegidas não possam ser alteradas nem mesmo por administradores com privilégios elevados.

ATUALIZAÇÃO TECNOLÓGICA

9.1. Enquanto o contrato de garantia e suporte estiver ativo, a atualização tecnológica do sistema deverá ocorrer, no máximo, a cada 6 anos, nas seguintes condições:
9.2. Substituição das controladoras de I/O da solução de armazenamento Flash pela versão mais recente disponível, sem custos para a CONTRATANTE.
9.3. Caso o modelo ofertado tenha sido descontinuado ou entrado em período de end-of-sale (o que ocorrer primeiro), o mesmo será substituído por um modelo equivalente e mais recente, com capacidade mínima igual à original, sem custos para a CONTRATANTE.
9.4. A atualização tecnológica, incluindo os serviços necessários, deve estar incluída na oferta, sem quaisquer custos adicionais para a CONTRATANTE.
9.5. A substituição das controladoras deve ser feita sem migração de dados, mantendo os identificadores de volume e sem necessidade de reconfiguração dos servidores conectados.
9.6. A substituição deverá ocorrer sem interrupções nos serviços de armazenamento de dados em produção e sem redução no desempenho ou aumento na latência da solução.

Justificativa itens 9.1 ao 9.6:

Podemos citar como exemplo o storage **IBM FlashSystem 5030**, que atingirá seu **End of Support (EOS)** em **31/12/2026**. Após essa data, não será mais possível realizar a renovação de suporte junto ao fabricante, o que implica na **descontinuidade de atualizações, correções de segurança e suporte técnico**. Consequentemente, todo o investimento feito nesse equipamento se tornará obsoleto, exigindo a **aquisição de um novo storage** para continuidade dos serviços.

Ao optar por uma solução que ofereça **atualização tecnológica** garantimos que o investimento realizado **permaneça válido ao longo do tempo**, eliminando a necessidade de substituição completa do equipamento ao final do ciclo de vida. Esse tipo de solução assegura que, ao término do período de suporte, a contratada seja **obrigada a realizar a atualização do hardware ou renovar a garantia**, mantendo o ambiente sempre atualizado tecnologicamente e **prolongando o retorno sobre o investimento inicial**.

Além do aspecto financeiro, essa abordagem contribui para:

- **Redução de desperdício de recursos** (ambientais e orçamentários), evitando o descarte de equipamentos em bom estado físico;

- **Continuidade operacional e mitigação de riscos** associados a falhas de hardware obsoleto;
- **Previsibilidade orçamentária**, uma vez que elimina a necessidade de novos processos de aquisição a cada ciclo de depreciação tecnológica.

Dessa forma, a aquisição de um storage com essa característica representa uma estratégia de investimento sustentável e de longo prazo, garantindo a modernização contínua da infraestrutura sem comprometer a disponibilidade dos serviços.

ERRATA

Texto no TR:

8.1.19. Ocorrida a eventual substituição de componentes, conforme item 4.1.1.17 permanecerão em vigor todas condições contratadas pelo período original contratado;

Texto corrigido:

8.1.19. Ocorrida a eventual substituição de componentes, conforme item **8.1.17** permanecerão em vigor todas condições contratadas pelo período original contratado;

ERRATA2

Texto no TR:

6.8.8. A solução de armazenamento deverá suportar no mínimo 350000 (trezentos e cinquenta mil)0 snapshots por equipamento.

Texto corrigido:

6.8.8. A solução de armazenamento deverá suportar no mínimo **150000 (cento e cinquenta mil)**0 snapshots por equipamento.