

Estudo Técnico Preliminar 48/2024

1. Informações Básicas

Número do processo: 08006.000647/2023-98

2. Descrição da necessidade

2.1. Introdução

2.1.1. Conforme previsto no artigo 11 da Instrução Normativa SGD/ME Nº 94, de 23 de Dezembro de 2022, a elaboração dos Estudos Técnicos Preliminares da Contratação serve essencialmente para definição e especificação das necessidades de negócio e tecnológicas, e dos requisitos necessários e suficientes à escolha da solução de TIC, contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição. A análise comparativa de soluções, deve considerar, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

2.1.2. É na elaboração dos Estudos Técnicos Preliminares da Contratação que diversos aspectos devem ser levantados com maior profundidade para que os gestores se certifiquem de que através de uma necessidade da área de negócio, claramente definida, que há condições de atendê-la, tendo como premissa que os riscos de atendê-la são gerenciáveis e os resultados pretendidos com a contratação valem o preço estimado inicialmente, além de embasar a elaboração do Termo de Referência, que somente é elaborado se a contratação for considerada viável.

2.1.3. O propósito desta análise é avaliar a possibilidade técnica e financeira de adquirir uma nova solução de armazenamento de dados que substitua, atualize tecnologicamente e expanda a capacidade de armazenamento dos atuais equipamentos, bem como uma nova solução de backup, que substitua e aprimore a solução de backup de dados existente, além de modernizar a infraestrutura dos data centers (centros de processamento de dados) do Ministério da Justiça e Segurança Pública. Isso poderá envolver a atualização dos equipamentos e programas, resultando em um melhor desempenho, confiabilidade e segurança da informação para os sistemas, aplicativos, bancos de dados e os dados em si que dependem dessa infraestrutura para atender às demandas do Ministério.

2.1.4. O projeto de modernização da infraestrutura de data centers do Ministério da Justiça e Segurança Pública visa a criação de uma infraestrutura hiperconvergência e de nuvem privada, sendo formado por segmentos:

a) Infraestrutura de processamento de dados, armazenamento de blocos SAN/vSAN e licenciamento de virtualização, bem como serviços auxiliares. Esta contratação está sendo tratada através do processo SEI 08006.000626/2023-72;

b) Infraestrutura de armazenamento de dados para arquivos (storage NAS) e objetos (storage de objetos) e de backup de dados, bem como serviços auxiliares. Esta contratação está sendo tratada no presente processo de contratação (SEI 08006.000647/2023-98).

2.1.5. A presente contratação integra o segmento “b” do projeto e possui dois escopos. O primeiro escopo tem como objetivo a substituição da solução de armazenamento de dados existente, ampliação da capacidade de armazenamento de dados, melhoria de performance, modernização tecnológica e de arquitetura para suprir a necessidade atual e futura dos sistemas corporativos hospedados nos ambientes de data centers do MJSP.

2.1.6. Atualmente a capacidade de armazenamento disponível para suprir os sistemas do Ministério encontram-se com utilização acima de 80%, considerando os *storages midrange* e NAS (*Network Attached Storage*), sendo necessária sua expansão para que não ocorra a interrupção dos serviços de TIC providos pela Subsecretaria de Tecnologia da Informação e Comunicação - STI/SE/MJSP.

2.1.7. A atual arquitetura de armazenamento existente não implementa as melhores práticas de mercado, sendo necessária sua modernização de arquitetura, para adequação ao modelo de camadas (*tiers*) de fato, segmentada em diferentes níveis (bloco, arquivos e objetos), de forma a alocar a solução mais adequada, especializada e com alta performance ao armazenamento em rede do projeto, de acordo com os requisitos das aplicações corporativas

ou necessidades dos usuários do órgão. Visa-se também melhorar a utilização da capacidade de armazenamento, de acordo com sua finalidade, com a utilização de *storages* NAS com integração nativa com *storages* de objetos para fins de *tiering* (transbordo).

2.1.8. Ainda, a modernização tecnológica da solução de armazenamento é fundamental, com tecnologias que agregam alta performance e durabilidade, além de implementar na nova infraestrutura de armazenamento, suporte a novos protocolos e recursos de *analytics* e inteligência artificial, buscando aperfeiçoar a gestão e governança de dados do Ministério para projetos em andamento e futuros. Outro requisito basilar desse escopo é implementar os requisitos de segurança da informação e salvaguarda dos dados armazenados, com a utilização de recursos e protocolos que forneçam camadas de proteção, inclusive contra ação de malwares e/ou ransomwares.

2.1.9. Migrar os dados dos *storages midrange* e NAS atuais para a nova solução devido a necessidade de atualização tecnológica, expansão da capacidade e desempenho do parque. Os equipamentos DELL EMC VNX 7500, VNX 5300 e NetApp FAS8080 instalados no parque encontram-se em *end-of-life* e *end-of-support*.

2.1.10. Em complemento ao segmento “b” do projeto, o segundo escopo tem como objetivo a substituição da solução de backup existente, bem como sua modernização em termos de arquitetura, estratégia aplicada, tecnologia, capacidade de retenção de dados e segurança, para suprir a necessidade atual e futura de salvaguarda dos dados corporativos, bem como atendimento à política de backup do órgão.

2.1.11. A atual solução de backup – *Veritas Netbackup* encontra-se sem atualização e sem suporte desde 2022. Além disso, atualmente os *appliances* de backup já estão com capacidade de armazenamento disponível insuficiente e a utilização de mídias de longa retenção, como fitas LTO, apresentam tecnologia obsoleta e não performática, considerando escrita e leitura de dados, bem como o tempo necessário à restauração de backups. Essa situação compromete a eficiência da solução, aumenta o tempo de recuperação de dados, diminui a confiabilidade das operações de *backup* e *restore*, além de sobrecarregar a atuação das equipes técnicas da STI/SE /MJSP e de suporte de infraestrutura de TIC nas atividades nestas operações. É fundamental que o Ministério tenha uma solução de backup que suporte o volume de dados gerados pelo usuários e sistemas corporativos, assegurando a continuidade das atividades e a integridade das informações.

2.1.12. Ressalta-se a importância de migrar a estratégia de backup atual, inadequada às atribuições do órgão e importância dos dados armazenados nos data centers, devido aos recursos e tecnologias obsoletos, para a implementação de uma nova estratégia, tal qual a estratégia 3-2-1, de forma a manter o ambiente seguro do MJSP em praticamente qualquer cenário de falha. Neste contexto, almeja-se ter ao menos 3 cópias dos dados, armazenar 2 delas em mídias físicas distintas e outra fora do ambiente produtivo, replicado no data center secundário ou em um serviço de nuvem.

2.1.13. Outro ponto crucial é a necessidade de uma solução que atenda a requisitos de segurança avançados. Com o aumento das ameaças cibernéticas, é essencial que o Ministério da Justiça e Segurança Pública esteja preparado para proteger seus dados contra criptografia indesejada ou ataques maliciosos. A solução de backup proposta deve possuir recursos robustos de segurança da informação, como criptografia de dados em repouso e em trânsito, autenticação forte, imutabilidade do backup e mecanismos de proteção de ameaças.

2.1.14. Além dos equipamentos e soluções de software, integram as soluções a serem contratadas:

- a) infraestrutura necessária, tais como servidores, *switches*, cabos, conectores de rede, entre outros, para interligá-los à rede LAN dos data centers, bem como às redes de gerenciamento da STI/SE/MJSP;
- b) licenças dos softwares necessárias para as soluções de armazenamento e backup, com o respectivo suporte e garantia integral de 60 meses;
- c) o serviço de instalação e implantação de todos os elementos das soluções;
- d) serviços de operação assistida, para os devidos fins de monitoramento, verificação de funcionamento das soluções após implantação, incluindo replicação dos dados, bem como repasse de conhecimento;
- e) serviço de treinamento teórico/prático para capacitação da equipe técnica da STI/SE/MJSP;
- f) serviços especializados sob demanda para suporte ou atualização das soluções sob demanda.

2.1.15. É fundamental esclarecer que o tipo de armazenamento em foco neste processo no escopo de armazenamento de dados se refere à soluções NAS (*Network Attached Storage*) e Storage de Objetos (*Object Storage*). Esta abordagem não deve ser confundida com o dimensionamento de armazenamento para os servidores virtualizados e bancos de dados planejados no processo 08006.000626/2023-72. São, portanto, dois processos de

contratações diferentes, destinados a objetivos distintos, porém complementares para a conclusão do projeto de modernização da infraestrutura de data centers do MJSP.

2.2. Motivação/Justificativa

2.2.1. Visão geral do Ministério da Justiça e Segurança Pública e seus objetivos estratégicos:

2.2.1.1. O Ministério da Justiça e Segurança Pública (MJSP), órgão da Administração Pública Federal, tem, dentre outras, as competências para atuar no “*combate ao tráfico de drogas e crimes conexos, inclusive por meio da recuperação de ativos que financiem ou sejam resultado dessas atividades criminosas*”, na “*prevenção e combate à corrupção, à lavagem de dinheiro e ao financiamento do terrorismo*”, na “*coordenação de ações para combate a infrações penais em geral, com ênfase em corrupção, crime organizado e crimes violentos*”, na “*coordenação e promoção da integração da segurança pública no território nacional, em cooperação com os entes federados*”, na “*promoção da integração e da cooperação entre os órgãos federais, estaduais, distritais e municipais e articulação com os órgãos e as entidades de coordenação e supervisão das atividades de segurança pública*” e, por fim, no “*desenvolvimento de estratégia comum baseada em modelos de gestão e de tecnologia que permitam a integração e a interoperabilidade dos sistemas de tecnologia da informação dos entes federativos*”.

2.2.1.2. Atualmente o Ministério, é composto de várias unidades em sua estrutura:

a) Órgãos de assistência direta e imediata ao Ministro: Gabinete do Ministro, Assessorias Especiais, Corregedoria-Geral, Ouvidoria-Geral, Secretaria Executiva e Consultoria Jurídica;

b) Órgãos específicos singulares: Secretaria Nacional de Justiça - SENAJUS, Secretaria Nacional do Consumidor - SENACON, Secretaria Nacional de Políticas sobre Drogas e Gestão de Ativos - SENAD, Secretaria Nacional de Segurança Pública - SENASP, Secretaria Nacional de Políticas Penais - SENAPPEN, Secretaria Nacional de Assuntos Legislativos - SAL, Secretaria de Acesso à Justiça - SAJU, Secretaria de Direitos Digitais - SEDIGI, Polícia Federal - PF e Polícia Rodoviária Federal - PRF;

c) Órgãos colegiados: Conselho Federal Gestor do Fundo de Defesa dos Direitos Difusos - CFDD, Conselho Nacional de Combate à Pirataria e Delitos contra a Propriedade Intelectual - CNPCP, Conselho Nacional de Políticas sobre Drogas - CONAD, Conselho Nacional de Política Criminal e Penitenciária - CNCP, Conselho Nacional de Segurança Pública e Defesa Social - CNSP, Conselho Gestor do Fundo Nacional de Segurança Pública - CFNSP, Conselho Nacional de Imigração - CNI e Comitê Nacional para os Refugiados;

d) Entidade vinculada: Conselho Administrativo de Defesa Econômica - CADE e Autoridade Nacional de Proteção de Dados (ANPD).

2.2.1.3. Como pode ser observado, a estrutura do Ministério é consideravelmente robusta e complexa, abrangendo diversas áreas de atuação que carecem de tratamento diferenciado, proporcionado de acordo às suas especificidades. Isso se aplica não apenas em termos de suas dimensões, mas também em relação ao grau de sensibilidade e sigilo requerido para o desempenho de suas atividades.

2.2.1.4. Alguns temas sensíveis podem ser destacados de cada um dos Órgãos específicos singulares e de acordo com as competências do Ministério com base no Decreto nº 11.348, de 1º de janeiro de 2023:

(...)

Art. 14. À Secretaria Nacional de Justiça compete:

(...)

II - coordenar, em parceria com os órgãos da administração pública, a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro - Enccda e outras ações do Ministério relacionadas com o enfrentamento da corrupção, da lavagem de dinheiro e do crime organizado transnacional;

III - coordenar a negociação de acordos e a formulação de políticas de cooperação jurídica internacional, civil e penal, e a execução dos pedidos e das cartas rogatórias relacionadas com essas matérias;

IV - coordenar as ações relativas à recuperação de ativos;

V - coordenar, em parceria com os demais órgãos e entidades da administração pública federal, a formulação e a implementação das seguintes políticas:

(...)

Art. 17. À Secretaria Nacional do Consumidor compete:

I - formular, promover, supervisionar e coordenar a política nacional de proteção e defesa do consumidor;

II - integrar, articular e coordenar o Sistema Nacional de Defesa do Consumidor;

(...)

X - receber e encaminhar consultas, denúncias ou sugestões apresentadas por consumidores, entidades representativas ou pessoas jurídicas de direito público ou privado;

(...)

Art. 20. À Secretaria Nacional de Políticas sobre Drogas e Gestão de Ativos compete:

I - assessorar e assistir o Ministro de Estado quanto às:

a) políticas sobre drogas relacionadas com a prevenção do uso indevido, a atenção e a reinserção social de usuários e dependentes de drogas, a redução da oferta e a repressão da produção não autorizada e do tráfico ilícito de drogas; e

(...)

VIII - organizar informações, acompanhar fóruns internacionais e promover atividades de cooperação técnica, científica, tecnológica e financeira com outros países e com organismos internacionais, e mecanismos de integração regional e sub-regional que tratem de políticas sobre drogas na sua área de atuação;

Art. 24. À Secretaria Nacional de Segurança Pública compete:

I - assessorar o Ministro de Estado:

a) na articulação, na proposição, na formulação, na implementação, no acompanhamento e na avaliação de políticas, de estratégias, de planos, de programas e de projetos de segurança pública e defesa social;

b) na definição, na implementação e no acompanhamento de políticas, de programas e de projetos de gestão, ensino e pesquisa em segurança pública;

c) nas atividades de inteligência e operações policiais, com foco na integração com os órgãos de segurança pública internacionais, federais, estaduais, municipais e distritais;

d) no exercício das funções de autoridade central federal, no âmbito da Política Nacional de Busca de Pessoas Desaparecidas, nos termos do disposto na Lei nº 13.812, de 16 de março de 2019; e

e) na articulação intersetorial de políticas públicas de prevenção à violência e ao crime;

(...)

X - implementar, manter e modernizar redes de integração e de sistemas nacionais de inteligência de segurança pública, em conformidade com disposto na Lei nº 13.675, de 11 de junho de 2018;

XI - promover a integração das atividades de inteligência de segurança pública, em consonância com os órgãos de inteligência federais, estaduais, municipais e distritais que compõem o Subsistema de Inteligência de Segurança Pública;

(...)

Art. 31. À Secretaria Nacional de Políticas Penais cabe exercer as competências estabelecidas nos art. 71 e art. 72 da Lei nº 7.210, de 11 de julho de 1984 - Lei de Execução Penal, e, especificamente:

I - planejar e coordenar a política nacional de serviços penais;

(...)

IV - prestar apoio técnico aos entes federativos quanto à implementação dos princípios e das regras da execução penal;

(...)

XII - promover a gestão da informação penitenciária e consolidar, em banco de dados nacional, informações sobre os sistemas penitenciários federal e dos entes federativos.

(...)

Art. 38. À Secretaria Nacional de Assuntos Legislativos compete:

I - promover o processo de articulação com o Congresso Nacional nos assuntos de competência do Ministério, observadas as competências dos órgãos que integram a Presidência da República;

II - providenciar o atendimento às consultas e aos requerimentos formulados, além de acompanhar a tramitação legislativa dos projetos de interesse do Ministério;

III - participar do processo de interlocução com os Governos estaduais, distrital e municipais, com as assembleias legislativas estaduais, com a Câmara Legislativa do Distrito Federal e com as câmaras municipais nos assuntos de competência do Ministério, com o objetivo de assessorá-los em suas iniciativas e de providenciar o atendimento às consultas formuladas, observadas as competências dos órgãos que integram a Presidência da República;

IV - auxiliar as comissões e grupos especiais de juristas constituídos pelo Ministro de Estado, com o objetivo de elaborar e consolidar leis; e

V - organizar e auxiliar as áreas temáticas nas consultas públicas de temas de competência do Ministério.

(...)

Art. 40. À Secretaria de Acesso à Justiça compete:

I - promover políticas públicas de modernização, aperfeiçoamento, transformação digital e democratização do acesso à justiça e à cidadania, inclusive no âmbito de plataformas digitais;

(...)

IV - promover ações para o aperfeiçoamento do sistema e da política de justiça, em articulação com os órgãos e as entidades dos Poderes Executivo e Judiciário e com o Ministério Público, a Defensoria Pública, a Ordem dos Advogados do Brasil, os órgãos e as agências internacionais e as organizações da sociedade civil;

(...)

VII - promover ações relacionadas ao Sistema de Justiça que contribuam para a redução da violência contra as mulheres, a população LGBTQIA+, os povos indígenas e as comunidades tradicionais e para o aprimoramento do Sistema de Justiça.

(...)

Art. 43. À Polícia Federal cabe exercer as competências estabelecidas no § 1º do art. 144 da Constituição, e, especificamente:

I - apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, além de outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, conforme previsto em lei;

II - prevenir e reprimir o tráfico ilícito de entorpecentes e drogas e o contrabando e o descaminho de bens e de valores, sem prejuízo da ação fazendária e de outros órgãos públicos, nas suas áreas de competência;

(...)

VI - acompanhar e instaurar inquéritos relacionados com direitos humanos e conflitos agrários ou fundiários e aqueles deles decorrentes, quando se tratar de crime de competência federal, além de prevenir e reprimir esses crimes.

(...)

Art. 58. À Polícia Rodoviária Federal cabe exercer as competências estabelecidas no § 2º do art. 144 da Constituição, no art. 20 da Lei nº 9.503, de 23 de setembro de 1997 - Código de Trânsito Brasileiro, no Decreto nº 1.655, de 3 de outubro de 1995, e, especificamente:

I - planejar, coordenar e executar o policiamento, a prevenção e a repressão de crimes nas rodovias e estradas federais e nas áreas de interesse da União;

II - exercer os poderes de autoridade de trânsito nas rodovias e nas estradas federais;

III - executar o policiamento, a fiscalização e a inspeção do trânsito e do transporte de pessoas, cargas e bens;

IV - planejar, coordenar e executar os serviços de prevenção de acidentes e de salvamento de vítimas nas rodovias e estradas federais;

(...)

2.2.1.5. Merecem também ser destacados os órgãos colegiados do Ministério, que atuam em temas sensíveis, e de importância nacional, como por exemplo o Conselho Nacional de Combate à Pirataria (CNCPP). Esse órgão é a instância que trata do assunto pirataria no Brasil, sendo responsável pela aplicação de abordagens e metodologias inéditas para o tratamento da questão, elaborando diretrizes para a formulação e proposição de plano nacional para o combate à pirataria, à sonegação fiscal dela decorrente e aos delitos contra a propriedade intelectual.

2.2.1.6. Outro importante órgão colegiado é o Conselho Nacional de Políticas sobre Drogas - CONAD, sendo o órgão máximo brasileiro que regulamenta e pesquisa o uso de substâncias químicas e determina quais são drogas e quais não são e sua classificação. Este conselho também realiza campanhas de esclarecimento quanto às drogas e projetos como o de dano mínimo.

2.2.1.7. Destaca-se também o Conselho Nacional de Política Criminal e Penitenciária - CNCP, que preconiza a implementação, em todo o território nacional, de uma nova política criminal e principalmente penitenciária a partir de periódicas avaliações do sistema criminal, criminológico e penitenciário, bem como a execução de planos nacionais de desenvolvimento quanto às metas e prioridades da política a ser executada.

2.2.1.8. O Ministério possui também em sua estrutura o Conselho Nacional de Segurança Pública - CNSP, que tem o objetivo de propor diretrizes para prevenir e conter a violência e a criminalidade no País. O CNSP está previsto na lei nº 13.675, de 11 de junho de 2018, que instituiu o Sistema Único de Segurança Pública (SUSP) e a Política Nacional de Segurança Pública e Defesa Social (PNSPDS), o órgão será composto por representantes da União, dos estados, Distrito Federal, municípios e sociedade civil.

2.2.1.9. De acordo com o alinhamento ao Plano Estratégico Institucional 2024-2027 o MJSP, possui os seguintes objetivos estratégicos:

a) OE-PEI-01 - Promover a segurança pública cidadã e humanizada, com especial atenção a pessoas em situação de vulnerabilidade;

b) OE-PEI-02 - Promover o acesso à justiça e proteger os direitos do cidadão, inclusive os digitais e os dados pessoais;

c) OE-PEI-03 - Fortalecer a prevenção e o enfrentamento à criminalidade;

c) OE-PEI-04 - Promover uma execução penal justa, que viabilize a reintegração social e a inatividade das lideranças criminosas;

d) OE-PEI-08 - Aprimorar o processo de recuperação de ativos e sua efetiva aplicação em políticas públicas;

e) OE-PEI-11 - Potencializar e aprimorar a estrutura e os serviços de Tecnologia da Informação e Comunicação;

f) OE-EGD-01 - Oferta de serviços públicos digitais;

g) OE-EGD-11 - Garantia da segurança das plataformas de governo digital e de missão crítica;

h) OE-EGD-16 - Otimização das infraestruturas de tecnologia da informação.

2.2.1.10. Para que todos os órgãos da estrutura do Ministério possam atuar de maneira eficiente e eficaz, e com os recursos necessários para o pleno desenvolvimento de suas atividades, **são necessários mecanismos tecnológicos que sejam capazes de gerar valor e entregar as informações necessárias, de forma a permitir a produção de conhecimento útil e tempestivo à tomada de decisão**, seja em nível estratégico, tático ou operacional.

2.2.1.11. Um aspecto relevante a ser considerado é a **natureza das informações com as quais o Ministério da Justiça e Segurança Pública deve lidar para a execução das suas competências, e o nível de sigilo que deve**

ser a elas assegurado. Em muitos casos trata-se de dados com características que ensejam o controle estrito do acesso, seja porque são informações que dizem respeito a intimidade e vida privada de cidadãos, seja porque incluem atos preparatórios para a execução de ações de segurança pública e investigação criminal ou ainda porque trata-se de informações com imposição da observância de sigilo por determinação legal.

2.2.1.12. Importante destacar, que a Segurança Pública é um processo, ou seja, uma sequência contínua de fatos ou operações que apresentam certa unidade ou que se reproduzem com certa regularidade, que compartilha uma visão focada em componentes preventivos, repressivos, judiciais, saúde e sociais.

2.2.1.13. Trata-se de um processo sistêmico, pela necessidade da integração de um conjunto de conhecimentos e ferramentas estatais que devem interagir a mesma visão, compromissos e objetivos. Deve ser também otimizado, pois dependem de **decisões rápidas, medidas saneadoras e resultados imediatos**. Sendo a ordem pública um estado de serenidade, apaziguamento e tranquilidade pública, em consonância com as leis, os preceitos e os costumes que regulam a convivência em sociedade, a preservação deste direito do cidadão só será amplo se o conceito de segurança pública for aplicado.

2.2.1.14. A segurança pública não pode ser tratada apenas como medidas de vigilância e repressiva, mas como um sistema integrado e otimizado envolvendo instrumento de prevenção, coação, justiça, defesa dos direitos, saúde e social. O processo de segurança pública se inicia pela prevenção e finda na reparação do dano, no tratamento das causas e na reinclusão na sociedade do autor do ilícito.

2.2.1.15. Para isso, houve a criação do Sistema Único de Segurança Pública (SUSP), que é um marco divisório na história do país. Implantado pela Lei nº 13.675/2018, sancionada em 11 de junho, o SUSP dá arquitetura uniforme ao setor em âmbito nacional e prevê, **além do compartilhamento de dados, operações e colaborações nas estruturas federal, estadual e municipal**.

2.2.1.16. Com a criação do SUSP, surgem novas regras, em que os órgãos de segurança pública, como as polícias civis, militares e Federal, as secretarias de Segurança e as guardas municipais serão integrados para atuar de forma cooperativa, sistêmica e harmônica.

2.2.1.17. Como já acontece na área de saúde, os órgãos de segurança do SUSP já realizam operações combinadas. Elas podem ser ostensivas, investigativas, de inteligência ou mistas e contar com a participação de outros órgãos, não necessariamente vinculados diretamente aos órgãos de segurança pública e defesa social – especialmente quando se tratar de enfrentamento a organizações criminosas.

2.2.1.18. O fato é que para exercer todas suas competências de modo cada vez mais eficaz, o Ministério precisa incorporar novas ferramentas de tecnologia da informação capazes de realizar o processamento e a análise de volumes massivos de dados com diferentes formatos e gerados de forma ininterrupta, dentro do conceito de *Big Data*. Atualmente, várias unidades do Ministério (por exemplo, SENASP, DRCI, DPF e DPRF) demandam a disponibilização de ferramentas capazes de processar grandes volumes de informações e gerar conhecimento e *insights* relevantes para a aplicação de políticas públicas nas áreas da segurança pública e do combate à corrupção e à lavagem de dinheiro.

2.2.1.19. A capacidade que as ferramentas de análise, pesquisa e cruzamentos de dados da administração pública federal possuem para potencializar o embasamento de políticas públicas e o combate às fraudes foi brilhantemente demonstrada pelo trabalho da SEFTI/TCU apresentado no Acórdão nº 2.587/2018 – Plenário. A metodologia de trabalho envolveu o cruzamento de dados disponibilizados por diferentes instituições para a investigação de determinadas tipologias (fatos que estariam em desconformidade com a legislação ou que denotariam a ocorrência, ao menos em tese, de fraudes ou ilícitos). A partir dos dados analisados foram identificadas diversas ocorrências destas tipologias em diferentes ações ou programas de governo, em um espectro de análises que englobaram, por exemplo, ocorrências não usuais e contrárias à legislação em licitações e contratações públicas, fatos suspeitos na execução financeira e orçamentária de órgãos públicos e a existência de possíveis fraudes em programas de governo como o Bolsa-Família e o Minha Casa Minha Vida.

2.2.1.20. O mesmo potencial demonstrado pelas análises realizadas no Acórdão TCU 2.587/2018 **pode ser aplicado às ações vinculadas às políticas de segurança pública e de combate à corrupção, mas, para isso, alguns entraves precisam ser vencidos**. Notadamente, existem ainda hoje uma série de dificuldades de ordens técnica e político-administrativa para um compartilhamento efetivo de dados entre os órgãos da Administração Pública, mesmo após a edição do Decreto nº 8.789/2016, que estabelece como regra o compartilhamento de informações entre as diversas entidades da Administração Pública Federal para viabilizar a execução e o monitoramento de políticas públicas.

2.2.1.21. Uma unidade crucial para que o MJSP cumpra suas funções e missão é a Subsecretaria de Tecnologia da Informação e Comunicações - STI, criada por meio do DECRETO Nº 11.348, DE 1º DE JANEIRO DE 2023, que é

responsável direta pelo planejamento, coordenação e execução das atividades relacionadas com o SISP no âmbito do Ministério, além de articulação com os órgãos centrais, elaborando e consolidando planos e programas de sua competência:

(...)

Art. 12. À Subsecretaria de Tecnologia da Informação e Comunicação compete:

I - planejar, coordenar e supervisionar a execução das atividades relacionadas com o Sistema de Administração dos Recursos de Tecnologia da Informação no âmbito do Ministério;

II - promover a articulação com os órgãos centrais do sistema federal referido no inciso I e informar e orientar os órgãos integrantes da estrutura do Ministério e da entidade a ele vinculada quanto ao cumprimento das normas estabelecidas;

III - elaborar e consolidar os planos e os programas das atividades de sua área de competência e submetê-los à decisão superior; e

IV - acompanhar e promover a avaliação de projetos e atividades, no âmbito de sua competência.

(...)

2.2.1.22. Importante salientar que com a criação da Subsecretaria de Tecnologia da Informação e Comunicação do Ministério, houve um aumento significativo de demandas, muitas represadas pela falta de pessoal e pela carência de uma estrutura organizacional mais robusta. Esse fato exigiu, e tem exigido, evolução constante dos ambientes da infraestrutura de Data Centers, redes, segurança, aplicações, armazenamento, dentre outros.

2.2.1.23. Como se observa, a abrangência e capilaridade dos resultados a serem alcançados requerem do corpo diretivo do Ministério a adoção de medidas consistentes na oferta de meios e instrumentos que permitam o aumento de produtividade e maturidade funcional do órgão. Assim, a STI vem em constante atualização, visto que seus sistemas e serviços possuem valor inestimado, sendo muito importante que os investimentos em Tecnologia da Informação sejam priorizados no sentido de garantir a segurança e a disponibilidade dos dados e informações em conjunto com as melhores práticas de mercado. O uso da Tecnologia da Informação como ferramenta para a otimização das atividades operacionais possibilita aos órgãos da Administração Pública programarem medidas que tornam seus procedimentos cada vez mais rápidos, seguros, integrados, eficientes e, sobretudo, acessíveis a toda a população brasileira.

2.2.1.24. Prezando pela constante melhoria da qualidade dos serviços e pela modernização dos ativos de Tecnologia em momento que se mostra viável e necessário, justifica-se a contratação de uma solução que visa a longevidade organizacional diante de parâmetros essenciais a nossa estratégia, como a Continuidade de Negócios, Alta Disponibilidade e Recuperação de Desastres. Muitas operações fundamentais para o funcionamento do Ministério da Justiça e Segurança Pública, e seus Departamentos, estão fortemente relacionadas e são dependentes dos serviços disponíveis em sua infraestrutura de Tecnologia da Informação e Comunicação, de maneira que toda e qualquer indisponibilidade produz impacto direto sobre o seu desempenho institucional, bem como reflete na qualidade dos aspectos de bem-estar populacional.

2.2.1.25. Entende-se por serviço de Tecnologia da Informação o conjunto de componentes computacionais necessários para o correto funcionamento de um sistema de negócio (software, processamento, conectividade e armazenamento). Além disso, a arquitetura pretendida garante as funcionalidades de governança e gestão para a devida operação e acompanhamento diário dos serviços de Tecnologia da Informação executados por esta diretoria. Este Órgão possui, atualmente, um parque computacional diversificado de equipamentos de informática utilizados como concentradores dos serviços corporativos. A integração desse conjunto, por meio da utilização de softwares, sistemas e aplicativos corporativos e da infraestrutura permite a subsidiar os trabalhos dos usuários da Instituição.

2.2.1.26. Devido ao constante aumento das demandas relacionadas a sistemas e aplicações disponibilizados pelo Ministério, nem como as mudanças e modernizações que os sistemas vêm sofrendo, o grau de complexidade quanto ao bom uso dos sistemas de informação tem uma tendência natural a aumentar quando novas tecnologias não são adotadas no dia a dia dos usuários. Não obstante, a arquitetura de Data Center do Ministério, hoje, é composta por equipamentos legados que compreendem servidores, sistemas de armazenamento, softwares de backups e plataformas de virtualização, sendo de extrema importância que a infraestrutura computacional do órgão acompanhe as mudanças e forneça toda a base operacional para os novos sistemas e serviços que o órgão necessita disponibilizar. Em virtude disso, a pasta necessita de uma infraestrutura que garanta estabilidade, segurança, alta disponibilidade e agilidade na utilização e no armazenamento de dados e informações.

2.2.1.27. Diante do cenário exposto, o Ministério buscou analisar soluções que possam contornar os desafios existentes de modo a maximizar o retorno sobre os investimentos (ROI) já feitos, bem como sanar as dificuldades tecnológicas alinhadas à missão organizacional. A adoção de solução de tecnologia da informação para provisão da

continuidade operacional dos serviços de tecnologia da informação e da capacidade de processamento de dados do Ministério, em caso de desastres e graves incidentes que impactem negativamente a atual infraestrutura de TI, se mostra viável e cumpre com requisitos essenciais que permitem a otimização de plataformas de virtualização existentes, o uso eficiente das camadas de armazenamento a integração entre os Data Centers com a alta disponibilidade de aplicações, migração de sistemas e serviços com a implementação de gerenciamento centralizado, funções avançadas de replicação contingência entre os SITES e nuvens públicas.

2.2.1.28. É imprescindível para o projeto contemplar em sua estrutura todas as vantagens que uma solução integrada pode agregar, como o uso de ferramentas que auxiliam na gestão proativa dos recursos computacionais, o emprego de mecanismos que possuem inteligência artificial e até mesmo algoritmos de aprendizado de máquina fomentam cada vez mais o uso da tecnologia como o meio para o Ministério garantir o cumprimento de sua missão.

2.2.1.29. Considerando esse prisma, a STI/MJSP tem envidado esforços técnicos e administrativos para equacionar da melhor maneira possível o atendimento ao previsto na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 (Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação), na Instrução Normativa nº 1, de 27 de maio de 2020 (Dispõe sobre a Estrutura de Gestão da Segurança da Informação) e na Instrução Normativa nº 5, de 30 de agosto de 2021 (Dispõe sobre os requisitos mínimos de Segurança da Informação para utilização de soluções de computação em nuvem) e aos desafios tecnológicos frente à quantidade de projetos estratégicos essenciais para a sociedade brasileira.

2.2.2. Visão geral da infraestrutura de Data Centers do MJSP e suas características:

2.2.2.1. Na atual conjuntura, a estrutura de Tecnologia da Informação do Ministério vem passando por mudanças de disposição física em suas unidades, o que tem provocado a necessidade de aquisição de equipamentos, processos de automatização e alta disponibilidade que suportem este dinamismo.

2.2.2.2. Adotando as melhores práticas de Tecnologia da Informação para grandes corporações, o Ministério centraliza seus serviços baseados em Tecnologia da Informação em Data Centers com infraestrutura local (*on-premise*), que se destinam à hospedagem de sistemas legados e sistemas com grau de restrição, além de contratos de nuvem (*on-cloud*) com a Microsoft (*Azure*) e com a Oracle (*Oracle Cloud*).

2.2.2.3. A estrutura de Data Centers *on-premises* do MJSP é formada pelo **Data Center principal** (localizado no núcleo central do Ministério, Esplanada dos Ministérios, Brasília-DF) pelo **Data Center secundário** (localizado no Centro Integrado de Comando e Controle Nacional de Brasília – CICCND-DF, Setor Policial Sul, Brasília-DF), conforme Figura 1:

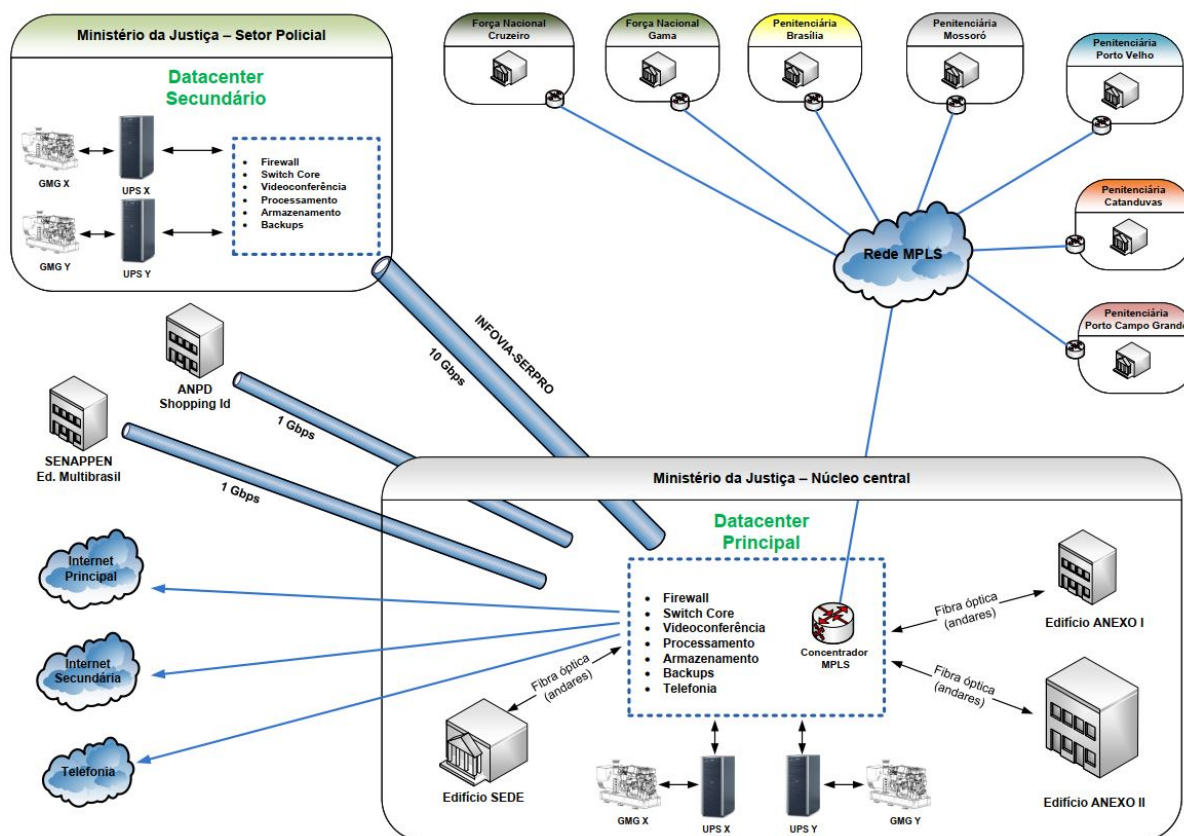


Figura 1 - Estrutura de Data Centers do MJSP.

2.2.2.4. Atualmente a STI vem adotando várias medidas para implantação de alta disponibilidade entre os dois Data Centers, de forma que as aplicações críticas possam ser replicadas em caso de *Disaster Recovery*.

2.2.2.5. Tratando-se do ambiente *on-premise*, é importante salientar que os recursos estão chegando em um nível de saturação considerável, tanto na parte de processamento quanto de armazenamento. Outro fator a ser considerado, é a coexistência entre ambientes *on-premises* e *on-cloud*, que demandam perfeita integração e gerência, as quais devem ser orientadas a serviço e não somente a ativos de infraestrutura.

2.2.2.6. Diante disso, são necessárias mudanças conceituais e tecnológicas de forma que seja possível a implantação de uma nuvem privada *on-premises* de alto desempenho, viabilizando a integração tanto com o Data Center secundário, quando com as nuvens públicas já em operação.

2.2.2.7. Importante destacar que o modelo de infraestrutura de nuvem pretendido no âmbito do MJSP, se baseia no conceito de nuvem híbrida (inciso IV, Art. 3º da Instrução Normativa Nº 5, de 30 de agosto de 2021), composta pela nuvem privada (Salas Cofres *on-premise*) e nuvem pública (*Microsoft Azure* e *Oracle Cloud*).

2.2.2.8. Cabe destacar que nos anos de 2020 e 2021, foi feita a contratação e a implantação de uma Sala Cofre certificada conforme a norma ABNT NBR 15.247, de forma a garantir a proteção física da infraestrutura e sistemas críticos de Tecnologia da Informação e Comunicações do Ministério da Justiça e Segurança Pública. A referida contratação foi executada por meio do processo 08006.000180/2019-08, tendo em vista que a infraestrutura não apresentava condições mínimas adequadas para acomodar e proteger a quantidade de equipamentos sensíveis e críticos, que em caso de sinistro poderia causar prejuízos incalculáveis ao funcionamento da rede e à imagem do órgão.

2.2.2.9. Além disso, foi feita a contratação, por meio do processo 08006.000602/2020-71, de solução de ativos de rede, balanceamento de carga e segurança para os Data Centers, incluindo serviços especializados, aquisição de equipamentos e softwares, modernização e expansão da capacidade atual para atendimento das demandas daquela época.

2.2.2.10. Para a sustentação de todos os ambientes das aplicações, o Ministério possui um robusto ambiente de virtualização, que atualmente possui quase 900 (novecentos) servidores virtuais. Todos os servidores virtuais funcionam nas redes SAN (*Storage Area Network*) dos Data Centers Principal e Secundário que possuem as topologias conforme ilustram as Figuras 2 e 3, respectivamente:

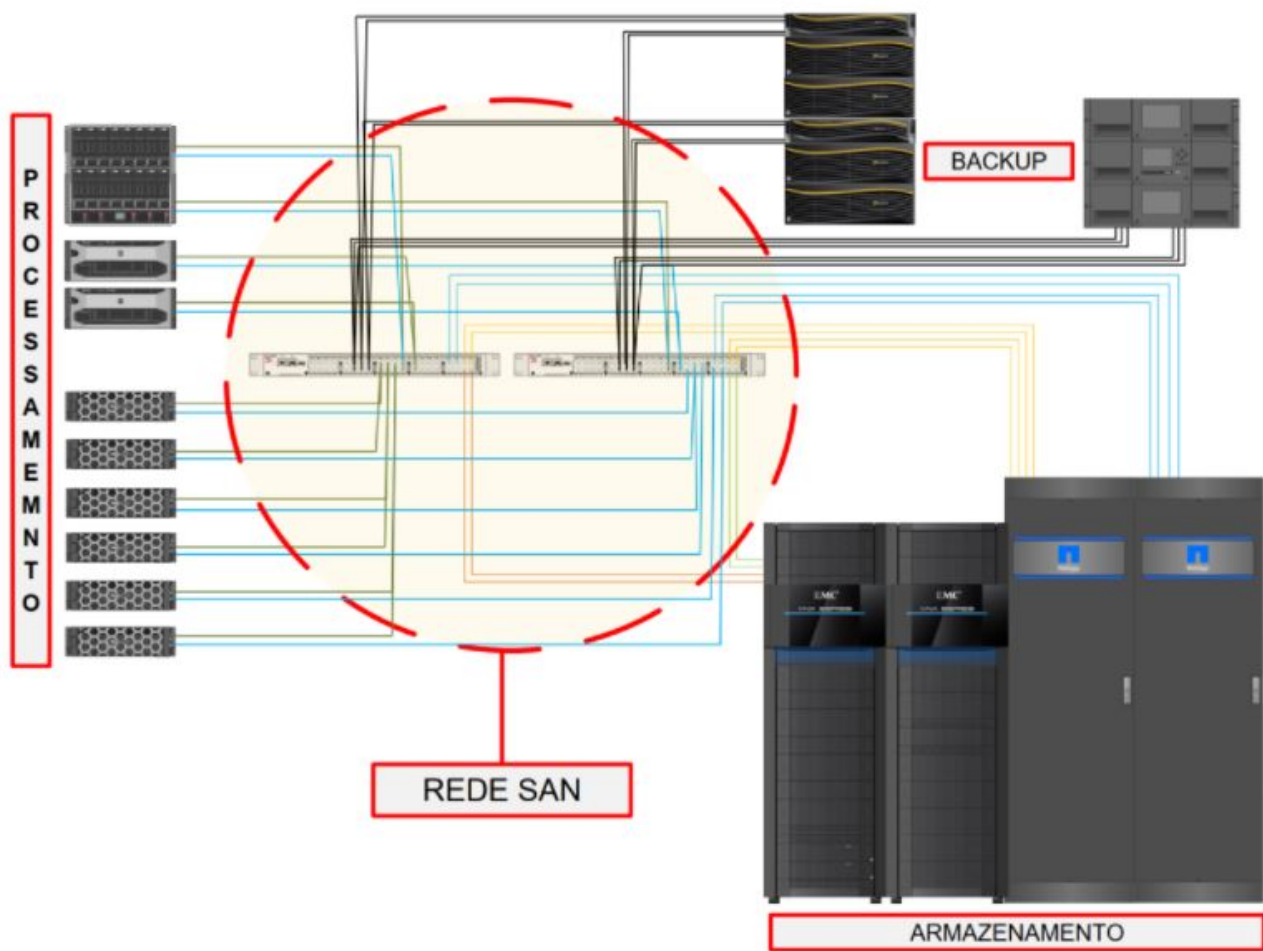


Figura 2 - Rede SAN do Data Center Principal.

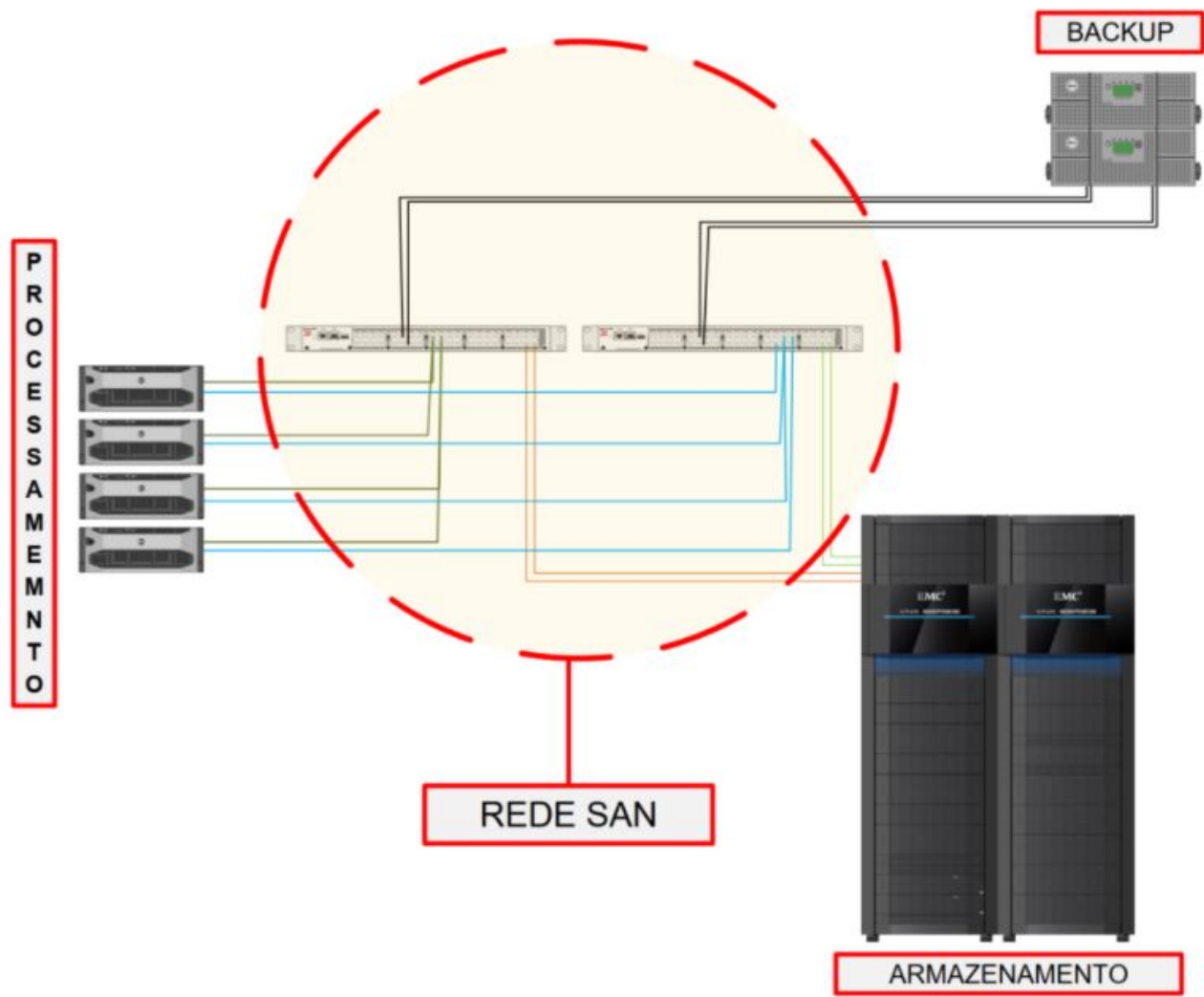


Figura 3 - Rede SAN do Data Center Secundário.

2.2.2.11. Na área de armazenamento, o Data Center Principal possui dois equipamentos de storages, sendo 01 equipamento EMC VNX 7500 e 02 equipamentos NetApp FAS8080. Na Tabela 1, estão dispostos os equipamentos com suas respectivas quantidades de armazenamento bruto:

Quantidade de equipamentos	Equipamento	Disco SATA (Terabyte)	Disco SAS (Terabyte)	Disco SSD (Terabyte)	Total bruto (Terabyte)	Contrato de Manutenção
01	EMC VNX 7500	115	170	11	296	Sim
01	NetApp FAS8080	401	75,21	3,7	479,91	Sim
01	NetApp FAS8080	401	75,21	3,7	479,91	Sim
TOTAIS		917	320,42	18,4	1.255,82	

Tabela 1 - Recursos do ambiente de armazenamento Data Center Principal.

2.2.2.12. O Data Center secundário, na área de armazenamento, possui dois equipamentos de Storages EMC VNX 5300. Na Tabela 2, estão dispostos os equipamentos com suas respectivas quantidades de armazenamento bruto:

Quantidade de equipamentos	de Equipamento	Disco SATA (Terabyte)	Disco SAS (Terabyte)	Disco SSD (Terabyte)	Total bruto (Terabyte)	Contrato de Manutenção
01	EMC VNX 5300	101	94	-	195	Sim
01	EMC VNX 5300	101	94	-	195	Sim
TOTAIS		202	188	-	390	

Tabela 2 - Recursos do ambiente de armazenamento Data Center Secundário.

2.2.2.13. O ambiente de backup do Data Center Principal é composto por 02 (dois) *appliances* Symantec NetBackup 5230 (configurados como Media Server), Licença do software NetBackup e 01 (uma) Tape Library TS4300. Já o Data Center Secundário possui 02 (duas) Tape Library PowerVault TL2000. Na Tabela 3, estão dispostos os equipamentos com suas respectivas características:

Quantidade de equipamentos	de Equipamento	Capacidade (Terabyte)	Contrato de Manutenção
01	NetBackup 5230	50	Não
01	NetBackup 5230	50	Não
01	Tape Library TS4300	-	Sim
01	Tape Library PowerVault TL2000	-	Não
01	Tape Library PowerVault TL2000	-	Não

Tabela 3 - Recursos do ambiente de backup Data Center Principal e Secundário.

2.2.2.14. Destaca-se que para interconexão de todos os equipamentos listados nos Data Centers em questão, bem como para futuras expansões, o Ministério dispõe de uma estrutura de *switches* de alto desempenho, recentemente adquiridos e implantados (Contrato nº 132/2020 - SEI nº 13489505), capazes de interligar à altas velocidades, os servidores do ambiente de processamento, os quais formam a base para todo o ambiente de virtualização.

2.2.2.15. Conforme exposto em tópicos anteriores, nos últimos anos, o ambiente computacional do Ministério tem passado por um grande processo de transformação. Mais especificamente no ambiente de virtualização, houve um crescimento expressivo no consumo de recursos, tais como utilização de disco, consumo de processamento e de memória volátil. Esse crescimento se deu em virtude da alta demanda de recursos de TIC pelas áreas de negócio para atendimento de seus projetos estratégicos. A Figura 4 demonstra a evolução do quantitativo de servidores virtuais nos últimos 6 anos:

Crescimento Servidores Virtuais Data Center Principal e Secundário

CLUSTER	2018	2019	2020	2021	2022	2023
CICCN-DELL-R930	14	7	1	13	4	47
MJ-BLADE-HP	115	93	69	68	40	14
MJ-R910	31	1	0	0	1	0
MJ-DELL-R940	106	112	115	89	25	14

Crescimento VMs Anual	2018	2019	2020	2021	2022	2023
	266	479	664	834	904	979

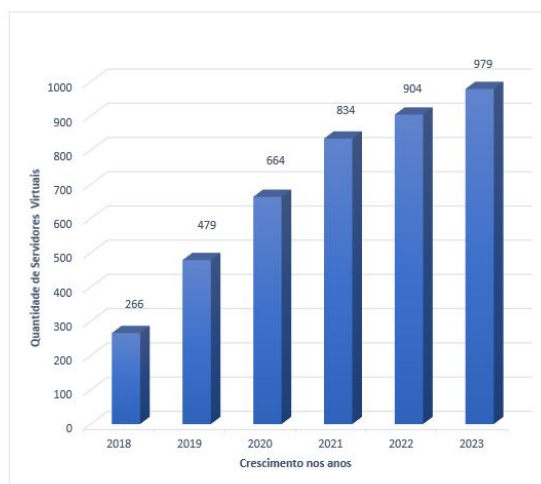


Figura 4 - Crescimento Servidores Virtuais.

2.2.2.16. Como consequência do aumento de servidores virtuais, naturalmente ocorreu o crescimento das necessidades dos recursos de armazenamento e backup que apesar de várias medidas de remanejamento, higienização e backups de dados, pela equipe técnica da STI, exigem medidas céleres de reestruturação pra evolução tecnológica dos ambientes. As Figuras 5, 6, 7 e 8 demonstram a evolução do consumo de armazenamento nos últimos 5 anos, destacando na cor vermelha o percentual de ocupação em cada equipamento:

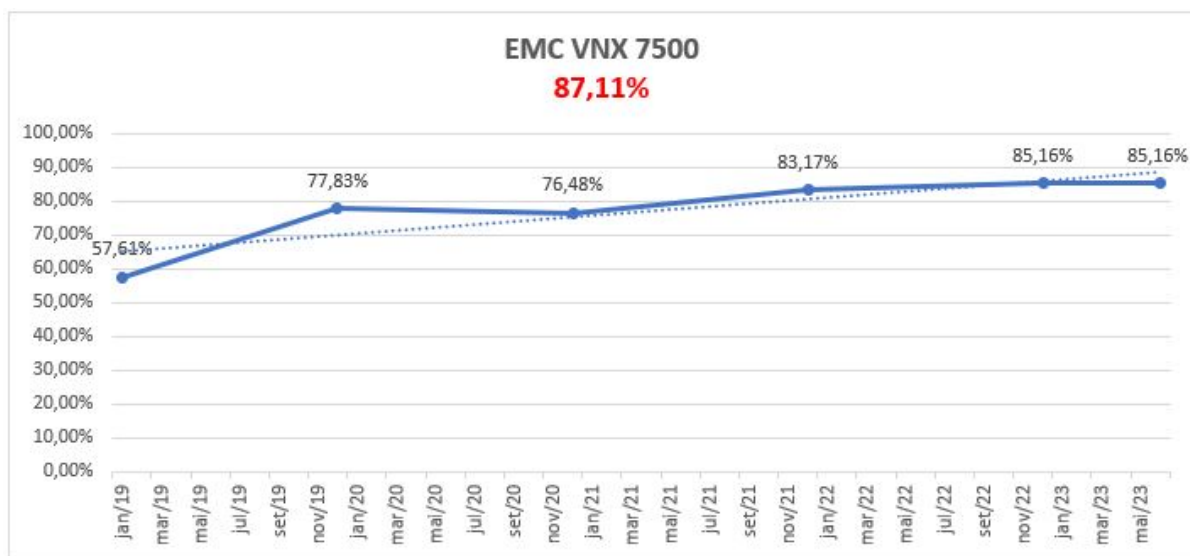


Figura 5 - Crescimento Storage EMC VNX 7500.

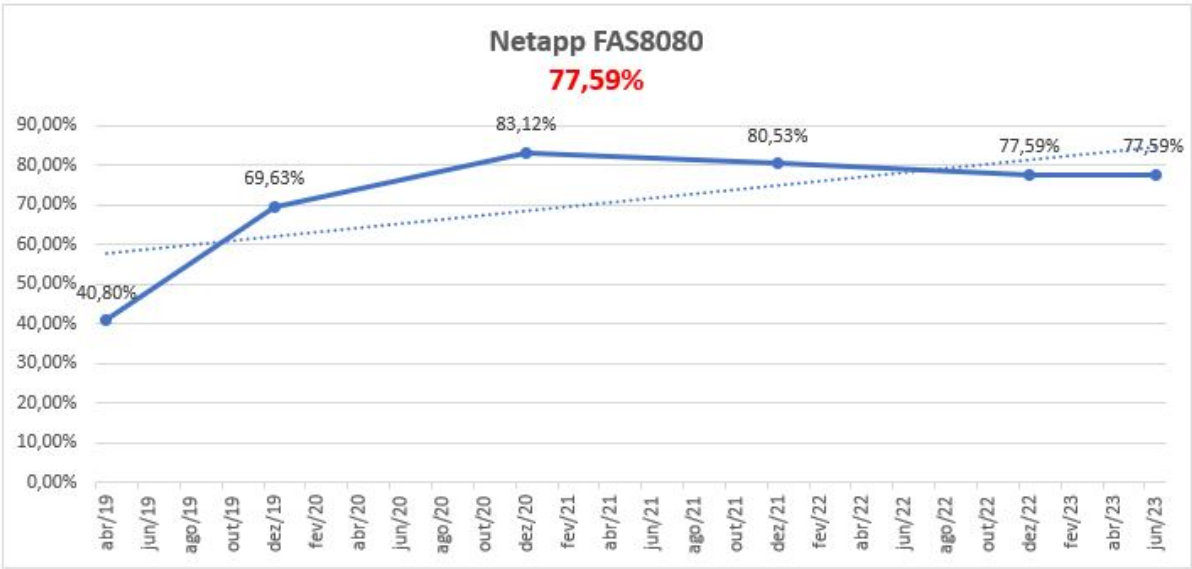


Figura 6 - Crescimento Storage NetApp.

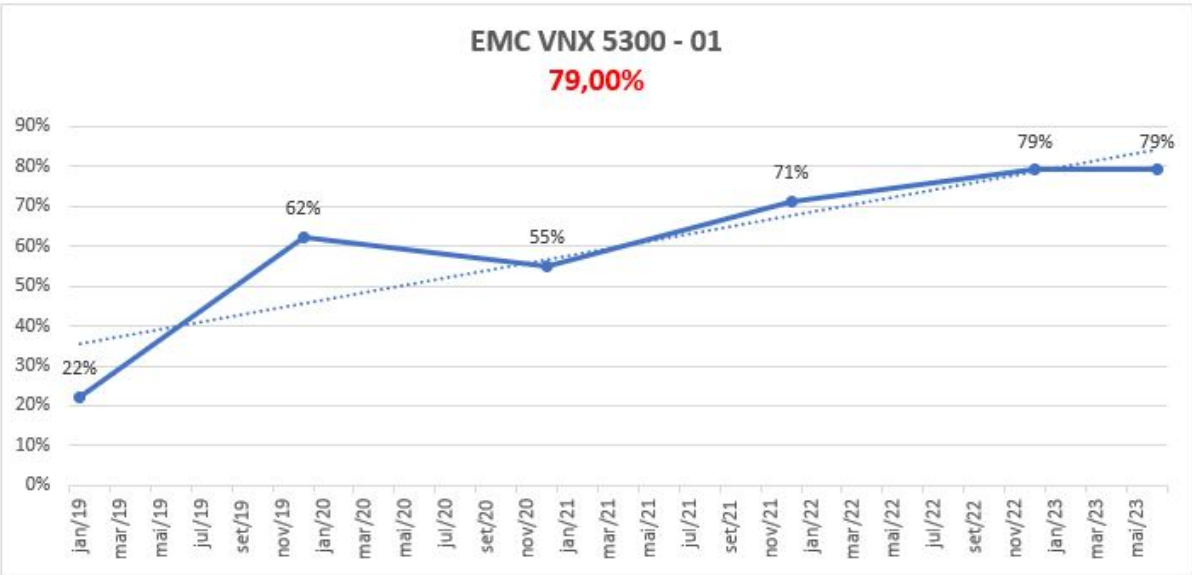


Figura 7 - Crescimento Storage EMC VNX 5300 01.

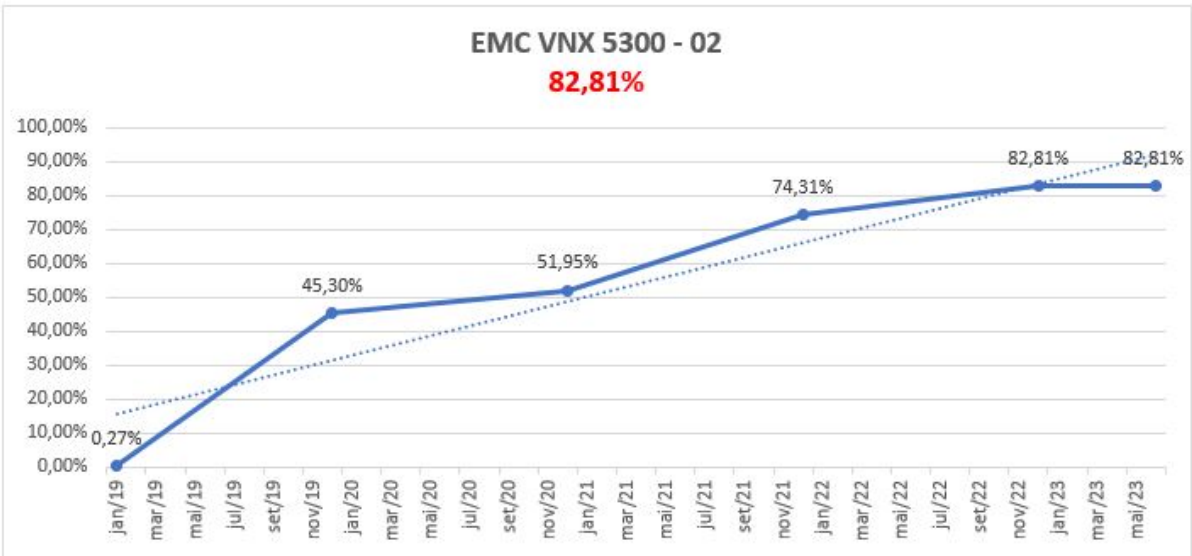


Figura 8 - Crescimento Storage EMC VNX 5300 01.

2.2.2.17. Importante destacar, que além do consumo de armazenamento demonstrado nas imagens acima, existe grande demanda por discos rápidos (SSD), para sistemas operacionais, aplicações e bancos de dados, que necessitam de desempenho aprimorado, bem como para entrega performática de arquivos via protocolo NFS, sendo que esse fator impacta consideravelmente no provisionamento de aplicações que necessitam maior desempenho. Como pode ser observado na Tabela 1, há atualmente 18,4 Terabytes de armazenamento com disco SSD, que não atende a demanda das aplicações do ambiente produtivo.

2.2.2.18. Destaca-se, conforme exposto em tópicos anteriores, que implantação de novas aplicações gera efeito em cascata, tendo como último ponto a cópia de segurança de todos os dados dos sistemas e bases de dados. O Ministério da Justiça possui hoje diversos serviços críticos que dependem da estrutura de backup para cópia de seus dados, e a atual solução de backup tem se mostrado insuficiente diante do crescimento do ambientes para atendimento das demandas do MJSP, fato que a partir do mês de maio de 2019, foi necessária a adição de porções do *storage* para serem utilizadas como pools de armazenamento de backup em disco, visto que o espaço nos *appliances* já não era suficiente. A Figura 9 demonstra o histórico da volumetria de backup, entre janeiro de 2019 a fevereiro de 2022:

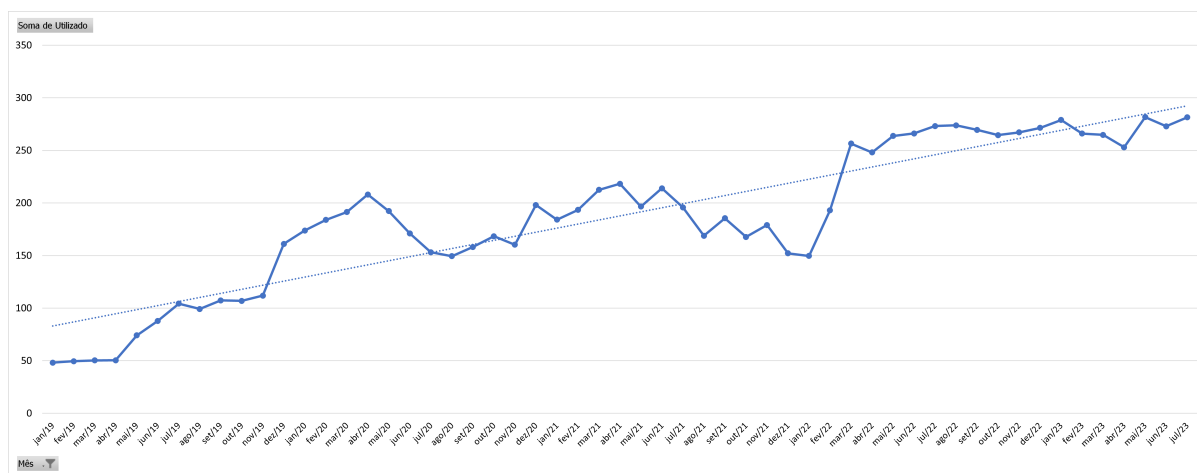


Figura 9 - Histórico da volumetria do backup.

2.2.2.19. Ainda convém informar as limitações de performance da tecnologia híbrida atualmente utilizada nos equipamentos de armazenamento, que podem ser aferidas em função da operações de input/output per second (IOPS) e, que nos equipamentos atuais, este indicador alcança até 37.500 iops para os equipamentos EMC VNX (Figura 10) e até 19.000 iops nos equipamentos NetApp (Figura 11). Essas taxas tem trazido lentidão aos sistemas corporativos do órgão, de forma que, tendo em vista os requisitos de aumento de performance desta contratação, as novas soluções de NAS devem trazer modernização tecnológica que proporcione alta performance.

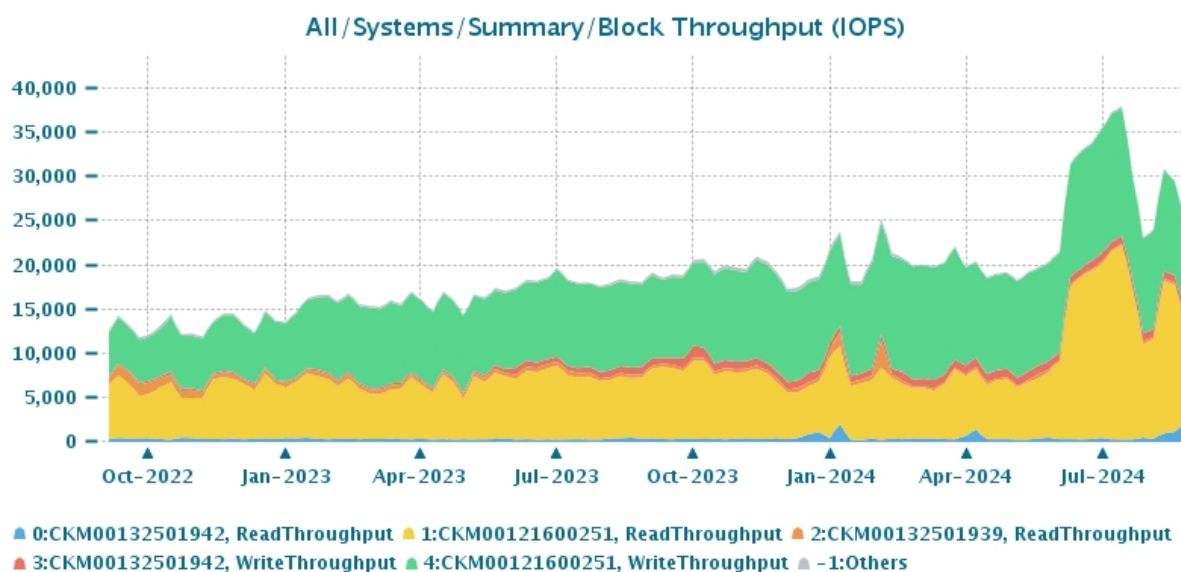


Figura 10 - Histórico da utilização de operações de I/O DELL VNX.

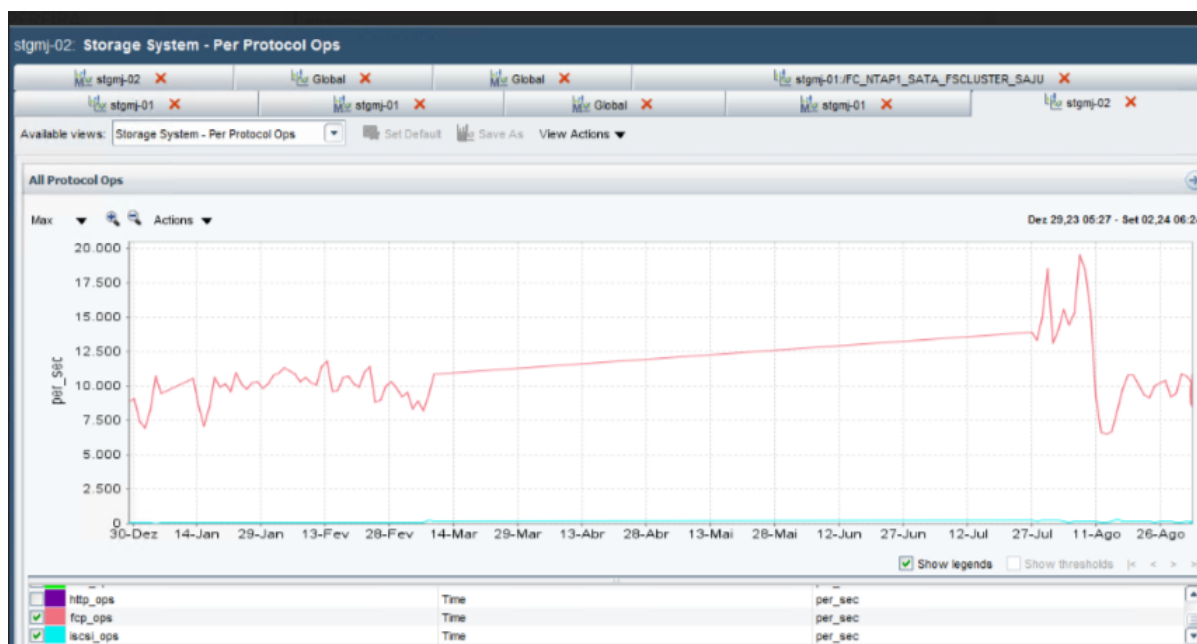


Figura 11 - Histórico da utilização de operações de I/O NetApp FAS.

2.2.2.19. Conforme demonstrado nos tópicos anteriores, é notável que existe uma sobrecarga nos ambientes de armazenamento e backup do Ministério, o que por si só já exige ações efetivas e céleres para que os Data Centers não entrem em colapso, mas não é somente isso. Salienta-se que existem outros fatores críticos que merecem ser destacados, como a defasagem tecnológica, tempo de vida útil e o suporte e garantia dos ativos do ambiente de virtualização, conforme veremos a seguir.

2.2.2.20. **STORAGES** (armazenamento)

2.2.2.20.1. O storage EMC VNX 7500 foi adquirido em 2012 por meio do Contrato 061/2012, estando coberto pelo primeiro contrato de suporte e garantia até o dia 05/11/2018. Já os storages NETAPP FAS 8080 foram adquiridos em 18/12/2014 por meio do Contrato 086/2014, estando coberto pelo primeiro contrato de suporte e garantia até o dia 08/12/2018. Por fim, os storages EMC VNX 5300 foram adquiridos pela SESGE por meio do Contrato MJ /SESGE nº 18/2013, sendo que em um primeiro momento não houve "*interesse operacional na continuação do contrato objeto do presente processo*" por parte da SESGE e, portanto, não houve a renovação da garantia e suporte dos referidos equipamentos.

2.2.2.20.2. Outro ponto que foi analisado, na estratégia de manutenção dos equipamentos, foi a questão do *End Of Life* (fim da vida útil ou descontinuação) por parte dos fabricantes. O EMC VNX 7500 atingiu o *End of Life* em 31/12/2014 e o suporte oficial do fabricante em 31/12/2019. Para o EMC VNX 5300, o *End of Life* finalizou-se 31/12/2014 e o suporte oficial esteve disponível para contratação até o dia 31/12/2020. Quanto ao NetApp FAS 8080, este possuía suporte oficial até dezembro de 2022.

2.2.2.20.3. Tendo em vista criticidade dos equipamentos listados acima, bem como a necessidade de prospectar novas soluções de acordo com as melhores práticas de mercado, optou-se por estender a sobrevida dos equipamentos com contratação de suporte técnico de terceiro para os referidos equipamentos (Data Center Principal e Secundário) por meio do contrato nº 23/2018 (7491436), com vigência expirada, tendo sido substituído no presente ano pelo contrato nº 01/2024 (26698614).

2.2.2.21. **BACKUPS** (cópias de segurança)

2.2.2.21.1. Os *appliances* Symantec NetBackup 5230 foram adquiridos no ano de 2014, por meio do contrato nº 097/2014, e teve como objeto a contratação de empresa especializada no fornecimento de solução de Backup/Restore e deduplicação de dados, em disco. A solução é composta de 02 (dois) *appliances* Symantec NetBackup 5230 (configurados como Media Server) e licença do software NetBackup, por volumetria, (60 TB). A solução foi adquirida com garantia e suporte por 36 (trinta e seis) meses, contados a partir da data do aceite definitivo (25/11/2015) estando coberta pelo suporte e garantia até 25/11/2018.

2.2.2.21.2. Posteriormente, com a finalização do Contrato nº 097/2014, foi feita uma nova licitação para contratação de empresa especializada para prestação de serviços de atualização e sustentação do Software Netbackup e Netbackup Appliance, pelo período de 36 (trinta e seis) meses, contemplando serviço de instalação, configuração, manutenção, garantia e suporte técnico especializado, com a inclusão do licenciamento por socket e diminuição do licenciamento por volumetria (*Front-end terabyte*). Ao optar por este cenário, o Ministério da Justiça e Segurança Pública buscou preservar os investimentos já realizados na atual solução de backup, bem como garantir a continuidade dos sistemas e serviços em produção. Dessa licitação foi gerado o Contrato nº 29/2018, com vigência e suporte finalizados em 28/02/2022.

2.2.2.21.3. Nesse contexto, e com o objetivo de manter todo ciclo de backup coberto por suporte e garantia, foi necessário adquirir uma nova solução de backup de longa retenção, já que a antiga tape library vinha apresentando diversos problemas, além de estar desatualizada tecnologicamente e sem garantia. Na época, optou-se por manter esses backups em tape library, já visando uma contratação conjunta, ao final do Contrato nº 29/2018, que incluísse software gerenciador de backup, *appliance* para armazenamento de curta retenção e longa retenção. Assim, em 13/12/2019, foi firmado o Contrato nº 46/2019, contemplando a aquisição de uma Tape Library e fitas LTO 8, atualmente em funcionamento no Data Center Principal do Ministério.

2.2.2.21.4. A presente contratação em referência, além de prover ambiente de armazenamento de alto desempenho, visa garantir a operação e manutenção de um dos mais importantes sistemas de infraestrutura de TIC do Ministério, relativo à proteção dos dados custodiados, doravante chamado genericamente de backup. O serviço de backup protege os dados e informações corporativas do MJSP, permitindo sua restauração granular. A depender da necessidade e criticidade do sistema ou da informação, os dados devem ser guardados por anos e em diversos locais e meios (discos, nuvem), garantindo que eventuais falhas não implicarão em perda de informação institucional.

2.2.2.21.5. Para atendimento de seus objetivos institucionais, o Ministério da Justiça e Segurança Pública necessita que seus equipamentos tenham recursos de hardware e software suficientes para a plena operação do ambiente produtivo do seus Data Centers, bem como para garantir a continuidade de suas operações em casos de desastres. Esses requisitos têm como objetivo garantir a prestação de serviços com qualidade e dentro dos prazos estabelecidos junto às áreas de negócio do órgão.

2.2.2.21.6. Ainda no contexto da garantia de salvaguarda das informações do MJSP e considerando ainda os mais recentes ataques do tipo *ransomware* e recomendação da consultoria Gartner, é altamente recomendável a utilização de uma solução que possibilite a orquestração da solução de longa retenção de dados (cofre de cibersegurança) de forma independente, conforme informado no documento "*Designing and Implementing a Ransomware Defense Architecture*", publicado em 20/07/2020 e atualizado em 14/02/2022.

"Orchestration technologies can provision an isolated environment that may be suitable for some recovery scenarios, but not all. The most secure would be to house it in a separate environment with dedicated systems and no network access to production. (Página 18)"

"As tecnologias de orquestração podem fornecer um ambiente isolado que pode ser adequado para alguns cenários de recuperação, mas não todos. O mais seguro seria alojá-lo em um ambiente com sistemas dedicados e sem acesso à rede de produção." (Tradução Livre)

2.2.2.21.7. Dessa forma, a contratação em referência inclui, além do backup tradicional, uma solução quem contempla a proteção avançada contra ataques do tipo ransomware.

2.2.2.21.8. Nos últimos cinco anos o número de ataques de *ransomware* aumentou de forma significativa contra as organizações públicas, com uma maior elevação, principalmente, após a pandemia do COVID-19, devido as mudanças dos hábitos dos funcionários dessas organizações e a falta de aparato tecnológico para prevenção e combate a esse tipo de ataque. Apenas para citar os mais relevantes, em 2021, pelo menos quatro instituições públicas sofreram de forma grave com ataques *ransomwares*.

a) TRF-3: O ataque ocorreu em 30 de março. A ação cibercriminosa impediu o uso de alguns equipamentos do tribunal e de "parte de seu ambiente de virtualização", afetando a visualização de processos. Segundo o colegiado, nenhum arquivo chegou a ser deletado.

b) STF: O *ransomware* também foi a principal característica da invasão do Supremo Tribunal Federal, em 5 de agosto de 2021. O acesso a processos e à pauta ficaram fora do ar por seis dias.

c) Ministério da Economia: Em 16 de agosto de 2021, o ataque foi contra o sistema do Tesouro Nacional. Na ocasião, o ministério não informou sobre como os hackers afetaram o sistema e serviços prejudicados.

d) STJ: Em 5 de novembro, foi a vez do Superior Tribunal de Justiça. À época, o tribunal informou que havia backup dos dados sequestrados pelos cibercriminosos.

e) Ministério da Saúde: Ocorrido em 10 dezembro de 2021. A emissão do certificado de vacinação ficou indisponível por dias, pois o ConectSUS foi o principal sistema prejudicado.

2.2.2.21.9. Atualmente a Subsecretaria de Tecnologia da Informação e Comunicação - STI do Ministério é responsável pela guarda de diversos dados sensíveis relacionados às atividades das suas áreas finalísticas, que vão desde o registro de refugiados e informações sobre demandas de consumidores até informações sobre investigações criminais e organizações criminosas.

2.2.2.21.10. De acordo com o Gartner, os ataques de *ransomware* continuam a aumentar globalmente, e os agentes de ameaças por trás deles se tornaram cada vez mais sofisticados em seus métodos. Os profissionais técnicos de segurança e gerenciamento de riscos devem planejar, projetar e implementar uma arquitetura técnica para defender suas organizações.

2.2.2.21.11. Hoje já não é mais suficiente ter somente uma solução de backup tradicional, pois há o risco de a organização estar fazendo cópias de dados criptografados, que não terão nenhuma serventia no caso de um ataque *ransomware*. Nesse sentido, o Gartner recomenda fortemente que as organizações implementem um programa de defesa contra *ransomware* alinhando técnicas preventivas e de detecção aos métodos de ataque usados por grupos de *ransomware*.

2.2.2.21.12. Conforme detalhado na linha do tempo abaixo, em média, um ataque cibernético já estava presente há 100 dias ou mais antes de sua primeira detecção por parte do time de segurança. Isso só reforça a necessidade da existência de uma proteção avançada e preditiva que já possa detectar os primeiros sinais de contaminação antes que os backups possam ser sobrescritos.

Cyberattack Timeline Impact on Backup Systems

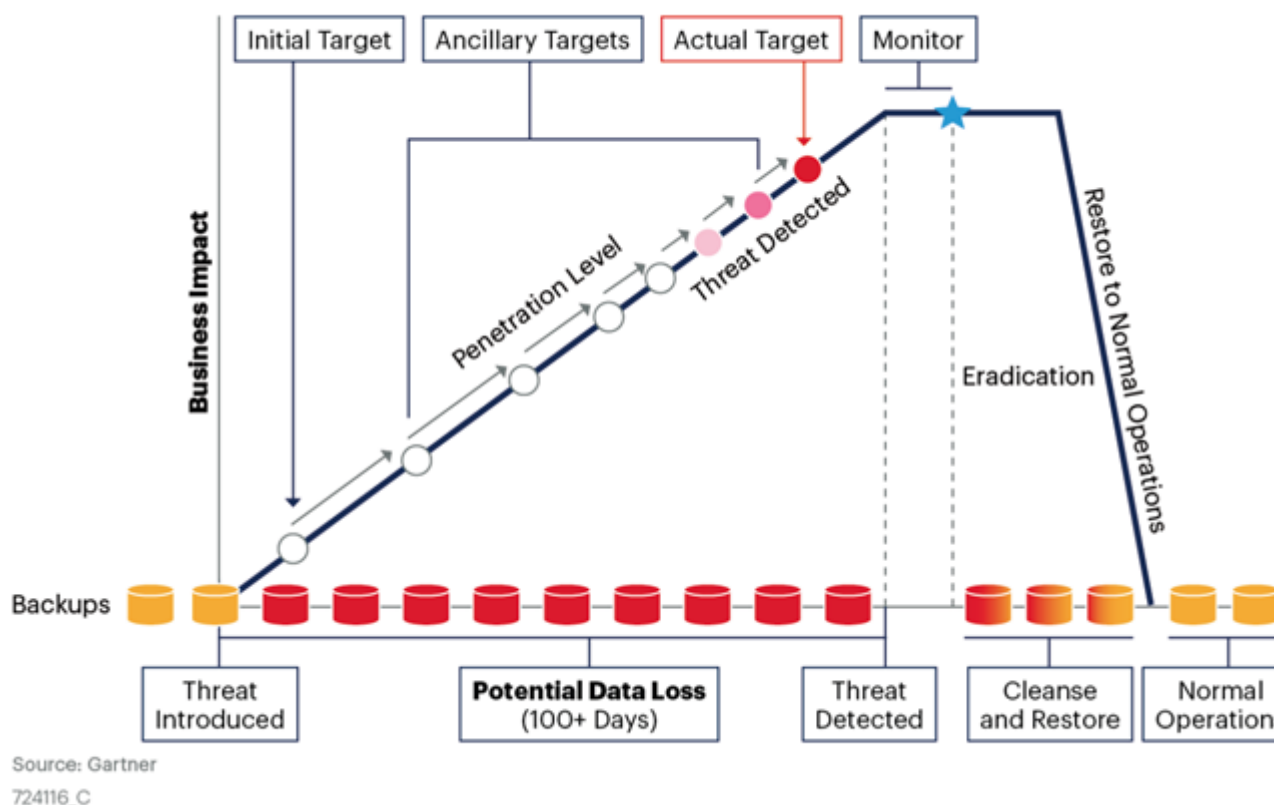


Figura 12 - Impacto da linha do tempo do ataque cibernético nos sistemas de backup.

Fonte: (<https://www.gartner.com/document/3987751>)

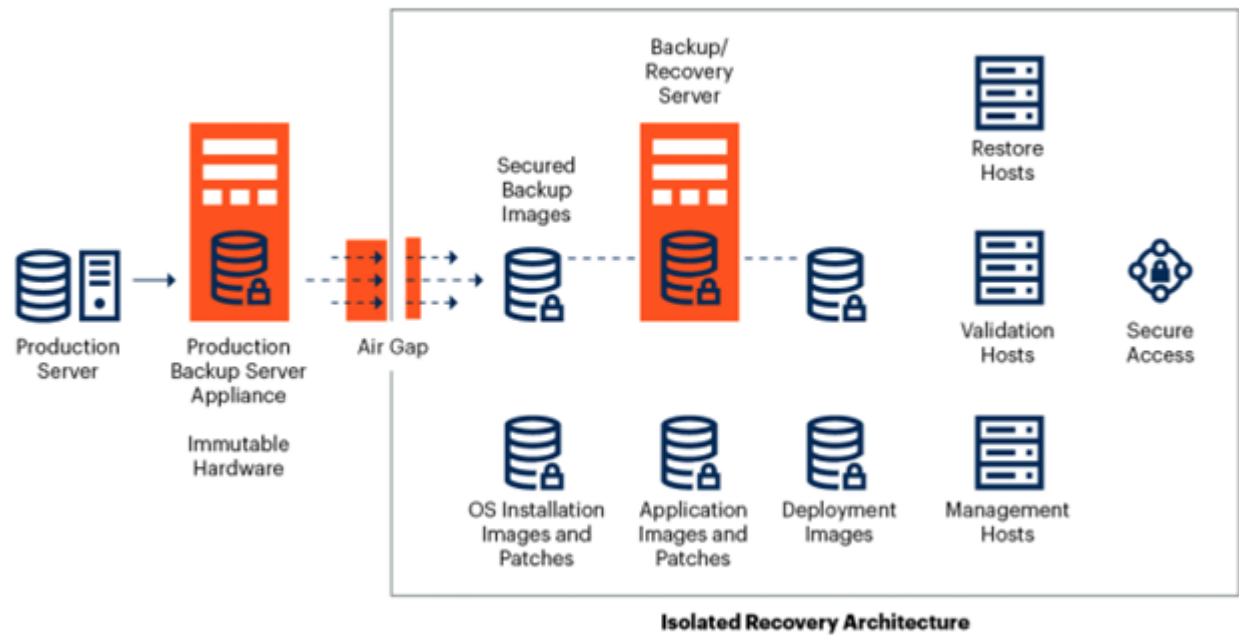
Table 2: Backup Architecture Design Features

Approach ↓	Advantage ↓	Challenges ↓
Air gap with removable media or network disconnect Options include removable media such as tape and hard drives Disk storage subsystems could be utilized, provided an effective network air gap is enabled	Reduces accessibility to attack backup storage	Recovery time objectives need to be carefully analyzed before selecting an air gap medium

Figura 13 - Abordagem para uma arquitetura de backup com segregação de redes.

Fonte: (<https://www.gartner.com/document/3987751>)

Secure Isolated Recovery Environment



Source: Gartner
724116_C

Figura 14 - Ambiente de recuperação isolado e seguro.

Fonte: (<https://www.gartner.com/document/3987751>)

2.2.2.21.13. A premissa mínima para o presente item é a utilização de uma camada extra de proteção, com as seguintes características mínimas:

- a) **Imutabilidade de dados:** consiste em um ambiente de armazenamento de dados com padrões certificados e que garanta, por meio de hardware, a imutabilidade dos backups, impedindo que os dados não sejam excluídos antes de sua expiração programada;
- b) **Air-Gap:** é um método de isolamento do ambiente de armazenamento/backup, que visa garantir a não infecção com dados contaminados. Remete à ideia da existência de uma lacuna entre os ambientes de backup primário e a solução de longa retenção de dados (cofre de cibersegurança imutável). Deverá ser fisicamente isolado e off-line (na maior parte do tempo);
- c) **Dupla Autorização:** garantir que ações críticas que possam comprometer a segurança da solução e dos dados somente sejam aplicadas mediante a aprovação de um segundo usuário, com papel específico de aprovador;

d) **Camada de Inteligência:** Deverá possuir detecção de anomalias de alertar sobre ataques “ransomware” ou outro tipo de ataques cibernéticos, evitando assim que dados comprometidos sejam replicados.

e) **Padrões de Segurança da Informação:** Atendimento aos principais padrões e regulamentos de segurança nacionais e internacionais, a exemplo do FIPS 140-2 e a SEC Rule 17a-4.

2.2.2.21.14. Essas recomendações também estão contidas no documento da consultoria Gartner citado anteriormente.

2.2.2.21.15. Além dos equipamentos da solução de armazenamento e da solução de backup, também fará parte das soluções:

- a) switches, cabos e conectores de rede necessários para interligá-los à LAN dos Data centers do MJSP e à rede de gerenciamento da STI/SE/MJSP;
- b) licenças dos softwares necessárias para a operacionalização dos equipamentos, com o respectivo suporte;
- c) o serviço de instalação de todos os elementos da solução;
- d) o serviço de operação assistida para suporte da solução;
- e) o treinamento das soluções implantadas; e
- e) o serviço especializado sob demanda para aperfeiçoamento da solução.

2.2.2.21.16. Nas próximas seções deste ETP, serão identificadas as principais necessidades de negócio para que se possa alinhar soluções tecnológicas adequadas e eficientes para o perfeito cumprimento dos objetivos estratégicos do Ministério.

3. Necessidades de Negócio

3.1. Conforme previsto no Art. 11, Inciso I da IN SGD/ME nº 94, o Estudo Técnico Preliminar da Contratação deve definir e especificar as necessidades de negócio e tecnológicas, e os requisitos necessários e suficientes à escolha da solução de TIC, contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição.

3.2. Em função disso, **é inegável que a atual situação do Ministério da Justiça e Segurança Pública, carece de atenção** frente à missão institucional a ser cumprida, por meio de seus objetivos estratégicos. Um órgão que possui dimensões consideráveis, bem como competências diretamente relacionadas ao combate ao tráfico de drogas e crimes conexos, corrupção, crime organizado e crimes violentos, lavagem de dinheiro, defesa do consumidor, entre outros, deve **evitar, tratar ou mitigar todos os riscos que possam impactar de alguma forma no desempenho de suas atividades fim**. Ademais, é de amplo conhecimento a necessidade do Governo e de seus executores de políticas públicas, de dispor de soluções de gestão completas e seguras, aptas a oferecer altos níveis de confiabilidade na geração e análise de informações, permitindo assim, soluções rápidas e ações eficientes para a tomada de decisão.

3.3. Principais necessidades de negócio:

- a) Fortalecer o enfrentamento à criminalidade, com enfoque em crimes violentos, organizações criminosas, corrupção e lavagem de dinheiro, inclusive com atuação na faixa de fronteira;
- b) Promover o acesso à justiça e proteger os direitos do cidadão;
- c) Aperfeiçoar a coordenação estratégica e a integração dos órgãos de segurança pública;
- d) Aprimorar e integrar a gestão e a governança institucional;
- e) Fortalecer e ampliar a estrutura e os serviços de TIC;
- f) Ampliar a oferta de serviços públicos digitais;
- g) Garantir a segurança das plataformas de governo digital e de missão crítica;

- h) Otimizar as infraestruturas de tecnologia da informação;
- i) Garantir a salvaguarda das informações do Ministério;
- j) Garantir a infraestrutura e os recursos tecnológicos adequados às atividades do Ministério;
- k) Garantir a disponibilidade e continuidade dos serviços de TIC;
- l) Aumentar o nível de atendimento e qualidade das operações de serviços de TIC;
- m) Aprimorar a gestão de segurança da informação e comunicações;
- n) Atender às disposições contidas no Sistema de Governança do Ministério da Justiça e Segurança Pública (Portaria do Ministro Nº 2/2022);
- o) Fornecer a infraestrutura de armazenamento de dados e de backup para a implantação da infraestrutura de data center hiperconvergente e de nuvem privada do MJSP;
- p) Promover a substituição da solução de armazenamento de dados existente (storages DELL e NetApp);
- q) Promover a modernização tecnológica das soluções de armazenamento de dados dos data centers do MJSP, com ampliação da capacidade de armazenamento de dados e reestruturação de arquitetura para suprir a necessidade atual e futura dos sistemas corporativos hospedados nos ambientes de armazenamento do órgão;
- r) Fornecer solução de backup com melhoria de performance e otimização da execução das rotinas de processamento, armazenamento e recuperação de dados, para que estas sejam executadas no menor tempo hábil possível, gerando interferência mínima nos serviços de TIC disponibilizados;
- s) Prover solução para atendimento à política de backup do órgão, atendendo aos requisitos de retenções exigidos para as cópias de backup, bem como para fins históricos e de auditoria;
- t) Possibilitar a recuperação dos serviços de TIC no menor tempo possível em caso de desastre ou perda de informações;
- u) Prover uma plataforma que viabilize testes de recuperação de dados;
- v) Suprir o término das vigências dos atuais contratos de suporte, garantindo a continuidade nos serviços prestados.

3.4. Funcionalidade

3.3.1. Para a solução de armazenamento de dados a nível de arquivos:

3.3.1.1. Garantir a disponibilidade e o desempenho da infraestrutura de armazenamento de dados da STI/SE/MJSP.

3.3.1.2. Suprir o aumento da demanda de armazenamento dos sistemas corporativos hospedados nos data centers do MJSP, e dos usuários, para os próximos 60 (sessenta) meses.

3.3.1.3. Migrar os dados dos ambientes de armazenamento, que perderam a garantia e suporte, para o novo ambiente de storages, devidamente coberto por garantia e suporte.

3.3.1.4. Suprir às necessidades das secretarias que têm solicitado áreas de armazenamento de dados performáticos e de maior capacidade para acesso e utilização pelas aplicações corporativas, bem como salvaguarda de arquivos para usuários e/ou decorrentes de projetos de segurança pública, dentre outros.

3.3.1.5. Conforme levantamentos realizados, há sistemas corporativos, tal qual o sistema SEI, que demandam acesso a arquivos criados ou gerados por longos períodos de retenção, e devem estar sempre disponíveis para acesso, até que haja políticas específicas para arquivamento desses dados. A partir desta necessidade negocial, vê-se a necessidade de se adquirir solução de armazenamento NAS escalável e integrada à uma solução de armazenamento de objetos, com a finalidade de otimizar os recursos mais nobres e fornecer uma área de armazenamento compatível com os sistemas corporativos do órgão.

3.3.1.6. Prover um ambiente de armazenamento altamente escalável, robusto, de alta disponibilidade e durável, compatível com os novos protocolos.

3.3.1.7. Suprir as necessidades de armazenamento de dados da nova estrutura de nuvem privada do ambiente de tecnologia de informação da STI para os próximos 60 (sessenta) meses.

3.3.2. Para a solução de armazenamento de dados a nível de objetos:

3.3.2.1. Atender às aplicações e sistemas corporativos do MJSP, para fins de armazenamento de dados não estruturados.

3.3.2.2. Prover um ambiente de salvaguarda dos dados de usuários que são pouco acessados (tierização dos dados antigos do NAS), mas que precisam estar disponíveis em tempo real para uso por parte dos usuários. 7.2.3.5.1. Esta “tierização”, além da disponibilidade de novos recursos tecnológicos, objetiva ter ganho no custo da solução considerando que o custo do armazenamento em storage de objetos é significativamente menor do que em um storage NAS.

3.3.2.3. Salvaguardar os dados advindos dos storages NAS para fins de cópia de backup (snapshot).

3.3.2.4. Prover um ambiente de armazenamento altamente escalável, robusto, de alta disponibilidade e durável, compatível com os novos protocolos.

3.3.2.5. Prover ambiente de armazenamento compatível com os protocolos de nuvem, considerando a possibilidade de facilitar a migração dos dados.

3.3.2.6. Suprir as necessidades de armazenamento de dados da nova estrutura de nuvem privada do ambiente de tecnologia de informação da STI para os próximos 60 (sessenta) meses.

3.3.3. Para a solução de backup de dados:

3.3.3.1. Prover recursos de backup automatizado, em intervalos regulares, conforme a política definida pelo MJSP e deve ser possível agendar backups para horários específicos, sem intervenção manual.

3.3.3.2. Prover recuperação rápida de ambientes e dados em caso de falha no sistema ou perda de dados.

3.3.3.3. Prover de recursos de armazenamento eficiente para otimização de cópias de backup, utilizando técnicas como deduplicação e compressão, para economia de espaço em disco e redução de custos de armazenamento.

3.3.3.4 Prover recursos de segurança e criptografia durante a transmissão e o armazenamento, além de possuir mecanismos de resiliência à ataques cibernéticos e de malwares/ransomwares.

3.5. Alinhamento estratégico

3.5.1. Alinhado com o PDTIC 2021-2023, conforme relação abaixo:

Necessidade de TIC	Código da Necessidade	Código da Ação
Solução de armazenamento de dados em storages de rede (NAS /Object Storage) e de backup de dados	N0448	A0553

3.5.2. O objeto da contratação está previsto no Plano de Contratações Anual 2024 MJSP, conforme detalhamento a seguir:

3.5.2.1. **ID PCA no PNCP:** 00394494000136-0-000001/2024;

3.5.2.2. **Data de publicação no PNCP:** 20/05/2023 (Última atualização 05/07/2024);

3.5.2.3. **Id do item no PCA:** 100;

3.5.2.4. **Classe/Grupo:** 7030 - Equipamentos de Armazenamento de Dados;

3.5.2.5. **Identificador da Futura Contratação:** 200005-30/2023.

3.6. Requisitos de capacitação

3.6.1. Para fins de capacitação da equipe, deverá ser contratado serviço de operação assistida após a implantação das soluções de armazenamento e backup. Considerando ser um novo serviço a ser adquirido pela STI/SE/MJSP, o repasse de conhecimento deverá ser realizado pelo fornecedor ou fabricante da solução contratada.

3.7. Requisitos Legais

3.7.1. A contratação deverá atender às determinações da Instrução Normativa SGD /ME nº 94, de 23 de dezembro de 2022, particularmente ao item 4 do Anexo I:

3.1. Os órgãos e entidades que necessitem criar, ampliar ou renovar infraestrutura de centro de dados deverão fazê-lo por meio da contratação de serviços de computação em nuvem, salvo quando demonstrada a inviabilidade em estudo técnico preliminar da contratação. (grifo nosso)

3.2. As contratações de serviços em nuvem devem observar as normas correlatas publicadas pelo Gabinete de Segurança Institucional da Presidência da República - GSI/PR.

3.7.2. No caso da solução de backup, a contratação deverá atender às recomendações do Acórdão TCU 1109/2021:

Acórdão TCU 1109/2021 – PLENÁRIO que recomendou ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), ao Conselho Nacional de Justiça (CNJ) e ao Conselho Nacional do Ministério Público (CNMP), com fundamento no art. 11 da Resolução - TCU 315/2020, que editem normativos para, cada um no seu âmbito de governança, orientar os gestores e regulamentar a obrigatoriedade de que as entidades e órgãos públicos aprovem formalmente e mantenham atualizadas políticas gerais e planos específicos de backup (para suas bases de dados e sistemas críticos, por exemplo), contemplando requisitos mínimos para endereçar os cinco subcontroles do controle 10 (Data Recovery Capabilities) do framework preconizado pelo Center for Internet Security (CIS), em especial quanto à definição do escopo dos dados a serem copiados, suas respectivas periodicidades, tipos, quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos de segurança.

3.8. Requisitos de Manutenção

3.8.1. Todos os equipamentos e devem possuir garantia softwares e suporte ao longo de sua vida útil para manutenções corretivas.

3.8.2. Deverá ser contratada horas de suporte especializado para implantação das soluções, considerando ser um serviço novo cuja expertise ainda não foi adquirida pelos analistas que sustentam o ambiente da STI/SE/MJSP. Estas horas serão necessárias para implantação de projetos em curso e novos projetos.

3.9. Requisitos Temporais

3.9.1. A CONTRATADA deverá entregar os equipamentos em até 60 (sessenta) dias contados da data da ordem de fornecimento de bens ou serviços (OFB/OS).

3.10. Requisitos de Segurança e Privacidade

3.10.1. Todas as informações obtidas ou extraídas pela CONTRATADA deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros. A CONTRATADA deve zelar por si e por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos e especificações técnicas e comerciais aos quais eventualmente tenham conhecimento ou acesso.

3.11. Requisitos Sociais, ambientais e culturais

3.11.1. Só será admitida a oferta de ativos que cumpram os critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos na Portaria nº 170 de 2012 do INMETRO.

3.11.2. O atendimento da CONTRATADA deverá ser preferencialmente em língua portuguesa do Brasil. Se não for possível, deverá ser em língua inglesa dos Estados Unidos.

3.11.3. Aplica-se, no que couber, os regramentos do Decreto nº 11.785/2023, que Institui o Programa Federal de Ações Afirmativas - PFAA, com a finalidade de promover direitos e a equiparação de oportunidades por meio de ações afirmativas destinadas às populações negra, quilombola e indígena, às pessoas com deficiência e às mulheres, consideradas as suas especificidades e diversidades.

4. Área requisitante

Área Requisitante	Responsável
MJSP/SE/STI/CGISE	Leonardo Garcia Greco

5. Necessidades Tecnológicas

5.1. Conforme detalhamento dos ambientes e soluções, com suas respectivas capacidades, apresentados nos tópicos anteriores, é notável que os recursos estão acima do nível de saturação seguro, tanto na parte de armazenamento, como de backup. Outro fator a ser considerado, é a coexistência entre ambientes *on-premises* e *on-cloud*, que demandam perfeita integração e gerência, as quais devem ser orientadas a serviço e não somente a ativos de infraestrutura.

5.2. Diante do crescimento expressivo no consumo de recursos nos últimos quatro anos (Figura 9, tais como utilização de disco, consumo de armazenamento de backup, e em virtude da alta demanda de recursos de TIC pelas áreas de negócio para atendimento de seus projetos estratégicos, além da defasagem tecnológica, tempo de vida útil e o suporte e garantia dos ativos do ambiente de armazenamento e backup, torna-se imprescindível a adoção de medidas céleres e efetivas, que atenda minimamente os seguintes requisitos:

- a) Reestruturação do ambiente de armazenamento e backup dos Data Centers do Ministério adequando suas capacidades e desempenho às demandas atuais das áreas de negócio, bem como projeções futuras;
- b) Aquisição de solução NAS (*Network Attached Storage*) para armazenamento e compartilhamento de arquivos;
- c) Aquisição de solução armazenamento baseado em objetos para proteção da solução NAS e hospedagem de dados de aplicações;
- d) Implantação de uma nuvem privada *on-premises* de alto desempenho, viabilizando a integração tanto com o Data Center secundário, quando com as nuvens públicas já em operação (Azure e Oracle);
- e) Implantação de alta disponibilidade entre os dois Data Centers, de forma que as aplicações críticas possam ser replicadas em caso de *Disaster Recovery*;
- f) Reestruturação das camadas de backups;
- g) Integração plena da ferramenta de backup e de recuperação de dados com os SGBD em utilização no MJSP, tais como: Oracle, MySQL/Percona, PostgreSQL, MongoDB e SQL Server;
- h) Deve realizar operações de backup de sistemas de arquivo de servidores virtuais (VMs) sem a necessidade de instalação de agentes nos próprios servidores virtuais;
- i) A solução de backup deverá prover *air-gap* com segregação de rede e orquestração por solução independente.

5.3. A reestruturação necessária, deve possibilitar a implementação de ambientes com alta disponibilidade e que consigam proporcionar uma imagem fiel e em tempo real do panorama local e global dos eventos e dos recursos envolvidos nas operações e incidentes relacionados à segurança pública, defesa civil, defesa do consumidor, segurança privada e mobilidade urbana, entre outros, a fim de embasar a tomada de decisão por parte de todas as instituições envolvidas.

5.4. De arquitetura tecnológica

5.4.1. A infraestrutura de armazenamento da STI/SE/MJSP é composta no data center principal por 3 equipamentos de storages, sendo 01 equipamento EMC VNX 7500 e 02 equipamentos NetApp FAS8080, e no data center secundário, por 2 equipamentos DELL VNX 5300. Os equipamentos são responsáveis por fornecer a infraestrutura de armazenamento em bloco e arquivos. O equipamento DELL EMC VNX 7500 possui capacidade líquida aproximada de 296 TB (Terabytes e os equipamentos NetApp FAS8080, de 479,91 TB (Terabytes).

5.4.2. Neste planejamento de contratação objetiva-se focar em um ambiente de armazenamento com níveis segmentados, de acordo com sua funcionalidade, a fim de atender as demandas do MJSP e da nova infraestrutura de hiperconvergência a ser contratada, considerando a melhor utilização dos recursos de armazenamento atuais a partir do uso otimizado de uma solução mais nobre, storage NAS, para uma solução menos onerosa, storage de objetos.

5.4.2.1. Esta EPC entende que é mais vantajoso substituir a solução de armazenamento atualmente implantada, pois, além da falta de capacidade do hardware atualmente implantado, qual seja, 3 (três) sistemas de armazenamento, sem suporte e garantia do fabricante, conforme end-of-support abaixo, apenas suporte de serviços de terceiros:

DELL EMC VNC 7500 - 31 / 12 /2019;
DELL EMC VNX 5300 - 31 / 12 /2020;
NEAPP FAS 8080 - 31 / 01 /2023;

5.4.3. Os NetApp FAS8080 são storages *mid-range* atualmente usados tanto na rede NAS como na rede SAN. Estão com taxa de ocupação acima de 80% do espaço disponível. Os storages DELL EMC também apresentam espaço livre abaixo de 20%.

5.4.5. Para o dimensionamento do ambiente de NAS, que será pormenorizado na seção 7, utilizou-se o histórico de aquisição e uso dos equipamentos e os dados armazenados obtidos a partir da ferramenta da DELL liveoptics.

5.4.7. A Solução de Armazenamento de Objetos deverá contemplar:

5.4.7.1. Retenção dos backups superiores à 2 anos;

5.4.7.1. Salvaguarda dos arquivos mortos e sem uso nos storages NAS desta STI/SE/MJSP.

5.4.8. Para tanto, a Solução de Armazenamento de Objetos deverá:

5.4.8.1. Possuir uma arquitetura escalável, scale-out;

5.4.8.2. Possuir recursos de proteção dos dados à ataques do tipo ransomware;

5.4.8.3. Ser compatível com o protocolo de nuvem S3, com sincronização nativa para os grandes fornecedores de nuvem do mercado (Amazon, Google e Microsoft);

5.4.8.4. Possuir criptografia em disco para salvaguarda dos dados;

5.4.8.5. Possuir desempenho de alta performance para os storages NAS;

5.4.8.6. Possuir integração nativa com storage NAS para “tierização” entre os sistemas e armazenamento.

5.4.9. A CONTRATADA deverá prover todos os componentes de software bem como os componentes de hardware – armazenamento, processamento e conectividade – que constituem a Solução, necessários ao cumprimento dos requisitos técnicos.

5.4.10. Todos os equipamentos fornecidos não deverão constar, na data de apresentação de propostas na respectiva fase licitatória, na lista de end-of-sale e end-of-support do seu fabricante, inclusive os ativos de conectividade.

5.4.11. Será necessário o fornecimento de suporte especializado considerando que todas as soluções são novas para a equipe técnica da STI/SE/MJSP, onde haverá a necessidade de horas do fabricante/fornecedor da solução para fins de planejamento e implantação dos novos projetos.

5.4.12. Será necessário que a solução seja facilmente expandida, sem a interrupção dos serviços e sem perda de desempenho, que forneça recursos internos de redundância, além daquela fornecida por RAID, de forma distribuída pelos nós, prevenindo redução de perda de dados e interrupção por falha no hardware. Devido estas necessidades, a solução deverá ser do tipo *scale-out*.

5.5. Solução de armazenamento NAS (Network Access Storage)

5.5.1. Deverá usar a arquitetura do tipo *scale-out*.

5.5.6. Possuir capacidade de sistema de armazenamento de dados escalável NAS com base no levantamento realizado na sessão 7, sem considerar ganhos com deduplicação e compressão de dados especializada para o armazenamento de documentos digitais com formato não estruturado.

5.5.3. O Chassi deverá operar com pelo menos 2 (duas) fontes de energia redundantes e independentes, do tipo “*hot swap*”, que possibilite o funcionamento normal dos módulos, sem prejuízo de nenhuma funcionalidade, no caso de uma das fontes de alimentação manifestar algum tipo de falha.

5.5.4. Cada módulo deverá possuir processador, memória e portas de comunicação suficientes para atender os requisitos de desempenho necessários para o correto funcionamento da solução, com *throughput* mínimo de leitura para SMB e NFS compatíveis com o ambiente atual do MJSP.

5.5.5. A solução deve ser baseada em linha exclusiva com tecnologia de discos NVMe.

5.5.6. Deve suportar escalabilidade até 24 controladoras, para os fins de expansão da solução.

5.5.7. Deve suportar tecnologia *NFS over RDMA* para os fins performance de comunicação de dados.

5.5.8. Cada módulo deverá possuir processador, memória e portas de comunicação suficientes para atender os requisitos de desempenho necessários para o correto funcionamento da solução, com *throughput* mínimo de leitura para SMB e NFS compatíveis com o ambiente atual do MJSP.

5.5.9. O equipamento deve ser fornecido de linha exclusiva para discos all-flash, com suporte à tecnologia NVMe.

5.5.10. A solução deverá contemplar o licenciamento de software para atender, pelo menos, as seguintes funcionalidades:

5.5.10.1. Monitoração;

5.5.10.2. Funcionalidade de gerenciamento e balanceamento de conexões;

5.5.10.3. Gerenciamento e assinalamento de cotas de utilização por usuário, grupo, diretório e subdiretórios;

5.5.10.4. Gerenciamento de snapshots;

5.5.10.5. Gerenciamento de replicação;

5.5.10.6. Gerenciamento de “tierização” (inclusive com storage de objetos);

5.5.10.7. Funcionalidade de deduplicação.

5.5.11. A solução deverá possuir, ao menos, os seguintes protocolos acesso: NFS, SMB e FTP;

5.5.12. A solução deverá possuir suporte mínimo ao protocolo S3;

5.5.13. A solução de armazenamento deverá se conectar à rede do MJSP por meio de interfaces de rede compatíveis com o ambiente atual.

5.5.13.1. Deverá ser fornecido junto à solução todos os equipamentos e dispositivos de rede e conectividade, inclusive cabos e *transceivers*. A contratada deverá compor a solução de storage de forma a suportar as métricas de desempenho que compõem o estudo, devem se conectar de forma redundante à rede do MJSP por meio de fibra óptica, padrão ethernet.

5.5.13.2. Tanto as portas das interfaces quanto os respectivos transceivers devem realizar adaptação automática (autonegociação) da banda de transmissão de acordo com a infraestrutura de conexão.

5.5.14. O produto ofertado deverá suportar todos os protocolos descritos e funcionalidades de forma global como um produto único, não sendo permitida composição de produtos para entrega da solução.

5.5.14.1. A solução não deve ser baseada em virtualização de subsistemas, ou sistemas de soluções *Software Defined Storage* que sejam compostas por hardwares e/ou softwares commodity;

5.5.14.2. O sistema operacional dos módulos/nós do sistema de armazenamento scale-out deverá ser nativo do produto, do mesmo fabricante do hardware, não se permitindo as modalidades OEM de sistemas operacionais de

propósito geral, baseado em Windows ou Unix/Linux e suas variações, exceto se completamente customizado e suportado integralmente pelo fabricante da solução.

5.5.14.3. A solução não deve ser baseada em gateways genéricos, baseados em servidores de rack comuns ou que não sejam de propósito específico.

5.5.15. A solução deverá fornecer console de monitoração e gerenciamento acessível via interface WEB(GUI) HTTPS e linha de comando (CLI ssh), que permita executar todas as funções de configuração e monitoração da solução.

5.6. Solução de armazenamento de objetos (Object Storage)

5.6.1. Deverá usar a arquitetura do tipo *scale-out*.

5.6.2 Possuir capacidade líquida de armazenamento definida na seção 7.

5.6.3. A capacidade entregue no cluster deverá ser expansível a, no mínimo, 30% da capacidade dimensionada inicialmente. A expansão para atingir essa capacidade deve ocorrer de forma não disruptiva, isto é, sem interrupção das operações de I/O das aplicações que estão acessando a solução.

5.6.4. Ser dimensionada para comportar objetos de 1MB cada, a partir do dimensionamento previsto na seção 7.

5.6.5. Deverá garantir que os objetos armazenados continuem acessíveis em caso de falha/perda de qualquer um dos componentes da solução, independentemente da funcionalidade de replicação.

5.6.6. Deverá prover acesso rápido aos objetos, garantindo autenticidade, imutabilidade, unicidade e disponibilidade, durante o período de retenção configurado, além de ser transparente quanto ao local de armazenamento (*Global Namespace*) para aplicações e usuários.

5.6.7. Deverá possuir capacidade para armazenar dados não estruturados (arquivos em geral como: XML, PDF, TXT, Microsoft Office, OpenOffice, databases SQL, mailbox Exchange, arquivos de máquinas virtuais, arquivos de sistema operacional Linux, etc.) e seus metadados, inclusive customizados, que devem conter informações relativas a um único objeto.

5.6.8. Deverá possuir, de forma nativa, as seguintes capacidades de proteção:

5.6.8.1. Permitir automaticamente que um objeto original possua múltiplas cópias, de forma que cada cópia seja armazenada em servidores e discos diferentes do objeto original;

5.6.8.2. Recuperar de forma automática um objeto original;

5.6.8.3. Fazer replicação e recuperação de forma automática de objetos entre soluções geograficamente distantes, sem envolvimento de aplicações e sem limites de distância.

5.6.9. Deverá possuir de forma nativa as seguintes capacidades de segurança:

5.6.9.1. Garantir de forma automática que um objeto original não seja alterado ou corrompido durante o período de retenção configurado, através de sua própria assinatura digital.

5.6.9.1.1 No caso de alteração do objeto original, a solução deverá recalcular a assinatura digital e tratá-lo como um novo objeto no sistema, não alterando nenhuma referência ou política do objeto original.

5.6.9.1.2 No caso de corrupção do objeto original, a solução deverá descartá-lo e fazer uma nova cópia a partir de uma cópia autêntica do objeto original, gerada pela política de proteção.

5.6.9.2. Garantir que um objeto não seja acessado por usuário ou aplicação não autorizados.

5.6.10. Deverá possuir de forma nativa os seguintes controles de retenção:

5.6.10.1 Após a configuração do período de retenção de um objeto, a solução não deverá permitir que este seja alterado ou apagado, até que o tempo de retenção configurado tenha expirado;

5.6.10.2 Uma vez configurado o tempo de retenção de um objeto, a solução não deverá permitir a reconfiguração do período de retenção para menos, mas deverá permitir que o período de retenção seja aumentado;

- 5.6.10.3. O prazo de retenção deverá ser atribuído a cada objeto armazenado, ou a uma classe de retenção ao qual o objeto esteja associado.
- 5.6.10.4. Possuir funcionalidade que permita que os objetos sejam mantidos mesmo após a expiração do seu prazo de retenção;
- 5.6.10.5. Permitir definição do tempo de retenção de, no mínimo, 25 (vinte e cinco) anos.
- 5.6.11. Deverá prover de forma nativa as seguintes funcionalidades no momento de deleção de um objeto:
- 5.6.11.1. Permitir que um objeto seja apagado somente após o tempo de retenção ter expirado;
- 5.6.11.2. Permitir que um objeto seja apagado fisicamente após a expiração do período de retenção.
- 5.6.12. O produto ofertado deverá suportar todos os protocolos descritos e funcionalidades de forma global como um produto único, não sendo permitido composição de produtos para entrega da solução.
- 5.6.12.1. As soluções não devem ser baseadas em virtualização de subsistemas, ou sistemas de soluções *Software Defined Storage* que sejam compostas por hardwares e/ou softwares commodity;
- 5.6.12.2. O sistema operacional dos módulos/nós do sistema de armazenamento scale-out deverá ser nativo do produto, do mesmo fabricante do hardware, não se permitindo as modalidades OEM de sistemas operacionais de propósito geral, baseado em Windows ou Unix/Linux e suas variações, exceto se completamente customizado e suportado integralmente pelo fabricante da solução.
- 5.6.12.3. As soluções não devem ser baseadas em softwares de clusterização de mercado, como Veritas Cluster, Microsoft cluster, Ceph Community, Minio ou similares;
- 5.6.12.4. As soluções não devem ser baseadas em gateways genéricos, baseados em servidores de rack comuns ou que não sejam de propósito específico.
- 5.6.13. A solução deverá fornecer console de monitoração e gerenciamento acessível via interface WEB(GUI) HTTPS e linha de comando (CLI ssh), que permita executar todas as funções de configuração e monitoração da solução.
- 5.6.14. O cluster deve incluir todos os ativos de rede necessários para sua instalação, com cabos de conectividade (inclusive cabos de fibra e UTP), switches de gerenciamento, switches de frontend e backend, outros componentes de hardware, incluindo racks para instalação dos equipamentos, conectores, transceivers, PDU's e demais componentes necessários para seu perfeito funcionamento.
- 5.6.15. A solução de armazenamento deverá se conectar à rede do MJSP por meio de interfaces de rede compatíveis com o ambiente.
- 5.6.15.1. Deverá ser fornecido junto à solução todos os equipamentos e dispositivos de rede e conectividade. A contratada deverá compor a solução de storage de forma a suportar as métricas de desempenho que compõem o estudo, devem se conectar de forma redundante à rede do MJSP por meio de fibra óptica, padrão ethernet.
- 5.6.16. Tanto as portas das interfaces quanto os respectivos transceivers devem realizar adaptação automática (autonegociação) da banda de transmissão de acordo com a infraestrutura de conexão.
- 5.6.17. Os canais de e de replicação entre sites (primário frontend e contingência) deverão possuir capacidade para criação de caminhos redundantes para conexão com dispositivos ligados à rede do MJSP.
- 5.6.18. Deverá garantir que um objeto seja único no sistema.
- 5.6.19. Deverá implementar protocolos de acesso seguro.
- 5.6.20. Permitir que a aplicação efetue pesquisa de objetos através de índices específicos configurados pela própria aplicação, definindo campos-chave e/ou através da indexação dos objetos.
- 5.6.21. Permitir que as aplicações clientes executem operações com as seguintes finalidades: leitura, gravação, deleção, configuração de retenção, busca e recuperação de objetos.
- 5.6.22. Possuir interface com as aplicações através do protocolo S3.

5.6.23. Possuir compatibilidade com os protocolos HTTP/HTTPS-RestAPI, CIFS, NFS e S3, para ingestão e recuperação de objetos.

5.6.24. A solução deverá permitir a reutilização do espaço liberado para otimizar os recursos de armazenamento.

5.6.25. A solução deve possuir a capacidade de gerenciar cotas de armazenamento definidas por políticas determinadas pelo administrador, aplicáveis no tenant/namespace ou por usuário. A implementação de quotas deve permitir a monitoração de sua utilização, garantindo que não sejam ultrapassados os limites determinados.

5.6.26. Deve possuir funcionalidade de criptografia de dados, com criptografia habilitada para todos os dados armazenados.

5.6.27. Deverá implementar mecanismos de replicação entre 2 (dois) ou mais sites em modalidade assíncrona. Todos os componentes de hardware e software necessários para utilização da funcionalidade deverão ser oferecidos.

5.6.28. Para a replicação assíncrona definida no item anterior, a solução deve permitir a seleção por grupos e/ou individualmente de buckets e objetos.

5.6.29. O acesso aos objetos via protocolo S3, assegurado o uso de todas as funcionalidades solicitadas, deve ser suportado pelo fabricante da solução para operação com softwares de backup do mercado.

5.6.30. O chassi/controladora deverá operar com pelo menos 2 (duas) fontes de energia redundantes e independentes, do tipo “hot swap”, que possibilite o funcionamento normal dos módulos, sem prejuízo de nenhuma funcionalidade, no caso de uma das fontes de alimentação manifestar algum tipo de falha.

5.6.31. A solução deverá contemplar o licenciamento de software para atender, ao menos, as seguintes funcionalidades:

5.6.31.1. Monitoração;

5.6.31.2. Funcionalidade de gerenciamento e balanceamento de conexões;

5.6.31.3. Gerenciamento e assinalamento de buckets;

5.6.31.4. Gerenciamento de replicação;

5.6.31.5. Funcionalidade WORM (*Write Once Read Many*) ou recurso equivalente;

5.6.31.6. Funcionalidade de proteção contra ransomware;

5.6.31.7. Funcionalidade de criptografia.

5.7. Replicação do storage NAS e de objetos

5.7.1. Para fins de salvaguarda dos dados que serão armazenados no storage NAS e de objetos, far-se-á necessário replicar os dados para uma solução de armazenamento no data center de contingência.

5.7.2. O cluster que receberá a replicação deverá incluir todos os ativos de rede necessários para conectividade (inclusive cabos de fibra e UTP), switches de gerenciamento, switches de frontend e backend, outros componentes de hardware, conectores, transceivers, PDU's e demais componentes necessários para seu perfeito funcionamento.

5.7.3. A solução de armazenamento da réplica deverá se conectar à rede do MJSP por meio de interfaces de rede compatíveis com o ambiente.

5.7.3.1. A solução deverá ser conectada à rede do MJSP e a contratada deverá compor a solução de armazenamento de forma a suportar as métricas de desempenho que compõem o estudo, não sendo inferior a 10 Gbps, e devem se conectar de forma redundante à rede do MJSP.

5.7.4. Os canais de replicação entre sites (primário e contingência) deverão possuir capacidade para criação de caminhos redundantes para conexão com dispositivos ligados à rede do MJSP.

5.7.5. Os dados a serem replicados serão aqueles exclusivamente armazenados no storage NAS primário e storage de objetos referente aos itens 1 e 5 e serão dimensionados na seção 7.

5.7.6. Replicação do storage de objetos

5.7.6.1. No caso do storage de objetos, a replicação pode ser realizada de forma síncrona e/ou assíncrona e a solução deve permitir a seleção por grupos e/ou individualmente de buckets e objetos.

5.7.6.2. Possuir compatibilidade e interface com o protocolo de nuvem S3, para ingestão e recuperação de objetos.

5.7.6.3. O acesso aos objetos via protocolo S3, assegurado o uso de todas as funcionalidades solicitadas, deve ser suportado pelo fabricante da solução para operação com softwares de backup do mercado.

5.7.6.4. Os dados replicados poderão ser salvaguardados apenas para cópias de segurança, não precisando ser acessados imediatamente quando solicitados. É compatível com este requisito o armazenamento do tipo cold storage, quando os dados solicitados podem ser entregues pela solução até 48hs após solicitados.

5.7.6.5. Deverá garantir que os objetos armazenados continuem acessíveis em caso de falha/perda de qualquer um dos componentes da solução.

5.7.6.6. Deverá prover acesso aos objetos garantindo autenticidade, imutabilidade, unicidade e disponibilidade, durante o período de retenção configurado, além de ser transparente quanto ao local de armazenamento (*Global Namespace*) para aplicações e usuários.

5.7.6.7. Deverá garantir que um objeto seja único no sistema.

5.7.6.8. Deverá implementar protocolos de acesso seguro.

5.7.6.9. Permitir que a aplicação efetue pesquisa de objetos através de índices específicos configurados pela própria aplicação, definindo campos-chave e/ou através da indexação completa dos objetos.

5.7.6.10. Permitir que as aplicações clientes executem operações com as seguintes finalidades: leitura, gravação, deleção, configuração de retenção, busca e recuperação de objetos.

5.8. Solução de Backup de Dados

5.8.1. Fornecer solução de backup e replicação de dados com suporte técnico e atualização do fabricante pelo período mínimo de 5 anos.

5.8.2. A CONTRATADA será responsável pela instalação, parametrização e de instalação dos recursos de hardware e software necessários à implementação da solução de backup.

5.8.3. Garantir solução tecnológica de Backup para ambiente de virtualização de servidores e para o ambiente de máquinas físicas (banco de dados Oracle e PostgreSQL, monitoração, etc).

5.8.4. As cópias de segurança deverão ser realizadas por meio de softwares corporativos que permitam manter e gerenciar as cópias de segurança dos arquivos e conteúdo de bases de dados, garantindo a disponibilidade e a acessibilidade das cópias feitas para propósitos de recuperação e para armazenamento de longo prazo.

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

5.8.6. Deverá garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através da solução de virtualização escolhida (Vmware).

5.8.7. Não deverá necessitar de instalação manual de agentes em ambientes virtualizados para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais, em ambientes virtualizados.

5.8.8. Deverá proteger o ambiente, sem interromper a atividade das máquinas virtuais, facilitando as tarefas de proteção (backup), replicação e restauração em conjunto.

5.8.9. Deverá ter a capacidade de testar a consistência do backup e replicação (S.O., aplicação, VM).

5.8.10. Deverá prover a deduplicação e compressão durante a operação de qualquer backup.

5.8.11. Deverá possibilitar a cópia de uma máquina virtual completa ou discos virtuais específicos.

5.8.12. Deverá ter a capacidade de integração através de API's dos fabricantes de infraestrutura virtualizada para a proteção de dados.

- 5.8.13. Deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (backup) a saber:
- 5.8.13.1. Diretamente através de Storage Area Network (SAN)
 - 5.8.13.2. Diretamente do storage, através do hypervisor I/O (Virtual Appliance);
 - 5.8.13.3. Mediante uso da rede local (LAN);
- 5.8.14. Deverá possibilitar o acesso ao conteúdo dos backups/réplicas para recuperação de arquivos, pastas ou anexos, diretamente do backup ou réplica de backup, sem a necessidade de recuperar completamente o backup e inicializar.
- 5.8.15. Deverá permitir a recuperação de mais de uma máquina virtual de forma simultânea, permitindo assim, agilizar a recuperação em casos de desastres.
- 5.8.16. Todo serviço de migração das máquinas virtuais do repositório de backup até o armazenamento na produção restabelecida não deverá afetar a disponibilidade e acesso pelo usuário, sem paradas atendendo VMware;
- 5.8.17. Deverá permitir realizar a truncagem de logs transacionais (*transaction logs*) para máquinas virtuais com SQL Server e Oracle;
- 5.8.18. Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos;
- 5.8.19. Deverá permitir recuperar, no nível de objetos, utilizando as ferramentas de gestão das aplicações existentes;
- 5.8.20. Deverá incluir ferramentas de recuperação para os servidores informados nos subitens abaixo, permitindo o gerenciamento específico do backup e restore, com ou sem a instalação de agentes específicos:
- 5.8.21. Microsoft Active Directory 2012 ou superior, possibilitando recuperar objetos individuais, no mínimo: usuários, recuperação de senhas de usuários e computadores, grupos, contas;
- 5.8.22. Microsoft SQL Server 2019 ou superior, possibilitando recuperar objetos individuais, no mínimo: bases de dados e tabelas;
- 5.8.23. Deverá suportar o backup consistente de bancos de dados PostgreSQL por meio do uso de agentes, sendo também aceitável a utilização de scripts pré/pós-backup para essa finalidade;
- 5.8.24. Deverá ser possível executar uma ou várias máquinas virtuais a partir do arquivo de backup, em um ambiente isolado, sem a necessidade de espaço de armazenamento adicional e sem modificar os arquivos de backup (read-only), para criação de ambiente de homologação, teste, etc;
- 5.8.25. Deverá oferecer arquivamento em fita, suportando VTL (*Virtual Tape Libraries*), biblioteca de fitas e drives LTO-7 ou superior.
- 5.8.26. Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção;
- 5.8.27. Deverá incluir um plug-in para VMware vSphere Web Client, a fim de permitir o monitoramento da infraestrutura de backup diretamente da console de gerência do ambiente VMware, com visibilidade detalhada e geral do estado dos trabalhos e recursos de backup;
- 5.8.28. Deverá operar em ambientes virtualizados através das soluções da VMware, incluído: VMware vSphere 5.5 e superiores.
- 5.8.29. Deverá ser capaz de realizar réplicas em outros sites ou infra estruturas a partir dos backups realizados;
- 5.8.30. Deverá permitir parametrizar o uso de recursos computacionais, de forma que se possa diminuir o impacto na infraestrutura de produção, durante as atividades de backup;
- 5.8.31. Deverá oferecer a possibilidade de armazenar os arquivos de backup de forma criptografada, com algoritmo mínimo de 256 bits, ativando e desativando tal operação, assim como assegurar o trânsito da informação através desse cenário;

5.8.32. Deverá permitir a criação de níveis de delegação de tarefas (perfis) de recuperação no nível de elementos da aplicação, inclusive para outros usuários, de forma a diminuir a carga de atividades executadas pelo administrador da plataforma;

5.8.33. Na console da ferramenta deverá ser possível visualizar todos os Jobs de backup e visualizar os objetos protegidos;

5.8.34. Deve suportar múltiplas operações dos componentes/servidores participantes da estrutura de backup, permitindo atividades de backup e recuperação simultâneas;

5.8.35. Garantir que as cópias de segurança (backups) sejam apropriadamente protegidas por meio de segurança física ou criptografia quando forem armazenadas, assim como quando são movimentadas através da rede. Isso inclui cópias de segurança (backups) remotas e em serviços de nuvem.

5.8.36. Deve ser ofertada a versão mais atual do software de backup, liberada oficialmente pelo fabricante do software.

5.8.37. As licenças devem ser do tipo perpétuas.

5.8.37.1. Será admitida licenças por subscrição, desde que as funcionalidades principais da solução de backup permaneçam funcionais após o fim do suporte e garantia.

5.8.38. Todos os softwares deverão estar cobertos pela manutenção de software, para que possa receber atualizações e suporte.

5.9. Serviço de Operação Assistida

5.9.1. O Serviço de operação assistida consiste no apoio à operação e monitoramento das soluções, replicação dos dados entre data centers, bem como a transferência contínua de conhecimento especializado da CONTRATADA à equipe do MJSP;

5.9.2. Abrange as seguintes atividades:

5.9.2.1. Auxiliar a STI/SE/MJSP na formulação da customização e parametrização do ambiente de produção, de acordo com as diretrizes e necessidades do MJSP;

5.9.2.2. Apoiar o monitoramento dos eventos gerados pelos módulos de administração e gerenciamento da Solução;

5.9.2.3. Apoiar o monitoramento de alertas dos módulos de administração e gerenciamento da Solução;

5.9.2.4. Propor novas configurações e ajustes para refinar e melhorar o processo de administração e gerenciamento da Solução;

5.9.2.5. Realizar e orientar testes de novas versões do software de Gerenciamento da Solução;

5.9.2.6. Apoiar na geração de informações para a gestão da capacidade e do desempenho.

5.9.3. Este serviço será utilizado sob demanda, aprovada por Ordem de Serviço (OS).

5.10. Serviços de Suporte Especializado

5.10.1. Tendo em vista a modernização da operação de infraestrutura de TI com recursos de de objetos faz-se necessário contratar os respectivos storage serviços de suporte especializado.

5.10.2. Após a devida implantação da solução, o suporte especializado será necessário para fins de melhor utilização dos novos recursos disponibilizados, inclusive para a adaptação de dados e de funcionalidades dos sistemas corporativos do Ministério da Justiça e Segurança Pública.

5.10.3. Existem diversos tópicos abrangidos pelos serviços de suporte especializado. Dentre eles, destacam-se:

5.10.3.1. Orientar na melhoria de métodos, procedimentos e técnicas utilizadas pela área de Suporte a Infraestrutura, Armazenamento e de Desenvolvimento de Sistemas;

5.10.3.2. Avaliar o desempenho do ambiente, com indicação das medidas recomendadas para sua otimização;

5.10.3.3. Orientar quanto à integração com:

5.10.3.3.1. Soluções de gestão de identidade e de acesso;

5.10.3.3.2. Soluções de orquestração de ambientes em nuvem;

5.10.3.3.3. Soluções de Data Analytics;

5.10.3.3.4. Ferramentas de Backup e Restore;

5.10.3.3.5. APIs de ferramentas de terceiros, entre outras tecnologias;

5.10.3.4. Orientar quanto à implementação de novas plataformas de desenvolvimento e/ou novas versões das plataformas existentes;

5.10.3.5. Orientar quanto a métodos e procedimentos para a migração de objetos para outros equipamentos.

5.10.4. Como este serviço é utilizado sob demanda, somente horas previamente aprovadas por Ordens de Serviço (OS) poderão ser utilizadas/executadas, e posteriormente faturadas. Tal fato dá liberdade à gestão das áreas técnicas quanto à utilização do serviço, flexibilizando o planejamento e execução dos projetos de interesse do MJSP.

5.11. Serviço de Treinamento Teórico/Prático

5.11.1. O Serviço de treinamento consiste na capacitação nas soluções contratadas para a equipe técnica e de colaboradores do MJSP;

5.11.2. O Serviço de treinamento será realizado em turmas, podendo ser nas modalidades presencial, remota ou híbrida;

5.11.3. O treinamento deve abranger tópicos básicos e avançados, de forma a capacitar a equipe do MJSP nos conhecimentos necessários para correta operacionalização da solução contratada;

5.11.4. A capacitação deve abranger conhecimentos teóricos e práticos (*hands on*).

5.11.5. Este serviço será utilizado sob demanda, aprovada por Ordem de Serviço (OS).

5.12. Serviços de Instalação e Implantação

5.12.1. Entende-se como serviço de instalação todos os serviços pertinentes ao completo funcionamento da solução, compreendendo instalação física, lógica e configuração inicial dos componentes do sistema.

5.12.2. Após a assinatura do contrato, a STI/SE/MJSP convocará reunião inicial com a CONTRATADA para alinhamento de expectativas e elaboração do plano de entrega, instalação e configuração dos equipamentos. Todas as condições da execução dependerão de aprovação da Contratante.

5.12.3. Após a instalação, a CONTRATADA deverá proceder a configuração dos componentes de forma que toda a capacidade seja disponibilizada para uso;

5.12.4. Os serviços deverão ser executados por profissionais qualificados e certificados pelo fabricante dos equipamentos, e a comprovação destes requisitos deverá ser emitida pelo fabricante e encaminhada à Contratante antes da aprovação do cronograma de execução dos serviços. Caso não haja certificado específico para o produto, o fabricante deverá atestar que a revenda é capacitada para prestar o serviço.

5.12.5. A certificação dos técnicos deverá contemplar a habilitação para instalar, configurar e customizar todas as funcionalidades demandadas no Termo de Referência.

5.12.6. A instalação e configuração deve seguir sempre as melhores práticas levando em consideração as recomendações dos fabricantes dos equipamentos.

5.12.7. A CONTRATADA deverá providenciar todos os materiais necessários à instalação física dos equipamentos; a CONTRATANTE será responsável pela disponibilização dos locais de instalação e pelo fornecimento de pontos elétricos necessários à instalação dos equipamentos.

5.12.7.1. As despesas de custeio com deslocamento dos equipamentos técnicos da proponente ao local de entrega, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos ficarão a cargo exclusivo da CONTRATADA;

5.12.8. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, podendo estas ser realizadas presencialmente, por telefone ou via conferência web, devendo a CONTRATADA sugerir as configurações de acordo com normas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

5.12.9. As configurações deverão seguir fielmente a padronização previamente estabelecida pela CONTRATANTE;

5.12.10. A prestação do serviço deve ser planejado e executado de modo que não cause interrupções e paralisações não programadas, ou qualquer outro tipo de transtorno ao correto funcionamento do ambiente operacional da CONTRATANTE; caso não seja possível manter a disponibilidade dos serviços básicos no momento da instalação, as manobras de implantação deverão ser realizadas durante janela de manutenção agendada previamente, em horários que não comprometam o funcionamento das atividades do órgão, inclusive aos sábados, domingos e feriados;

5.12.10.1. Ao término do serviço deve ser fornecido um relatório detalhado (*as-built*) contendo todas as configurações realizadas, com comentários sobre os principais comandos e as justificativas das opções de parametrização de modo a facilitar a posterior administração da solução e a continuidade de seu funcionamento.

5.13. De projeto e de implementação

5.13.1. O projeto para implantação deverá ser apresentado até 30 (trinta) dias antes da entrega dos equipamentos e deverá ser aprovado pela CONTRATANTE.

5.14. De implantação

5.14.1. Todo o hardware e solução a ser adquirido devem ser implantados pela CONTRATADA.

5.14.2. É de responsabilidade da CONTRATADA fornecer todos os insumos necessários para a implantação da solução, a exemplo de cabos e conectores de rede e de energia, SFPs, PDUs e trilhos de montagem.

5.14.3. A CONTRATADA deverá realizar a implantação da solução em até 60 (sessenta) dias após o recebimento provisório dos itens, devendo seguir o projeto aprovado pela CONTRATANTE. Qualquer eventualidade deve ser comunicada à CONTRATANTE, sendo de responsabilidade da CONTRATADA fornecer qualquer insumo de hardware ou software para realizar a correta implantação do(s) item(ns) adquirido(s).

5.14.3.1. Conforme tratado neste ETP, a CONTRATADA deverá entregar, instalar e configurar os equipamentos em até 120 (cento e vinte) dias contados da data de assinatura do contrato, considerando a entrega em 60 dias (item 3.9) e sua implantação em 60 dias.

5.14.4. A emissão do Termo de Recebimento Definitivo está condicionada à aprovação pela CONTRATANTE de Relatório Final (*as-built*) emitido pela CONTRATADA.

5.14.5. Após o recebimento definitivo a CGISE/STI/SE/MJSP, em conjunto com a CONTRATADA, deverá realizar a configuração dos ambientes de armazenamento de acordo com planejamento interno.

5.15. De garantia e manutenção

5.15.1. A CONTRATADA deverá fornecer garantia de 60 (sessenta) meses, conforme os itens do Guia “1.4.5 (Equipamentos de Armazenamento)” “Diretrizes para Contratação de Ativos de TIC” (https://www.gov.br/governodigital/pt-br/contratacoes/orientacoes_ativos-de-tic-v-4.pdf), vinculado à Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, conforme § 2º do Art. 8º.

5.15.1.1. a garantia deve abranger atualização de software e manutenção corretiva do hardware, inclusive com substituição do hardware caso necessário, pelo período de vigência do contrato.

5.15.1.2. Após expirado o período de garantia, todos os produtos devem continuar funcionando normalmente na última versão de software instalada.

5.15.2. A CONTRATADA deverá fornecer suporte e assistência técnica on-site com atendimento 24x7x365 e nível de serviço a ser definido em Termo de Referência.

5.15.2.1. A CONTRATADA deverá oferecer ao menos os seguintes canais de atendimento para abertura de caso /chamado/ticket de acionamento da garantia:

5.15.2.1.1. Telefone 0800; e

5.15.2.1.2. Site próprio.

5.16. De capacitação

5.16.1. Para fins de capacitação da equipe, deverá ser contratado serviço de operação assistida após a implantação das soluções de armazenamento e de backup, bem como, para capacitação aprofundada, dos serviços de treinamento teórico/prático. Considerando ser novos produtos a serem adquiridos pelo MJSP, o repasse de conhecimento ou treinamento deverá ser realizado pelo fornecedor ou fabricante da solução contratada.

5.16.2. Deverá ser contratada horas de suporte especializado para implantação das soluções, considerando serem produtos novos, cuja expertise ainda não foi adquirida pelos analistas que sustentam o ambiente do MJSP. Estas horas serão necessárias para implantação dos novos projetos e aqueles em curso.

5.17. De experiência profissional da equipe que executará os serviços relacionados à solução de TIC

5.17.1. A instalação dos ativos (*storages*) e passivos ficará a cargo da CONTRATADA, que deverá usar mão de obra qualificada e comprovadamente certificada pelo fabricante da solução para instalar, configurar e operar os produtos objeto da contratação.

5.17.2. A contratada deverá alocar profissionais devidamente certificados pela fabricante e qualificados para realizar as atividades de operação assistida, para fins de transferência de conhecimento à equipe de sustentação desta STI /SE/MJSP, assim como para as atividades de suporte especializado para implantação de projetos.

5.17.3. O perfil profissional de tecnologia da informação a STI/SE/MJSP, necessário para adquirir o conhecimento específico da solução a ser contratada, está abrangido no contrato de sustentação da STI/SE/MJSP ora em vigor.

5.18. De formação da equipe que projetará, implementará e implantará a solução de TIC

5.18.1. Os serviços deverão ser executados por profissionais qualificados e certificados pelo fabricante dos equipamentos, e a comprovação destes requisitos deverá ser emitida pelo fabricante e encaminhada à CONTRATANTE antes da aprovação do cronograma de execução dos serviços. Caso não haja certificado específico para o produto, o fabricante deverá atestar que a revenda é capacitada para prestar o serviço.

5.19. De metodologia de trabalho

5.19.1. Não se aplicam.

5.20. De segurança da informação e privacidade

5.20.1. A CONTRATADA deverá assegurar todas as atualizações de firmware, microcódigos e softwares, com disponibilização de patches de segurança e suporte ao longo da vida útil do hardware e/ou enquanto estiver disponível ao mercado a respectiva versão do software fornecido.

5.21. Dependência Tecnológica e Monopolização de Mercado

5.21.1. A Instrução Normativa SGD nº 94/2022, em seu Anexo I, subitem 1.4.1, estabelece diretrizes para evitar a dependência tecnológica e a monopolização de mercado no âmbito da administração pública. Essa preocupação reflete a necessidade de assegurar que as soluções de tecnologia da informação e comunicação (TIC) adotadas nesta contratação sejam sustentáveis, interoperáveis e promotoras de um ambiente competitivo. Nesse contexto, é essencial que a contratação e o desenvolvimento de soluções priorizem padrões abertos e interoperabilidade, promovendo a pluralidade de fornecedores e prevenindo a concentração de mercado em poucos agentes econômicos.

5.21.2. Atualmente o MJSP possui soluções de mercado para armazenamento e backup, como já foi informado neste documento que irão ser substituídas por outras dentro de um processo licitatório com ampla competição de mercado. Desta forma, busca-se tanto evitar dependência tecnológica e monopolização de mercado, quanto encontrar a solução com melhor custo-benefício que atenda às expectativas e necessidades do órgão. As

especificações técnicas foram selecionadas para permitir tanto a competitividade de mercado, a redução da dependência tecnológica e monopolização de mercado, sem olvidar daqueles requisitos técnicos necessários ao atendimento das necessidades do MJSP.

5.21.3. Outro aspecto fundamental é a implementação de práticas de governança que garantam a diversificação de fornecedores e evitem a formação de monopólios. A equipe do MJSP deve ao realizar contratações, realizar estudos de mercado detalhados e fomentar a competição entre empresas, utilização de padrões interoperáveis, além de cláusulas contratuais que impeçam a dependência excessiva de um único fornecedor. Essas ações fortalecem o ecossistema tecnológico nacional, ampliam a resiliência das operações públicas e contribuem para a criação de um mercado mais justo e dinâmico.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

6.1. Necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual

6.1.1. Será necessário avaliar se as soluções a serem fornecidas necessitarão de ajustes fins em termos elétricos na infraestrutura instalada dos data centers do MJSP para seu funcionamento adequado. Destaca-se a necessidade de adequação do posicionamento dos equipamentos aos racks já existentes, para os fins de fluxo de refrigeração do equipamento, conforme fluxo já estabelecido com os equipamentos existentes e instalados.

6.2. Possíveis Impactos Ambientais

6.2.1. Critérios de Sustentabilidade

6.2.1. A Constituição Federal estabeleceu, no art. 170, inciso VI, como um dos princípios da ordem econômica a defesa do meio ambiente, quanto ao impacto ambiental dos serviços e de seus processos de prestação. No art. 225, caput, destaca-se o dever constitucional de o Estado preservar o meio ambiente, o que se efetiva com o uso de poder de compra. O inciso IV, a seu turno, traz a exigência de estudo prévio de impacto ambiental para toda obra ou atividade causadora de significativa degradação do meio ambiente.

6.2.2. Instrução Normativa nº 1, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão, a qual prevê expressamente que as especificações técnicas para aquisições de bens e contratações de obras e serviços deverão conter critérios ambientais nos processos de extração, fabricação, utilização e descarte de matérias-primas, sem frustrar o caráter competitivo do certame.

6.2.3. Destaque-se da Declaração do Rio sobre Meio Ambiente o Princípio 15, que traduz o Princípio da Precaução, nos seguintes termos: “Com o fim de proteger o meio ambiente, o princípio da precaução deverá ser amplamente observado pelos Estados, de acordo com suas capacidades. Quando houver ameaça de danos graves ou reversíveis, a ausência de certeza científica absoluta não será utilizada como razão para o adiamento de medidas economicamente viáveis para prevenir a degradação ambiental.”

6.2.4. Preferência por produtos de baixo impacto ambiental: não geração, redução, reutilização, reciclagem e tratamento dos resíduos sólidos, bem como disposição final ambientalmente adequada dos rejeitos;

6.2.5. Preferência para produtos reciclados e recicláveis, bem como para bens, serviços e obras que considerem critérios compatíveis com padrões de consumo social e ambientalmente sustentáveis (Lei 12.305/2010);

6.2.6. Aquisição de produtos e equipamentos duráveis, reparáveis e que possam ser aperfeiçoados;

6.2.7. Adoção de procedimentos racionais quando da tomada de decisão de consumo, observando-se a necessidade, oportunidade e economicidade dos produtos a serem adquiridos;

6.2.8. Materiais menos agressivos ao meio ambiente;

6.2.9. Produtos concentrados, que utilizam menor quantidade de matéria prima e água na sua fabricação e acondicionados em embalagens menores;

6.2.10. Produtos com embalagens recicladas ou recicláveis, de papelão ou de plástico à base de etanol de cana-de-açúcar;

6.2.11. Os produtos deverão ser notificados ou registrados na ANVISA, conforme determina a legislação(www.anvisa.gov.br/saneantes/legis/index.htm);

6.2.12. Dessa forma a contratada deverá observar as seguintes legislações, no que couber:

6.2.12.1. Lei Federal nº 6.938, de 31/08/1981 (Política Nacional do Meio ambiente), Resolução CONAMA nº 275, de 25/04/2001 (cores para coleta seletiva), Decreto nº 5.940, de 25/10/2006 (Separação dos Resíduos Sólidos Recicláveis) e Recomendação do CNJ nº 011, de 22/05/2007 (Adoção de Políticas Públicas);

6.2.12.2. Instrução Normativa nº 01 STIL/MPOG, de 19/01/2010 (Sustentabilidade Ambiental) Decreto nº 6.746, de 05/06/2012 (Desenvolvimento Sustentável nas Contratações).

6.3. Da participação de Consórcios

6.3.1. Com relação à participação de consórcios, entende-se ainda que os serviços a serem contratados não exigem empresas de diferentes segmentos/capacidades reunidas para atuarem na execução dos serviços. Os resultados serão produzidos a partir de equipes, técnicas e procedimentos complementares e integrados, não havendo benefício, ou ampliação da competitividade, ou necessidade de segmentação ou divisão empresarial para a realização dos serviços objeto dessa contratação.

6.3.2. Observa-se, também, que existem empresas no mercado com plenas condições de reunir todos os componentes necessários à realização dos serviços. A Pesquisa de Preços desta contratação trouxe relação de diversos contratos semelhantes vigentes em órgãos da Administração Pública Federal.

6.4. Da participação de Cooperativas

6.4.1. Cooperativas também não poderão participar deste certame, pois a natureza dos serviços a serem executados apresenta características incompatíveis com a organização do trabalho em forma de cooperativa e possui as características abaixo descritas que são incompatíveis com a organização do trabalho em forma de cooperativa:

6.4.1.1. Demandas com mecanismos de gestão e controle continuados visando assegurar a adoção de métodos e padrões que são rotineiramente verificados;

6.4.1.2. Relação de hierarquia técnica e funcional entre os profissionais e a contratada;

6.4.1.3 Níveis diferenciados de responsabilização técnica.

6.4.2. A natureza da presente contratação não enseja a necessidade da previsão da participação de cooperativa, uma vez que o objeto consiste nos equipamentos (com softwares agregados), operação assistida, suporte e garantia de equipamento cujos objetos interagem de forma dependente. Desse modo, não há situação fática que comprove a necessidade da previsão do uso desse instituto no presente processo.

6.5. Condições de aquisição e pagamento semelhantes às do setor privado

6.5.1. O presente processo de contratação foi amoldado para atender a modernização dos datacenters do MJSP na instalação de uma infraestrutura hiperconvergente que irá reunir servidores, storages e solução de backup. Neste caso, a aquisição prevê conforme detalhado neste Estudo, processo faseado para implantação, conforme necessidades já apresentadas neste documento.

6.5.1.1. Foram realizadas reuniões com os principais fornecedores de mercado nos segmentos da contratação, aos quais apresentaram as especificações técnicas de suas soluções, como trabalham na fase de execução/implantação e também as condições de pagamento disponíveis. Este Estudo reuniu, portanto, as condições mínimas e necessárias ao atendimento das necessidades do órgão, trazendo a prática de mercado e ampla competitividade para as especificações técnicas e para o processo licitatório.

6.5.1.2. No quesito de condições de aquisição, este processo prevê de maneira geral a modernização dos dois datacenters do MJSP. Entretanto, a depender das condições orçamentárias disponíveis e o cenário macroeconômico nacional, esta contratação pode iniciar com a aquisição de equipamentos e serviços para o datacenter principal e após, para o datacenter secundário (datacenter de contingência). Esta prática também está aderente às condições de aquisição e pagamento semelhantes às do setor privado, não havendo empecilho para tal cenário.

6.5.1.3. Em termos de condições de pagamento, este processo adotou as práticas de mercado apresentadas pelos fornecedores, bem como adotou o rigor legal necessário para contratações inerentes de governo, conforme será detalhado no capítulo "Condições de medição e pagamento" do Termo de Referência.

6.5.2. Por fim, foi especificado para esta contratação padrões de SLA e garantia dos equipamentos e serviços praticados de mercado.

6.6. Outros requisitos

6.6.1. Além das necessidades de negócio, tecnológicas e os supramencionados, outros requisitos devem ser considerados ao longo do planejamento da contratação para se assegurar o alcance aos objetivos pretendidos com a contratação/aquisição, conforme a seguir:

- a) A solução deve ser entregue instalada e configurada, de modo a permitir seu pleno e perfeito funcionamento;
- b) A implantação da solução será acompanhada e supervisionada pela equipe técnica da STI;
- c) A equipe técnica da STI deverá ser capacitada para operar a solução de armazenamento e backup e recuperação de dados (hands-on);
- d) A versão dos softwares da solução deverão ser as mais atualizadas, considerando-se a data da implantação;
- e) O suporte técnico será prestado 24h (vinte quatro) por dia, durante 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias ao ano. Para tanto, a CONTRATADA deverá fornecer suporte telefônico (Central de Atendimento) para acionamento, por meio de ligação gratuita (0800) ou local à Brasília/DF, e/ou Ferramenta Web (sítio acessível via Internet) para abertura ou acompanhamento dos chamados realizados.

6.6.2. Por fim, ressalta-se que a presente contratação integra o projeto de reestruturação de infraestrutura dos data centers do MJSP e de instalação e implantação da nuvem privada do MJSP, devendo portanto estar alinhada temporalmente com a contratação em andamento via processo SEI 08006.000626/2023-72 - Aquisição de solução de infraestrutura de processamento e armazenamento de blocos para instalação de clusters nos Data Centers principal e secundário para implantação de nuvem privada.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. A definição das necessidades, a serem dimensionadas por esta Equipe de Planejamento da Contratação, levará em consideração, principalmente:

- a) Os objetivos estratégicos constantes no Plano Estratégico Institucional 2020-2023, descritos na seção 3 deste ETP;
- b) As principais necessidades de negócio, tecnológicas e demais necessidades elencadas nas seções 3, 5 e 6 deste ETP, respectivamente;
- c) Levantamentos feitos sobre a capacidade de armazenamento e backup dos últimos anos, analisando características, comportamentos e tendências futuras;
- d) Projeções, de acordo com melhores práticas de mercado e em conjunto com os principais fabricantes, com base em análises históricas e estimativas futuras com pelo menos 60 meses de crescimento.

7.2. Com base nessas necessidades, serão estabelecidos vários requisitos relacionados ao armazenamento, backup, licenciamento, integração, além de serviços de implantação e suporte. O objetivo é garantir alta disponibilidade para os serviços de tecnologia da informação críticos, considerados essenciais, e integrar o Data Center Principal, o Data Center Secundário e as soluções em nuvem já em uso pelo órgão, conforme mostrado na Figura 13:

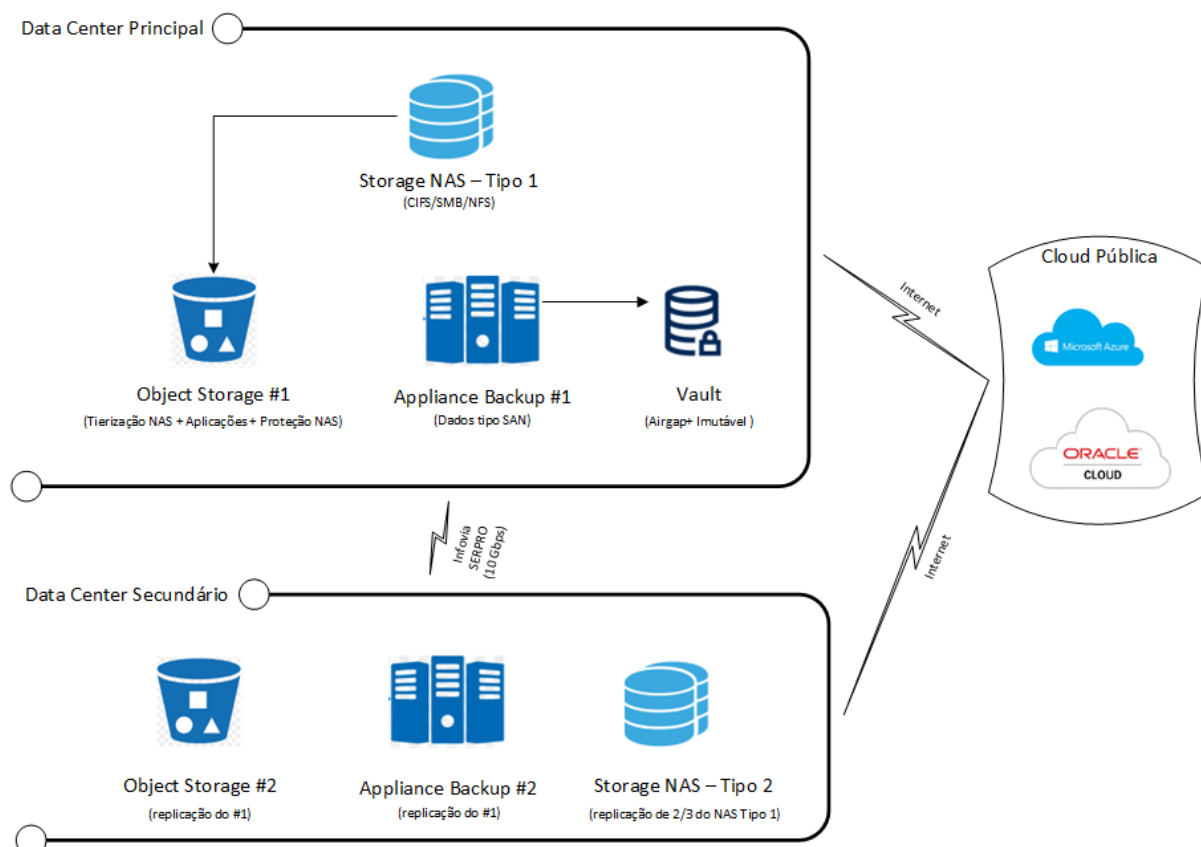


Figura 13 - Visão geral do cenário desejado.

Recomendações CIS/Auditoria TCU: regras de "backup 3-2-1": a organização precisa de três cópias dos dados em dois meios físicos e um isolado (offsite).

Detalhamento:

- a) Será implementado no site principal, uma solução NAS que chamaremos de NAS#1. O NAS#1 fará a replicação dos dados críticos no NAS#2, localizado no site secundário, tendo em vista que o referido site está sendo preparado para Disaster Recovery.
- b) O sistema de armazenamento de objetos, localizado no site principal, terá duas finalidades principais. Primeiramente, ele servirá como o repositório para a proteção dos dados contidos no NAS#1. Além disso, será usado para armazenar dados relacionados a aplicações que requerem armazenamento de objetos. Haverá uma réplica no site secundário.
- c) O equipamento de backup número 1, localizado no site principal, desempenhará o papel de repositório para armazenar cópias de backup dos dados armazenados na solução de hiperconvergência (vSAN), como servidores virtuais, dados de aplicações e bancos de dados. Além disso, esses dados serão replicados para o equipamento de backup número 2, situado no site secundário.
- d) Seguindo as melhores práticas, bem como recomendações da Gartner, será implementado os appliances de backup devem possuir mecanismos de segurança para isolado por mecanismo de interrupção de conectividade no nível da rede (*Air Gap*), com o objetivo de proteger os dados mais sensíveis da organização da incidência de ataques de ransomware e de sequestro ou corrupção de dados de sistemas críticos armazenados no ambiente de TIC.
- e) Resumidamente, o sistema de proteção de dados proposto será estruturado da seguinte forma:
 - e1) Para garantir a segurança dos dados armazenados na solução de hiperconvergência, será utilizado o Appliance de Backup número 1 e cópia extra para o Appliance de Backup número 2, ambos com mecanismos de segurança nativos para proteção das cópias de backup.
 - e2) Para proteger os dados armazenados nos dispositivos de armazenamento conectados à rede (NAS), será utilizado como primeira camada de proteção, mecanismos de snapshot, nativos da

própria solução. Como segunda camada de proteção, será utilizada a replicação dos dados da solução NAS do site principal para a solução NAS do site secundário. Por fim, como terceira camada de proteção serão replicados os dados da solução NAS para a camada dos Storage de Objetos.

7.3. Abaixo alguns arranjos simulados para a composição da solução de backup:

- a) Cenário 1: Neste cenário, teríamos dois dispositivos de backup: um para retenção de curto prazo no data center principal e outro para retenção de longo prazo no data center secundário. O problema é que em caso de um incidente grave em um dos data centers, poderíamos perder o backup de curto prazo ou o de longo prazo.
- b) Cenário 2: Aqui, teríamos dispositivos de backup de curto e longo prazo no data center secundário. O problema é que se ocorrer um incidente significativo nesse data center, perderíamos o backup, além de haver risco de sobrecarregar o período de backup.
- c) Cenário 3: Neste cenário, usaríamos dispositivos de backup de curto e longo prazo no data center principal, com a mesma configuração replicada no data center secundário. O problema é o custo associado a essa abordagem. Seria necessário ter uma quantidade significativa de dados armazenados por um período de retenção prolongado para justificar a implementação desse cenário.
- d) Cenário 4: Aqui, teríamos um único dispositivo de backup que reúna todos os dados, com uma réplica para o data center secundário. Esse foi o cenário escolhido.

Em todos esses cenários, houve preocupações específicas relacionadas à disponibilidade, perda de dados e custos. Cada cenário apresenta suas próprias vantagens e desvantagens. Foi considerado o melhor custo benefício.

7.4. Para determinar as atuais quantidades de armazenamento, usamos várias ferramentas de medição, incluindo o LiveOptics, OpsCenter, as ferramentas internas da VMware e também fizemos extrações manuais. Nesse processo, coletamos uma variedade de dados que serão usados como informações essenciais para planejar futuras necessidades de dimensionamento.

7.5. REQUISITOS DE ARMAZENAMENTO

7.5.1. Quanto ao armazenamento, é importante destacar que os recursos são tratados de forma global, já que todos os ambientes (produção, desenvolvimento/teste/homologação/treinamento e legado) necessitam de algum tipo de armazenamento ao longo do tempo. Da mesma forma que na área de processamento, na área de armazenamento também existe priorização de recursos de melhor desempenho para o ambiente produtivo, como por exemplo a alocação discos rápidos sempre que possível.

7.5.2. Considerando que a evolução de ocupação de espaço se dá de forma global e distribuída nos Data Centers Principal e Secundário, foram levantadas todas as taxas de alocação de espaço em todos os equipamentos e também o espaço ocupado pelo SEI na nuvem conforme as Tabelas 04 e 05:

SITE PRINCIPAL E SECUNDÁRIO - ATUAL				
Equipamento	Total de Armazenamento (TB)	Alocado (TB)	Livre (TB)	Percentual de Alocação
EMC VNX 7500	233,86	199,40	34,46	85,26%
Netapp FAS8080	608,22	477,26	130,96	78,47%
EMC VNX 5300 01	145,17	113,11	32,06	77,92%
EMC VNX 5300 02	145,17	123,82	21,35	85,29%
TOTAIS	1132,42	913,59	218,83	80,68%

Tabela 4 - Alocação de espaço Site Principal e Secundário.

Armazenamento Vmware (TiB)	Armazenamento Banco de Dados (TiB)	Armazenamento NFS (TiB)
0,409	5,06	20

Tabela 5 - Alocação de espaço SEI na nuvem.

7.5.3. Conforme demonstrado nas tabelas 04 e 05 a análise do armazenamento teve como objetivo não só o levantamento das taxas de ocupação por equipamento, mas principalmente a classificação do armazenamento por tipo de dado, tais como:

- a) armazenamento de dados de SAN (armazenamento VMware e armazenamento Banco de Dados);
- b) armazenamento de dados tipo NAS (armazenamento File Server e armazenamento NFS);
- c) armazenamento de backups.

7.5.4. Com a classificação dos tipos de dados armazenados foi possível definir a porção de armazenamento necessária para alocação na solução de hiperconvergência e na solução de NAS que será adquirida para armazenamento e compartilhamento de arquivos (objeto desse ETP). Importante mencionar que os dados de SAN e de NAS se comportam de maneira diferente, e portanto possuem taxas de crescimento próprias ao longo dos anos.

7.5.5. Com base nos levantamentos e análises feitas nos ambientes, foram definidos alguns critérios para fazer a projeção da quantidade de armazenamento para o novo ambiente, tais como:

- a) Levantamento do armazenamento atual de dados de NAS em todos os equipamentos de storage e do SEI na nuvem;
- b) Consolidação inicial dos valores;
- c) Projeção de 8,5% ao ano sobre o valor inicial pelo período de 60 meses, tendo em vista que foi feita a análise histórica da média de crescimento dos últimos 36 meses para dados de NAS;
- d) Área de snapshot para proteção de dados NAS (15% da capacidade líquida);

7.5.6. Para determinar o tamanho de armazenamento necessário para o sistema NAS, fizemos uma estimativa para um período de 60 meses. Essa estimativa resultou em uma quantidade de 274,48 tebibytes (TiB), que foi arredondada para **412 TiB (tebibytes)** ao final de 60 meses, para atender às necessidades do ambiente no site principal, conforme indicado na Tabela 6:

ARMAZENAMENTO NAS (TiB)				Crescimento					Armazenamento Final
				8,5%	8,5%	8,5%	8,5%	8,5%	
Armazenamento on-premise	SEI	Área de Snapshot	Total	2024	2025	2026	2027	2028	
218,68	20,00	35,80	274,48	297,81	323,12	350,60	380,40	422,32	412,00 TiB

Tabela 6 - Projeção de armazenamento NAS para o ambiente de armazenamento Site Principal.

7.5.7. Para o site secundário, estamos dimensionando uma capacidade projetada de armazenamento (NAS) de 2/3 do site principal (**274 TiB**), para proteção de dados em produção.

7.5.8. É importante explicar que no campo do armazenamento de dados, existem três abordagens principais: armazenamento em bloco, armazenamento de arquivos (NAS) e armazenamento de objetos. No momento, o Ministério possui soluções para armazenamento em bloco por meio de uma rede SAN de alta velocidade, bem como soluções para armazenamento de arquivos, como o NFS, por exemplo. No entanto, ainda não dispõe de uma solução para armazenamento de objetos.

7.5.9. O armazenamento de objetos é um método no qual os dados são armazenados em unidades individuais chamadas objetos. Cada unidade possui uma chave ou identificador exclusivo que permite sua localização em

qualquer parte de um sistema distribuído. O armazenamento de objetos é compatível com vários protocolos, incluindo HTTP e REST, que são amplamente usados em muitos sites e aplicativos de *Software-as-a-Service* (SaaS).

7.5.10. No presente projeto está sendo prevista a concepção de uma área para armazenamento de objetos, que terá basicamente duas finalidades: **hospedagem de objetos**, que serão acessados diretamente por algumas aplicações e **proteção dos dados NAS**.

7.5.11. Sobre a segunda finalidade, que é a proteção dos dados NAS, é preciso fornecer uma explicação mais detalhada.

7.5.12. De modo geral, gestores de tecnologia da informação vêm enfrentando há algum tempo os desafios decorrentes do rápido crescimento dos dados em formato de arquivos, que tem aumentado significativamente os custos e a complexidade dos ambientes de armazenamento.

7.5.13. Essa proliferação de dados não estruturados deixou as arquiteturas tradicionais de armazenamento incapazes de atender às demandas desse crescimento, tornando necessário o desenvolvimento de uma nova geração de tecnologias de armazenamento. Além disso, requisitos mais amplos de retenção de dados, conformidade regulatória, acordos de nível de serviço de disponibilidade mais rigorosos com as unidades internas ou externas, e iniciativas de nuvem e virtualização estão apenas agravando esse problema.

7.5.14. Nesse sentido, a proposta é que a proteção de dados do tipos NAS seja feita não mais através de uma abordagem tradicional de backup, mas através das próprias funcionalidade presentes nos sistemas internos dos servidores NAS, através de mecanismos avançados de snapshots.

7.5.15. O snapshot cria uma espécie de cópia instantânea de um arquivo específico. Chamamos de "pseudo cópia" porque não cria uma duplicata real do arquivo. Em vez disso, ele registra uma referência aos dados originais e monitora todas as alterações feitas nesses dados específicos. A cada modificação, o snapshot captura as mudanças bloco por bloco até atingir um ponto em que pode representar completamente o estado atual do arquivo. Isso inclui o cenário em que o arquivo original é excluído.

7.5.16. Para ilustrar, suponha que você tenha gravado o arquivo "A" e criado um snapshot dele. Se você fizer uma alteração para a versão "A.1", o snapshot será atualizado com essas alterações. Se posteriormente você alterar para a versão "A.2", o snapshot também registrará essas modificações. Tudo isso ocorre instantaneamente e praticamente em tempo real. Se, porventura, o arquivo original for excluído, todo o seu conteúdo permanecerá preservado no snapshot, mantendo o arquivo completo. O administrador, terá a capacidade de restaurar o arquivo a qualquer momento a partir desse snapshot.

7.5.17. Além disso, é possível integrar o snapshot com uma ferramenta chamada VSS (*Volume Shadow Copy Service*) ou Shadow Copies do Windows. Isso permite que os usuários restaurem versões anteriores de arquivos ou realizem rollbacks de arquivos para estados anteriores. Por exemplo, um usuário pode clicar com o botão direito do mouse em um arquivo e selecionar a versão desejada.

7.5.18. Se um arquivo for excluído, seja intencionalmente ou por engano, o administrador terá a capacidade de recuperá-lo a partir do snapshot. Isso fornece a segurança de ter um "ponto no tempo" em qualquer momento da existência do arquivo, permitindo a restauração, mesmo se o arquivo tiver sido excluído intencionalmente ou acidentalmente pelos usuários.

7.5.19. Durante a análise dessa proposta fizemos alguns questionamentos aos principais players de solução de armazenamento sobre se essa era uma prática de mercado utilizada pelas organizações públicas e privadas. O que foi respondido afirmativamente.

7.5.20. As principais organizações que trabalham com "grandes volumes de dados" - uma expressão comum nos dias de hoje - adotam essa abordagem devido aos diversos benefícios que ela proporciona. O principal desses benefícios é a simplificação do processo de proteção, resultando em uma redução significativa no tempo necessário para proteger e restaurar os dados. Isso ocorre porque as técnicas e ferramentas incorporadas ao próprio NAS assumem a responsabilidade pela proteção e restauração dos dados, tornando esses processos praticamente instantâneos.

7.5.21. No backup tradicional de grandes volumes de dados NAS, geralmente se recorre a protocolos como o NDMP, que foi originalmente criado para acelerar o processo de backup em ambientes NAS. No entanto, mesmo com esse protocolo, a velocidade é consideravelmente inferior à obtida ao combinar técnicas de snapshot e replicação, que é a abordagem proposta neste Estudo Técnico.

7.5.22. Do ponto de vista da segurança, a abordagem envolve o uso de snapshots, que oferecem proteção local no cluster principal. Além disso, os dados mais críticos são replicados para um cluster secundário, o que significa que já existe uma cópia desses dados em uma localização externa, em um segundo site.

7.5.23. A proposta é estabelecer uma terceira cópia integral, correspondente ao "Nível 3" de proteção do NAS, com recursos de expiração e imutabilidade. O "Nível 1" representa a proteção local, o "Nível 2" envolve a replicação entre o "NAS 1" e o "NAS 2", e o "Nível 3" consiste na cópia dos snapshots e dados para o storage de objetos (#1 e #2).

7.5.24. Superado os desafios técnicos, realizamos também uma análise do aspecto econômico. Nas simulações que conduzimos, identificamos que o custo mensal estimado para gerenciar e armazenar 1 TiB em um ambiente de backup tradicional era de em média R\$ 323,27. No entanto, ao adotar a proteção por meio da abordagem de snapshot + replicação + imutabilidade para armazenamento no storage de objeto, o custo mensal estimado diminuiu para R\$ 175,28 (já levando em conta o custo das duas cópias no storage de objeto e a área de snapshot adicional em ambos os storages NAS).

7.5.25. Nos exercícios efetuados, caso incluíssemos a porção NAS para ser protegida pela abordagem tradicional de backup (em torno de 153 TiB), o custo do grupo de backup praticamente dobraria de valor.

7.5.26. A projeção do espaço necessário para o storage de objetos foi calculada da seguinte forma:

- a) Estimativa de 6,84 terabytes para dados acessados diretamente por aplicações;
- b) Proteção de dados NAS.

ARMAZENAMENTO STORAGE DE OBJETOS (TiB)			Crescimento					Armazenamento Final
Dados acessados diretamente por aplicações	Proteção NAS	Total	8,5%	8,5%	8,5%	8,5%	8,5%	
			2024	2025	2026	2027	2028	
5,00	274,48	279,48	303,24	329,01	356,98	387,32	420,24	420,00

Tabela 7 - Projeção de armazenamento objeto para o ambiente de armazenamento.

7.5.27. Utilizando os critérios definidos, bem como a projeção para 60 meses, foi estimada a quantidade, individual, de **420 TiB** para o storage de objetos do site principal e secundário.

7.5.28. Os dois storage de objetos irão trabalhar em um cluster geograficamente distribuído com a definição de namespace global para acesso ao conteúdo armazenado.

7.6. REQUISITOS DE BACKUP

7.6.1. Atualmente os procedimentos de backup realizados pela STI são executados por estágios e abrange os dados gravados nos diretórios de rede privativos de cada unidade do Ministério da Justiça e Segurança Pública. Os arquivos objeto do backup são armazenados inicialmente no conjunto de *appliances* NetBackup 5230, limitado a 100 TiB; posteriormente esses dados são expirados para o conjunto de fitas LTO-7, por meio de um robô de backup (Tape Library TS4300). Ainda no contexto da disponibilidade e integridade das informações, o Ministério dispõe de 03 (três) cofres de mídias anti-chamas onde são armazenadas as fitas LTO (cópias off-site) aumentando a possibilidade de restauração do ambiente computacional em caso de incidente no data center.

7.6.2. A figura 14, apresenta o diagrama contendo o atual ambiente de backup do Ministério da Justiça e Segurança Pública:

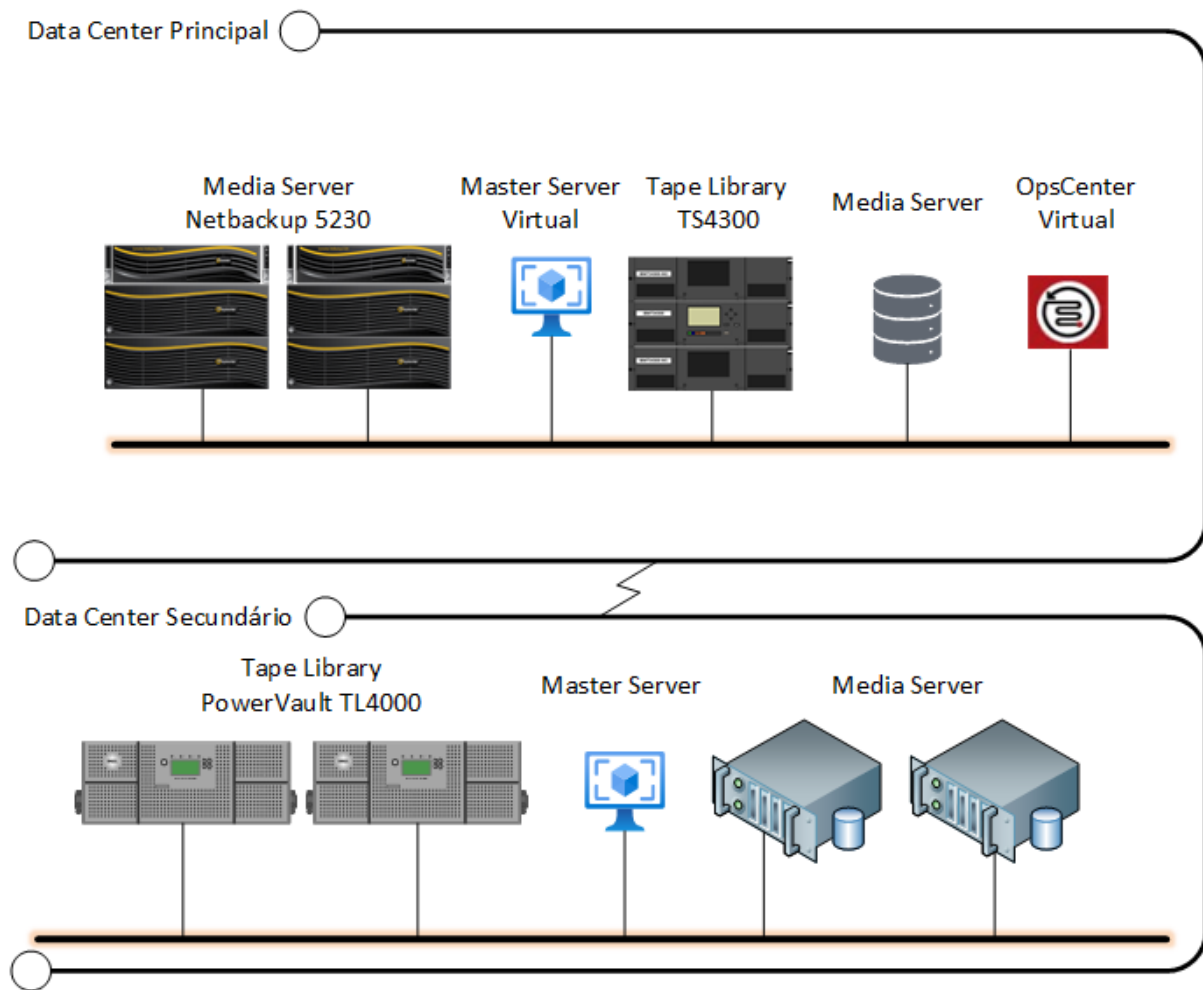


Figura 14 - Visão geral do ambiente Atual de Backup do Ministério.

7.6.3. Importante destacar que a atual solução tem se mostrado insuficiente, tanto no aspecto quantitativo, como qualitativo:

- Os appliances estão com a utilização acima do permitido, tendo sido necessário a criação de appliances virtuais para suprir a necessidade por armazenamento;
- Os appliances encontram-se na última versão suportada, porém estão com o *End of Life* anunciado pelo fabricante;
- Necessidade de uma solução mais moderna e eficiente para o backup de longa retenção;

7.6.4. A atual solução de backup está licenciada por volumetria (Front End Terabyte - FETB) e socket. O licenciamento por volumetria traz algumas vantagens porque diminui os riscos de inadequação da ferramenta em virtude de possíveis mudanças no ambiente. Esta modalidade é muito versátil e evita erros no dimensionamento dos dispositivos e softwares que serão alvos de backup, atendendo as necessidades tanto no ambiente on-premise como em cloud. Neste contexto, há uma diferenciação importante a saber. Armazenamento de *Backend*: leva-se em consideração a quantidade total de dados protegida pelo backup durante toda a política de retenção da organização, ou seja, em um servidor de arquivos é a soma do volume dos arquivos atuais e todas as versões de modificações efetuadas nestes arquivos, desde que ainda não tenham expirado. Armazenamento de *Frontend*: leva-se em consideração somente o volume do dado protegido, sendo independente do tempo de retenção da política da organização, ou seja, em um servidor de arquivos irá considerar somente o volume dos arquivos atuais, não importando o tamanho das versões modificadas salvas que ainda estejam válidas. Esse é um dos tipos de licenciamento atualmente vigente no Ministério, para o backup de volumes fora do ambiente de virtualização.

7.6.5. No licenciamento por agente, a solução de backup é licenciada pelo número de dispositivos e softwares utilizados pelos mesmos, não importando o volume de dados a ser processado. Esta solução é geralmente utilizada quando a quantidade de dispositivos a serem protegidos pela solução de backup é pequena ou quando o valor das licenças por agentes é compensatório em relação a outras formas de licenciamento. Pode ser uma opção não

vantajosa do ponto de vista de escalabilidade e apresentar inconvenientes em relação a compatibilização de agentes ao ambiente tecnológico.

7.6.6. Há também o licenciamento por socket de CPU. Nesse caso, a solução de backup é licenciada pelo número de sockets de CPU em uso (sockets com o processador instalado) nos servidores de dados, não importando o volume de dados ou quantidade de máquinas virtuais. Esta solução é comumente utilizada para licenciar servidores de máquinas virtuais, mas está sendo aos poucos descontinuada pelos principais fabricantes.

7.6.7. A partir de maio de 2019, foi necessária a adição de porções do storage para serem utilizadas como *pools* de armazenamento, visto que o espaço nos *appliances* já não era suficiente.

7.6.8. Pelo fato de tais produtos representarem requisitos essenciais para o ambiente computacional do Ministério, faz-se necessário que os estes estejam com o licenciamento vigente junto ao fabricante, com número e tipo de licenças compatíveis com a necessidade e com os mecanismos de garantia e possibilidades de atualização de versões vigentes.

7.6.9. A pretendida contratação se faz indispensável por tratar-se de serviços com características de execução contínua, uma vez que provê disponibilidade, proteção e automação do acesso a informação do órgão, minimizando a contaminação dos serviços e sistemas informatizados pelo mau uso da informação e garantindo a proteção dos dados confidenciais do órgão. Como se sabe, o processo backup é crítico e gera atividades de grande carga de execução, que podem comprometer o ambiente computacional de produção, causando lentidão e até indisponibilidade dos sistemas, caso não seja adequadamente implementado com robustos *softwares* e equipamentos.

7.6.10. REQUISITOS DE LICENCIAMENTO DO AMBIENTE DE BACKUP

7.6.10.1. O licenciamento para o software de Backup será baseado no modelo de licenciamento por volume de dados ("Capacity Licensing Model" do tipo Permanente), com habilitação para todas as funcionalidades nativas do fabricante.

7.6.10.2. Como já mencionado anteriormente, o modelo de licenciamento em questão possui várias vantagens. Uma das principais é a sua versatilidade, o que o torna especialmente adequado para ambientes que abrangem uma variedade de sistemas e tipos de dados heterogêneos. Além disso, ele oferece uma série de outros benefícios significativos que merecem destaque.

a) Simplificação de custos: Com o licenciamento por volumetria, os custos são geralmente baseados no volume de dados armazenados, tornando mais fácil prever e gerenciar os custos relacionados ao backup. Isso elimina a necessidade de calcular custos de licenciamento complexos com base em recursos específicos ou número de máquinas.

b) Flexibilidade: Esse modelo de licenciamento permite que as organizações escolham como desejam distribuir suas licenças de backup. Isso significa que você pode usar as licenças para proteger uma variedade de sistemas, servidores, máquinas virtuais e aplicativos, adaptando-se às necessidades específicas da sua infraestrutura.

c) Eficiência operacional: O licenciamento por volumetria pode simplificar a gestão do backup, já que as licenças são frequentemente centralizadas e podem ser aplicadas a diferentes componentes de backup. Isso reduz a complexidade e o esforço necessários para acompanhar várias licenças individuais.

Tipo	Volumetria TiB
Aplicações on-premise (tag: "APP PROD")	45,00
Aplicações nuvem (SEI)	0,409
Banco de Dados on-premise (tag: "BD PROD")	43,00
Banco de Dados nuvem (SEI)	5,06
NAS - File Server (tag: "FILE SERVER*" planilha Excel)	99,00
NAS - NFS	35,00
NFS SEI Azure	20,00
Total	247,61

Tabela 8 - Volumetria de dados elegíveis a serem protegidos (ambiente produtivo).

7.6.10.3. Aplicando um crescimento de 8,5% ao ano a um valor inicial de 247,61 durante 5 anos, o valor final do licenciamento seria de aproximadamente 380,98 TiB.

7.6.10.4. Conforme está registrado no Estudo Técnico Preliminar, referente ao processo SEI nº 08006.000626 /2023-72, que envolve a compra de uma solução de infraestrutura para processamento e armazenamento em blocos, está previsto que serão adquiridos 8 nós de HCI (Infraestrutura Hiperconvergente) no site principal e 5 nós no site secundário. Cada um desses "nós" deverá ser equipado com 2 processadores físicos, totalizando 26 processadores físicos ou sockets.

7.6.10.5. Desse modo, considerando que teremos um ambiente de processamento bem definido e consolidado para os próximos 60 meses, opcionalmente, poderá também ser ofertado o licenciamento por socket.

7.6.10.6. Se não estivesse sendo cessado, esse modelo de licenciamento poderia ser uma escolha vantajosa para garantir a proteção completa de grandes quantidades de dados, pois independe do volume de dados ou do número de máquinas virtuais.

7.6.10.7. Além dos 26 sockets mencionados anteriormente, é necessário também adicionar mais 16 sockets que são provenientes dos servidores das quatro Penitenciárias Federais, totalizando 42 sockets. Se aplicarmos um aumento de 8,5% ao ano durante 5 anos, o total poderá alcançar 64 sockets.

7.6.10.8. No entanto, conforme já explanado no tópicos anteriores, na presente contratação, adotaremos uma abordagem de proteção para os dados NAS através de snapshot + replicação de dados + imutabilidade.

7.6.10.9. Essa abordagem está regulamentada, inclusive, através da Portaria DTIC/SE/MJSP Nº 6, DE 31 DE MARÇO DE 2022 (17615301), que instituiu a Norma de Segurança de Replicação de Dados e Backup no âmbito da Diretoria de Tecnologia da Informação e Comunicação do Ministério da Justiça e Segurança Pública.

Art. 7º No caso dos repositórios de arquivos ou objetos, as rotinas de realização backups em pontos do tempo podem ser substituídas pela realização periódica de instantâneos (snapshots) do estado dos repositórios para viabilizar a recuperação para um estado anterior, desde que os equipamentos suportem esta funcionalidade e que cada um dos repositórios possua ao menos uma réplica integral do seu conteúdo.

7.6.10.10. Desconsiderando a quantidade de dados do tipo NAS (CIFS, SMB, NFS), teríamos uma necessidade de licenciamento de backup de 93,00 TiB. Se aplicarmos uma taxa de crescimento de 8,5% ao ano (arredondando as casas decimais pra cima), durante 5 anos, chegaremos a um total de 140 TiB. Tendo em vista a necessidade de crescimento, o referido projeto será realizado em forma de ata de registro de preço para que possamos expandir o ambiente conforme necessidade e conveniência do ministério, tornando o aumento da capacidade gradual enquanto a ata estiver vigente, chegando o final da vigência com o quantitativo necessário para atender toda a demanda prevista no prazo de 5 anos.

7.6.10.11. Além disso, estaremos incluindo 8,5% do total do último ano como reserva técnica (arredondando as casas decimais pra cima), que corresponde à 14 TiB de reserva técnica, totalizando **152 TiB**. Essa será a volumetria máxima anual.

Volumetria Atual	93
1º Ano (8,5% a.a)	101
2º Ano (8,5% a.a)	110
3º Ano (8,5% a.a)	119
4º Ano (8,5% a.a)	129
5º Ano (8,5% a.a)	140
Reserva Técnica	12
Volumetria Máxima	152 TiB

Tabela 9 - Previsão de volumetria para o licenciamento.

7.6.11. VOLUMETRIA DE BACKUP - ARMAZENAMENTO EM DISCO

7.6.11.1. Atualmente o sistema de backup em disco possui os seguintes pools de armazenamento: XX01, XX02, XX016, XX214, XX123 e XX215. O XX01 e XX02 correspondem aos dois *appliances*, os quais estão com utilização acima de 90%. O demais correspondem a porção de discos do storage disponibilizados como repositórios de backup.

Disk Pool	Total Capacity(GB)	Used Space (GB)	Free Space (GB)	%
XX01	46.227,26	44.258,27	1.968,99	96%
XX02	49.571,82	47.511,43	2.060,39	96%

XX215	77.216,39	72.144,85	6.071,54	92%
XX214	59.963,93	57.238,05	2.725,88	95%
XX016	41.285,46	32.990,97	7.294,49	80%
XX123	37.353,42	35.853,26	1.500,17	96%

Tabela 10 - Pools de armazenamento reservados para o backup.

7.6.11.2. Conforme pode ser observado, o nível de utilização dos backups em discos está quase integralmente acima de 90%, e isso exige que seja feita análise da forma que os backups estão sendo feitos, bem como o tipo de dado a ser protegido de forma que se tenha o RPO (*Recovery Point Objective*) e o RTO (*Recovery Time Objective*) adequado para cada tipo de dado. A tabela abaixo apresenta informações sobre a política de retenção que deve ser levada em consideração, juntamente com a quantidade de dados associada a cada tipo específico.

Tipos de Dados	Diário	Semanal	Mensal	Volumetria (TiB)	Tipo de Proteção
Bancos de dados relacionais e não-relacionais	15	12	12	49,00	Backup
Aplicações	30	1	-	45,00	Backup
Arquivos ou objetos gerenciados por aplicações	30	12	12	55,00	Snapshot+Replicação+Imutabilidade
Servidor de Arquivos	30	12	12	99,00	Snapshot+Replicação+Imutabilidade
Configurações de ativos de infraestrutura de TIC	30	1	-	1,00	Backup

Tabela 11 - Política de retenção e volumetria por tipos de dados.

7.6.11.3. Diante disso, para a projeção da solução de backup em disco estão sendo analisados os dados a serem protegidos na origem, ou seja, qual o montante e quais tipos de dados que se deseja proteger, desconsiderado a volumetria de dados do tipo NAS. Isso é importante tendo em vista que os dados de SAN (armazenamento Vmware e armazenamento Banco de Dados) serão protegidos de forma diferente que os dados de NAS (armazenamento File Server e armazenamento NFS).

7.6.11.4. A Tabela 12 demonstra os dados que servirão de base para o dimensionamento do appliance de backup:

RETENÇÃO						
Tipos de Dados	FETB	1º Ano	2º Ano	3º Ano	4º Ano	5º Ano
Bancos de dados relacionais e não-relacionais	49	53	57	62	67	73
Aplicações	45	49	53	57	62	67
Configurações de ativos de infraestrutura de TIC	1	1,1	1,2	1,3	1,4	1,5

Tabela 12 - Evolução da capacidade de armazenamento para 60 meses.

Bancos de dados relacionais e não-relacionais	Diário	Diário Inc.	Semanal	Mensal	Volumetria (TiB)	Appliance (TiB)	Desdup.	Appliance (TiB)
Retenção	1	14	12	12	53	1356	80%	271
Volumetria (TiB)	53	37	633	633				
Aplicações	Diário	Diário Inc.	Semanal	Mensal	Volumetria (TiB)	Appliance (TiB)	Desdup.	Appliance (TiB)
Retenção	1	29	1	0	49	168	90%	17
Volumetria (TiB)	49	71	49	0				
Configurações de ativos de infraestrutura de TIC	Diário	Diário Inc.	Semanal	Mensal	Volumetria (TiB)	Appliance (TiB)	Desdup.	Appliance (TiB)
Retenção	1	29	1	0	1,1	4	90%	0,4
Volumetria (TiB)	1,1	1,6	1,1	0				
							Appliance 1Y	288

Tabela 13 - Capacidade de armazenamento em appliance necessária para o primeiro ano, considerando a deduplicação.

Bancos de dados relacionais e não-relacionais	Diário	Diário Inc.	Semanal	Mensal	Volumetria (TiB)	Appliance (TiB)	Desdup.	Appliance (TiB)
Retenção	1	14	12	12	75	1880	80%	376
Volumetria (TiB)	73	51	878	878				

Aplicações	Diário	Diário Inc.	Semanal	Mensal	Volumetria (TiB)	Appliance (TiB)	Desdup.	Appliance (TiB)
Retenção	1	29	1	0	67	233	90%	23
Volumetria (TiB)	67	98	67	0				

Configurações de ativos de infraestrutura de TIC	Diário	Diário Inc.	Semanal	Mensal	Volumetria (TiB)	Appliance (TiB)	Desdup.	Appliance (TiB)
Retenção	1	29	1	0	1,5	5,2	90%	0,5
Volumetria (TiB)	2	2,2	1,5	0				
							Appliance 5Y	400

Tabela 14 - Capacidade de armazenamento em appliance necessária para o 5º ano, considerando a deduplicação.

7.6.11.5. Importante salientar que os dados expostos nas Tabelas 13 e 14 são dados de SAN considerando somente os ambientes produtivos. Foi aplicada a taxa de deduplicação média verificada atualmente.

7.6.11.6. A volumetria do appliance de backup mínima para atendimento das demandas de backup do MJSP é de **400 TiB**.

7.7. SERVIÇO DE INSTALAÇÃO E IMPLANTAÇÃO

7.7.1. Faz-se necessária a aquisição de serviços de instalação e implantação de todas as soluções adquiridas, conforme estimativas de capacidade realizadas nos itens anteriores.

7.7.2. Para tal, estima-se que a solução será composta pelos seguintes sistemas de armazenamento e de backup, totalizando a necessidade de se realizar até 7 instalações:

- 01 (uma) Solução de Armazenamento NAS no data center principal;
- 01 (uma) Solução de Armazenamento NAS no data center secundário, com replicação;
- 01 (uma) Solução de Armazenamento de objetos no data center principal;
- 01 (uma) Solução de Armazenamento de objetos no data center secundário, com replicação;
- 01 (uma) Solução de Orquestração de Software de Backup no data center principal e secundário;
- 01 (uma) Solução de Appliance de Backup no data center principal;
- 01 (uma) Solução de Appliance de Backup no data center secundário, com replicação.

7.8. SERVIÇO DE OPERAÇÃO ASSISTIDA

7.8.1. Assim que os novos sistemas de armazenamento estiverem devidamente instalados e implantados, faz-se necessário que a equipe técnica da STI/SE/MJSP conheça o produto, seus recursos e suas especificidades. É preciso que haja um acompanhamento na operação dos storages, bem como de toda a solução de backup, logo após a implantação de forma a subsidiar a equipe técnica de sustentação a utilizar devidamente os recursos, conforme definido na sessão 5.

7.8.2. De tal forma, estima-se que a solução de armazenamento será composta por 2 subsistemas de armazenamento (storage NAS e storage de objetos) e considera-se razoável o acompanhamento operacional por um analista do fabricante da solução por um período mínimo de 80 horas (1 mês) para as soluções implantadas,

logo após a sua implantação, totalizando 160 horas (2 meses) disponíveis, que serão ser contratados sob demanda (em horas).

7.8.3. De forma análoga, estima-se que a solução de backup será composta por até 3 subsistemas de software ou hardware, considera-se razoável o acompanhamento operacional por um analista do fabricante da solução por um período mínimo de 80 horas (1 mês) para a solução implantada, logo após a sua implantação, totalizando 160 horas (2 meses) disponíveis, que serão ser contratados sob demanda (em horas).

7.9. SERVIÇO DE SUPORTE ESPECIALIZADO

7.9.1. Considerando que a implantação das soluções de armazenamento e backup são produtos com recursos tecnológicos novos, que pode ser utilizado tanto pela equipe de infraestrutura de TIC como para equipe de desenvolvimento de sistemas, faz-se necessária mão-de-obra especializada para orientar o correto uso desta nova tecnologia para o ambiente do MJSP, inclusive para implantação de projetos que venham a usar os novos recursos tecnológicos que a aquisição proporcionará, conforme descrições apenas na sessão 5.

7.9.2. De tal forma, considera-se necessária a aquisição de horas objetivando a boa utilização dos recursos conforme sumarizado a seguir:

	Suporte Especializado Storage NAS e Storage de Objetos (horas)	Suporte Especializado Solução de Backup -Hardware e Software (Horas)
Ano 1	160	160
Ano 2	160	160
Ano 3	160	160
Ano 4	160	160
Ano 5	160	160
Total	800	800

7.10. OPORTUNIDADE DE ATAS DE REGISTRO DE PREÇOS

7.10.1. Conforme detalhado neste documento, as soluções de TIC a serem contratadas são muito específicas e amoldadas à realidade da infraestrutura de TIC do MJSP. Neste sentido, foram realizados amplos estudos de mercado para determinação da solução adequada e com melhor custo-benefício, o que foi traduzido nas especificações técnicas dos equipamentos e serviços desta contratação. Dito isso, informa-se que foram realizadas buscas por Atas de Registro de Preço válidas, entretanto, como se trata de uma contratação muito customizada ao órgão, não foram encontradas soluções disponíveis que pudessem ser utilizadas para suprir a demanda do MJSP.

7.10.2. Em complemento, informa-se que todos os anos, decorrente de normatização da Portaria nº 405/2020 - MJSP (Plano de Compras Compartilhadas do MJSP - PCCOM), que instituiu os mecanismos de governança e determina as diretrizes e procedimentos para o planejamento e o gerenciamento de contratações públicas de bens, serviços, obras, soluções de tecnologia da informação e comunicação, e para o compartilhamento e centralização de contratações no âmbito do Ministério da Justiça e Segurança Pública, conforme documentações apenas no processo administrativo (SEI 30329635 e 30329642), são realizadas reuniões entre os órgãos colegiados que compõe o MJSP e não foram detectadas contratações semelhantes à almejada por este processo administrativo, pela motivação principal de ser uma solução especialíssima à realidade do MJSP, com especificações técnicas e definições de volumetria e de serviços que dificultam a busca por Atas semelhantes. Da mesma forma, é complexa a situação de publicar esta IRP abertamente, tendo em vista que outro órgãos podem ter necessidade próximas, mas a solução é aderente apenas à realidade do MJSP, o que pode trazer problemas de gastos públicos inadequados e especificações de serviços que não atendem àqueles órgãos que porventura tivessem interesse na adesão.

7.11. JUSTIFICATIVA DO REGISTRO DE PREÇOS

7.11.1. Será adotado o Sistema de Registro de Preços, haja vista a conveniência da contratação com previsão da forma parcelada conforme a necessidade, visando minimizar os riscos de implantação do projeto por questões orçamentárias, dado o alto valor da solução. Desta forma, é possível planejar as atividades de implantação da solução com os recursos disponíveis no ano fiscal de contratação e realizar a contratação parcial da solução, sem deixar de atender às necessidades de infraestrutura de TIC do órgão, tendo em vista que a solução é composta por dois ambientes (datacenter principal e datacenter secundário), sendo possível criar fases do projeto, instalando a

solução inicialmente no datacenter principal (fase 1) e posteriormente no datacenter secundário (fase 2). Ressalta-se que o datacenter secundário atua como ambiente de recuperação de desastres em caso de indisponibilidade do datacenter principal, nos termos de alta disponibilidade da solução a ser implantada.

7.11.2. O Sistema de Registro de Preços (SRP), segundo Marçal Justen Filho, "apresenta diversas virtudes, propiciando a redução de formalidades e a obtenção de ganhos econômicos para a Administração Pública". Tal o é que, diante de situação que se amolde às hipóteses previstas na Lei Federal nº 14.133/21 e em regulamentação própria, a adoção do Sistema de Registro de Preços constitui-se em verdadeira obrigação para o gestor, devendo apresentar justificativa em caso de não adoção.

7.11.3. O regulamento determina que nas licitações o planejamento deverá considerar a expectativa de consumo anual, e ser processada por meio de sistema de registro de preços, quando pertinente. (Art. 40, inciso II, e Art. 82, §5º, ambos da Lei Federal nº 14.133/21).

7.11.4. Não se trata de nova modalidade de licitação, mas de um instrumento auxiliar das licitações e contratações, para a aquisição de bens e a contratação de serviços mediante a adoção das modalidades concorrência e pregão.

7.11.5. Ademais, a opção pelo Sistema de Registro de Preço originário de licitação, é a mais viável, pois possui características vantajosas para a administração pública, por exemplo o fato da existência de facultatividade na contratação do objeto licitado, sendo assim, a Administração tem a discricionariedade de agir conforme suas necessidades, podendo flexibilizar suas despesas, com a devida adequação aos recursos disponíveis, conforme previsão legal no art. 3º do Decreto 7.892/2013 (*quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados*).

7.11.6. Nesse sentido, justifica-se ainda a motivação para utilização do Sistema de Registro de Preços em razão da demanda ter a característica de poder ser parcelada, sendo utilizado o registro de acordo com a necessidade dos serviços demandados, levando em consideração os recursos disponíveis. desgaste natural. Outro ponto que merece destaque é o emprego de recursos financeiros somente para o atendimento da demanda momentânea.

8. Levantamento de soluções

8.1. Necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas

8.1.1. Foram realizadas pesquisas no painel de preços e no "comprasnet" com a finalidade de encontrar soluções de armazenamento do tipo NAS e de Objetos, bem como de soluções de backup de dados para fins de análise dos editais e termos de referência. Nas análises de contratações específicas de soluções de armazenamento NAS, foram excluídas aquelas que tratavam de storages híbridos, de forma a trazer objetos semelhantes aos que se pretende adquirir neste processo (storages NAS *all-flash*).

8.1.2. Soluções de Armazenamento de Dados

8.1.2.1. Processo de aquisição de storage all-flash e storage híbrido pela Polícia Rodoviária Federal. O item 1 é relativo à solução de armazenamento NAS all-flash do tipo scale-out.

Órgão: Polícia Rodoviária Federal	UASG: 200109
Pregão: 108/2022	Itens 1 e 3
Objeto: 1) Solução de armazenamento all-flash NVMe, com serviços de instalação e 60 meses de garantia e suporte on-site. 3) Expansão da Solução de armazenamento all-flash NVMe.	
Valor total unitário dos itens: R\$ 5.637.248,73	

Capacidade líquida total adquirida por unidade: 600 TiB
Valor por tebibytes: R\$ 9.395,41

8.1.2.2. Processo de aquisição de storage all-flash pelo Conselho de Justiça Federal. O item 1 é relativo à solução de armazenamento NAS all-flash do tipo scale-out. Também foi incluído no processo, contratação de suporte técnico e garantia por 60 meses e serviços de instalação.

Órgão: Conselho de Justiça Federal	UASG: 90026
Pregão: 18/2023	Itens 1 a 3
<p>Objeto:</p> <p>1) Solução de Armazenamento de Dados, All Flash NVMe, com 380 TiB líquido, garantia por um período de 60 meses.</p> <p>2) Suporte técnico por um período de 60 meses para o Item 1.</p> <p>3) Serviço de instalação, configuração e integração do storage fornecido</p>	
Valor total unitário do item 1: R\$ 3.960.570,00	
Capacidade líquida total adquirida por unidade: 380 TiB	
Valor por tebibytes: R\$ 10.422,55	

8.1.2.3. Processo de aquisição de storage all-flash pelo Tribunal de Justiça de Pernambuco. O item 1 é relativo à solução de armazenamento NAS all-flash do tipo scale-out. Também foi incluído no processo, contratação de suporte técnico e garantia por 60 meses, treinamento/repasso de conhecimento e serviços de instalação.

Órgão: Tribunal de Justiça de Pernambuco	UASG: 926496
Pregão: 07/2024	Itens 1 a 5
<p>Objeto:</p> <p>1) Solução de Armazenamento de Dados All-Flash, do tipo STORAGE, de no mínimo 1PiB líquido/2 PiB utilizáveis e expansível a pelo menos 2 PiB líquidos/4 PiB utilizáveis</p> <p>2) Expansão da Solução de armazenamento all-flash NVMe.</p> <p>3) Serviços de Planejamento, Instalação, Configuração e Migração de Dados para Solução STORAGE All-Flash</p> <p>4) Treinamento Presencial, de Natureza Teórica e Prática, para Repasse de Conhecimento Tecnológico com Carga Horária Mínima de 20 horas</p> <p>5) Serviço de Suporte Técnico para Soluções de Armazenamento de Dados All-Flash, do tipo STORAGE</p>	

Valor total unitário do item 1: R\$ 10.289.288,88
Capacidade líquida total adquirida por unidade: 1.000 PB / 909,50 TiB
Valor por tebibytes: R\$ 11.313,13

8.1.2.4. Aquisição de storage de objetos compatível com a solução de armazenamento NAS do STF.

Órgão: STF	UASG: 40001
Pregão: 49/2023	Item: 2
Objeto: Solução de Armazenamento de Objetos, incluindo instalação, configuração, licenciamento de <i>software</i> , garantia e suporte técnico pelo prazo de 36 (trinta e seis) meses.	
Valor total do item: R\$ 7.876.537,20 (duas unidades)	
Capacidade líquida total adquirida: 1024 TB / 931,32 TiB	
Valor por tebibyte: R\$ 4.228,70	

8.1.2.5. Aquisição pelo SERPRO de oito clusters de storage de objetos com 500TB cada. Nesta aquisição também foi contratado serviço de migração, consultoria e suporte técnico.

Órgão: SERPRO	UASG: 803080
Pregão: 509/2022	Item: 1
Objeto: SOLUÇÃO DE ARMAZENAMENTO DE OBJETOS (500TB).	
Valor total: R\$ 19.200.000,00 (oito unidades)	
Capacidade líquida total adquirida: 4.000 TB / 3.637,98 TiB	
Valor por tebibyte: R\$ 5.277,65	

8.1.2.6. Aquisição do BRB de dois clusters de *storage* de objetos com 1PB cada.

Órgão: BRB	UASG: 925008
Pregão: 40/2021	Item: 1
Objeto: Sistema de Armazenamento do tipo Objeto (1 PB útil) para longa retenção.	
Valor total do item: R\$ 3.938.268,60 (cada unidade, total de duas)	
Capacidade líquida total adquirida: 1024 TB / 931,32 TiB	
Valor por tebibyte: R\$ 4.228,70	

8.1.2.7. Aquisição pelo TJPI de um cluster de *storage* de objetos com 440TB. Também foi contratada a implantação e consultoria.

Órgão: TJPI	UASG: 926454
Pregão: 25/2021	Item: 1
Objeto: Hardware de Armazenamento de <i>Backup</i> em Disco.	
Valor total: R\$ 890.040,80	
Capacidade líquida total adquirida: 440 TB / 400,18 TiB	
Valor por tebibyte: R\$ 2.224,10	

8.1.2.8. Não foi encontrada solução de aquisição de *storage* tipo NAS com *storage* de Objetos na mesma contratação. Contudo, pode-se avaliar as soluções do tipo NAS nos itens 8.1.2.1 ao 8.1.2.4 e as soluções de *storage* de Objetos nos itens 8.1.2.5 a 8.1.2.7.

8.1.3. Soluções de Backup de Dados

8.1.3.1. Aquisição pelo TRF3 de solução de backup. Também foi contratado serviços garantia, serviços de de implementação da solução, serviços de suporte e serviços de treinamento.

Órgão: TRF3	UASG: 90029

Pregão: 36/2022	Itens: 3, 4, 13, 14 e 15
<p>3) Hardware do appliance de backup veritas Flex Appliance 5250 com capacidade utilizável de 271 TB, 256GB RAM, 6 portas 10Gb/25Gb, 4 portas FC 16Gbps, com suporte e manutenção por 36 meses</p> <p>4) Software do appliance de backup Veritas Flex Appliance 5250 com capacidade utilizável de 271 TB, com suporte e manutenção por 36 meses</p> <p>13) Serviços de Suporte Crítico Premier por 36 meses</p> <p>14) Serviços de Implementação: Instalação e Configuração dos itens contemplados de ATUALIZAÇÃO e EXPANSÃO</p> <p>15) Serviços de treinamento oficial do fabricante para todos os produtos ofertados</p>	
<p>Valor total item 3: R\$ 1.406.553,92 (4 unidades de appliance)</p> <p>Valor total item 4: R\$ 3.831.068,12 (4 unidades de licença)</p>	
<p>Capacidade líquida total adquirida item 3: 271 TB / 246 TiB</p> <p>Capacidade líquida total adquirida item 4: 271 TB / 246 TiB</p>	
<p>Valor por tebibyte item 3: R\$ 1.426,68</p> <p>Valor por tebibyte item 4: R\$ 3.885,89</p>	

8.1.3.2. Aquisição pela ABIN de solução de backup. Também foi contratado serviços garantia, serviços de suporte e serviços de operação assistida.

Órgão: ABIN	UASG: 110120
Pregão: 11/2023	Itens: 1 a 6
<p>1) Expansão de licenciamento Veritas NetBackup por volumetria (TB), com suporte técnico de 12 meses</p> <p>2) Suporte técnico Veritas NetBackup por volumetria (TB), por 12 meses</p> <p>3) Suporte técnico Veritas NetBackup Appliance Controladora 5240 de 4 TB, por 12 meses</p> <p>4) Aquisição de Gaveta de expansão de 49 TB do Veritas NetBackup Appliance 5240, com suporte técnico de 12 meses</p> <p>5) Suporte técnico Veritas NetBackup Appliance Gaveta 5240 de 49 TB, por 12 meses</p> <p>6) Operação assistida</p>	
<p>Valor unitário item 1: R\$ 40.743,45 (15 TB)</p>	
<p>Capacidade líquida total adquirida item 1: 15 TB / 13,64 TiB</p>	
<p>Valor por tebibyte item 1: R\$ 2.987,06</p>	

8.1.3.3. Aquisição pelo TJPB de solução de backup com proteção de dados. de solução de backup. Também foi contratado serviços de instalação e configuração e serviços de treinamento.

Órgão: TJPB	UASG: 926222
Pregão: 90002/2024	Itens: 1 a 3
1) Solução de armazenamento e proteção de dados em disco (appliance + licenciamentos) com garantia de 60 (sessenta) meses. 2) Serviço de instalação e configuração. 3) Treinamento na solução.	
Valor total item 1: 4.748.843,29	
Capacidade líquida total adquirida item 3: 350 TB / 318 TiB	
Valor por tebibyte item 1: R\$ 14.918,31 por TiB (software e hardware)	

8.2. Alternativas do mercado

8.2.1. Foi realizada avaliação das empresas de mercado de armazenamento de dados em estudo realizado pela Gartner a partir do artigo “*Magic Quadrant for Distributed File Systems and Object Storage*”, publicado em 01/11 /2023. Segue o quadrante mágico, conforme artigo:

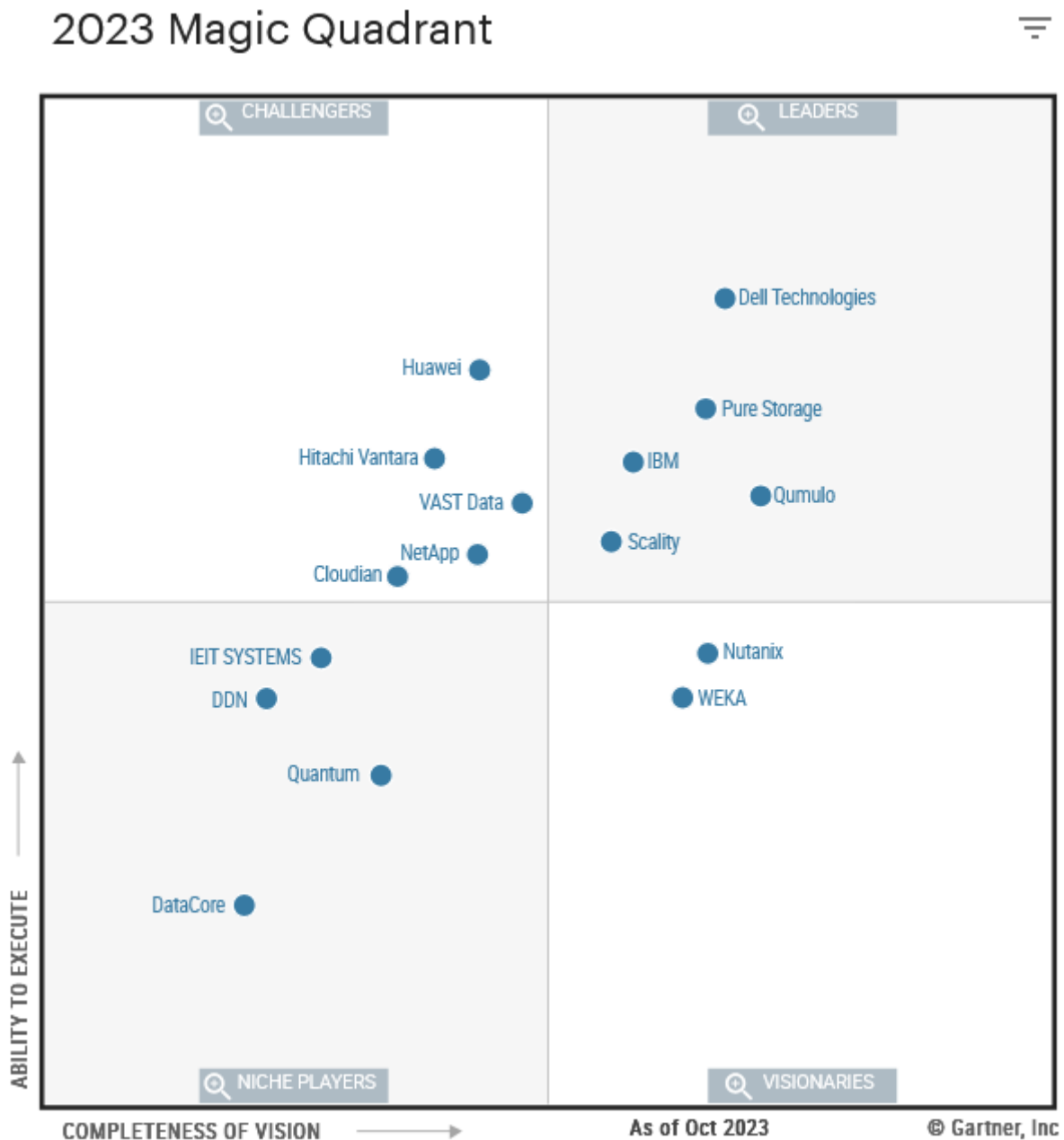


Figura 17 - Quadrante Mágico Gartner de empresas com soluções de armazenamento de dados.

Fonte: <https://www.gartner.com/interactive/mq/4899731?ref=TypeAheadSearch>

8.2.2. De forma análoga, foi realizada avaliação das empresas de mercado de soluções de backup enterprise em estudo realizado pela Gartner a partir do artigo "*Magic Quadrant for Enterprise Backup and Recovery Software Solutions*", publicado em 05/08/2024. Segue o quadrante mágico, conforme artigo:

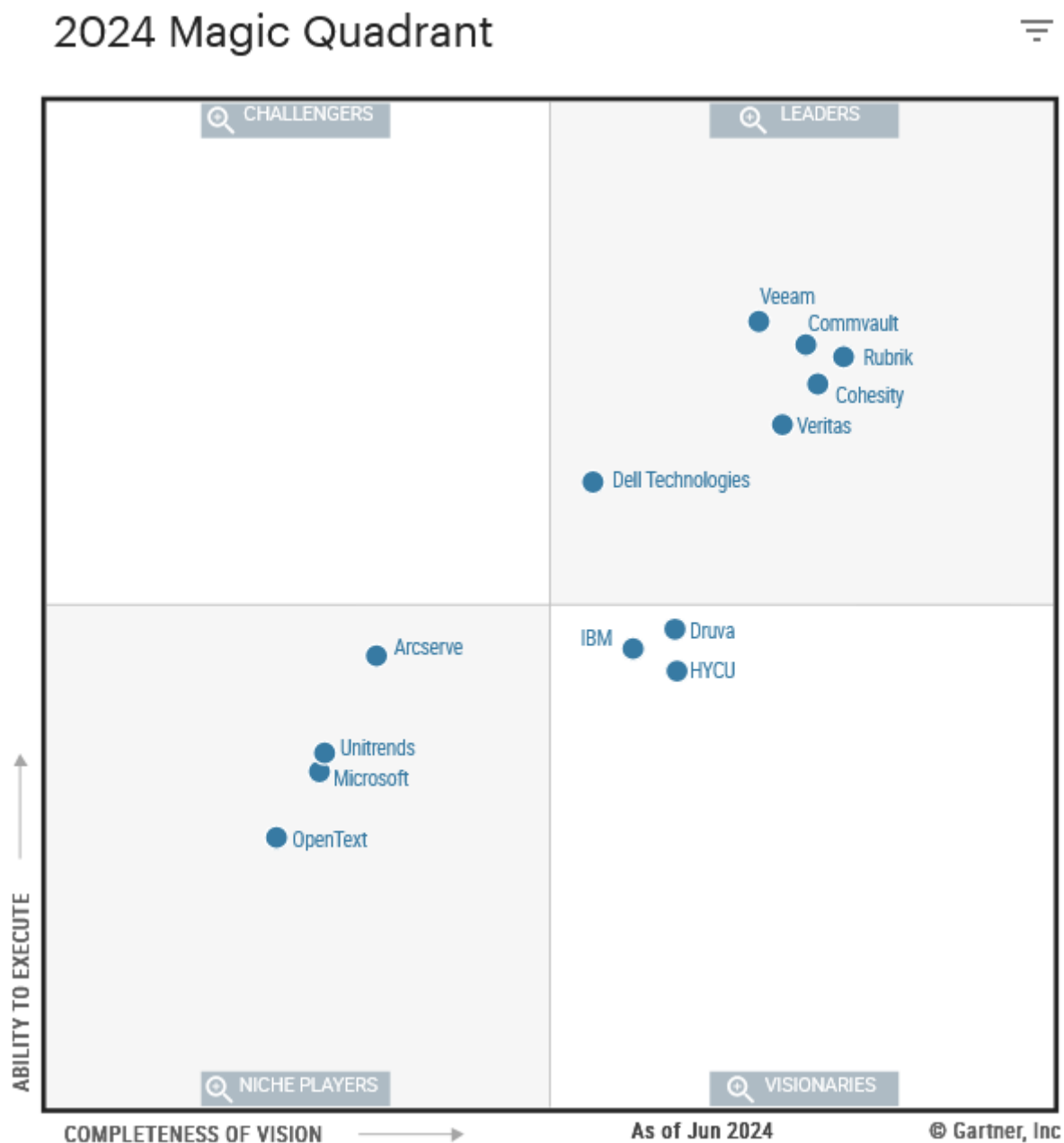


Figura 18 - Quadrante Mágico Gartner de empresas com soluções de backup enterprise.

Fonte: <https://www.gartner.com/interactive/mq/5649023?ref=solrAll&refval=425875494>

8.2.3. Pode-se observar a partir dos artigos da Gartner que há várias empresas que possuem soluções de armazenamento de arquivos e objetos, bem como de soluções de backup, cabendo a esta equipe de planejamento analisar as características técnicas necessárias para atender à demanda atual deste MJSP.

8.2.4. Realizados os estudos de contratações semelhantes e a identificação de fornecedoras de mercado que pudessem atender aos requisitos levantados, esta EPC realizou reunião com fabricantes das soluções que atendiam os requisitos necessários, sendo eles: NETAPP, DELL, HITACHI, IBM, HPe, PURE STORAGE, LENOVO, VERITAS, VEEAM, EXAGRID e COMMVAULT. Nestas reuniões foram apresentadas as soluções dos fabricantes. Também foram discutidas características técnicas e feitas análises sob a perspectiva de mercado para definição das arquiteturas.

8.2.5. Após as reuniões, ficou claro que diversos equipamentos do mercado atendem as necessidades atuais, assim como a superioridade dos equipamentos disponíveis em relação aos equipamentos instalados, visto os grandes avanços da tecnologia nos últimos dez anos. Muitas funções disponíveis nos novos modelos não existem nos storages atuais, principalmente recursos tecnológicos de segurança, recursos de compactação de dados, bem como tecnologias performáticas e que permitem a utilização de inteligência artificial.

8.3. Existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016, e suas atualizações

8.3.1. Esta EPC não identificou nenhuma solução compatível com a demandada dentre aquelas disponibilizadas no portal do Software Público Brasileiro (<https://www.gov.br/governodigital/pt-br/software-publico>, acesso em 16/07/2024), no que se refere a existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016, e suas atualizações.

8.4. Políticas, modelos e padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico – ePing, Modelo de Acessibilidade em Governo Eletrônico – eMag, Padrões Web em Governo Eletrônico – ePwg, padrões de Design System de governo, Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil, quando aplicáveis

8.4.1. As políticas, padrões e modelos eMag, ePwg, padrões de Design System de governo, ICP-Brasil e e-ARQ Brasil não se aplicam à presente contratação.

8.4.2. Após análise detalhada dos Padrões de Interoperabilidade do Governo Eletrônico tem-se que os requisitos técnicos apresentados são aderentes ao ePING. As soluções avaliadas neste ETP são soluções de mercado, amplamente adotadas pelas empresas e órgãos que necessitam de soluções de armazenamento de dados e solução de backup com proteção de dados/segurança. Os requisitos técnicos descritos na seção 5 buscam definir uma solução que amplia o acesso aos sistemas de informação e escaláveis, atendendo ao dimensionamento técnico realizado, bem como de proteção de dados com segurança com backup. Acerca das dimensões semântica e organizacional, apesar de não ser diretamente fornecida pelo objeto da contratação, por meio dele é possível desenvolvê-las, seja pela integração de soluções de software desenvolvida para isto, por projetos que usem os recursos disponibilizados, ou configurando-a para fins de atender às políticas a serem definidas, a exemplo da garantia à privacidade da informação armazenada. Também foram avaliadas as cinco segmentações definidas pelos padrões do ePING (interconexão, segurança, meios de acesso, organização e intercâmbio de informações e área de integração para o Governo eletrônico) sendo observado que a solução a ser adquirida encontra-se aderente, quando aplicável, aos padrões definidos como “adotado” e/ou “recomendado”. De tal forma, esta EPC tem a informar que o presente planejamento de contratação se encontra aderente aos padrões de interoperabilidade do governo eletrônico (ePING) e que tal aderência será também observada quando da elaboração do Termo de Referência e demais artefatos desta contratação.

8.5. Necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual

8.5.1. Não se aplica, pois a infraestrutura básica para instalar as soluções encontram-se prontas nos data centers primário e secundário. Os ajustes finos necessários serão alinhados com os fornecedores das soluções adquiridas.

8.6. Diferentes modelos de prestação do serviço

8.6.1. As possibilidades são abordadas na sessão 9 - ANÁLISE COMPARATIVA DAS SOLUÇÕES.

8.7. Diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes

8.7.1. As soluções consistem basicamente dos itens que seguem:

8.7.1.1. Solução de armazenamento de dados

8.7.1.1.1. Solução de armazenamento NAS de alto desempenho;

8.7.1.1.2. Solução de Armazenamento de Objetos;

8.7.1.1.3. Serviços de Operação Assistida;

8.7.1.1.4. Serviços de Treinamento Teórico/Prático;

8.7.1.1.5. Serviços de Suporte especializado.

8.7.1.2. Solução de Backup de Dados

8.7.1.2.1. Software de Orquestração de Backup;

- 8.7.1.2.2. Solução de Armazenamento para Backup;
- 8.7.1.2.3. Serviços de Operação Assistida;
- 8.7.1.2.4. Serviços de Treinamento Teórico/Prático;
- 8.7.1.2.5. Serviços de Suporte especializado.

8.7.2. Considerando os levantamentos realizados, aventou-se a possibilidade de ser realizada uma “tierização” entre storages, com a finalidade de ser ter um ganho de custo da solução considerando o exposto no item 3.3.2.2. Tal “tierização” vincula o fornecimento dos storages NAS e de Objetos para um mesmo fabricante. Contudo, nas reuniões realizadas com os fabricantes, notou-se que vários possuem tal integração, a exemplo da HITACHI, DELL, IBM, NETAPP e PURE STORAGE. Mesmo considerando os dois storages partes de um mesmo grupo, ainda assim há concorrência no fornecimento de soluções e respectivo ganho financeiro ao adquirir uma solução de armazenamento NAS de menor capacidade e uma de objetos de maior capacidade, sendo o custo do terabyte desta inferior ao daquela, dadas as características das próprias soluções, sem grandes impactos em aspectos técnicos (latência, desempenho de I/O, administração). Ainda há de se considerar que o ganho de escala no fornecimento de uma solução de storage de objetos trará um custo muito menor por terabyte, conforme pode ser observado ao comparar as contratações realizadas no serviço público, pormenorizadas nos itens 8.1.2.5 a 8.1.2.7, a diferença no fornecimento de sistemas de armazenamento de objetos por um mesmo fabricante, nestes casos DELL, chegaram a uma economia considerável por terabyte adquirido.

8.8. Possibilidade de aquisição na forma de bens ou contratação como serviço

8.8.1. As possibilidades são abordadas no item 9. ANÁLISE COMPARATIVA DAS SOLUÇÕES.

8.9. Ampliação ou substituição da solução implantada

8.9.1. A ampliação do ambiente atual levaria a uma menor concorrência considerando que o parque de soluções de armazenamento desta STI/SE/MJSP são dos fabricantes DELL e/ou NETAPP) e para a solução de backup é da fabricante VERITAS. Logo, optou-se por uma nova contratação, sem serviços de migração, para fins de aumentar a competitividade, buscando o menor preço no mercado, atendendo as necessidades de negócio do órgão.

8.10. Métricas de prestação do serviço e de pagamento

8.10.1. Caso algum serviço de nuvem venha e ser escolhido no item que segue, a métrica de prestação do serviço e pagamento serão avaliadas ainda em tempo de elaboração do Termo de Referência.

8.11. Levantamento de soluções

8.11.1. A partir das consultas realizadas, foram delineadas os cenários apresentados abaixo.

8.11.1.1. Solução de Armazenamento e Orquestração de Backup com Replicação de Dados:

- a) Solução 1 - Manutenção dos equipamentos atuais, com adoção de software livre;
- b) Solução 2 - Contratação de nova solução de mercado;
- c) Solução 3 - Adoção exclusiva de armazenamento em nuvem.

9. Análise comparativa de soluções

9.1. A análise comparativa de custos será feita considerando apenas as soluções técnica e funcionalmente viáveis.

9.2. A comparação de custos totais de propriedade (*Total Cost Ownership* - TCO) é realizada por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia, manutenção.

9.3. Para a análise das possíveis soluções, serão considerados fatores tecnológicos ou não, essenciais para manter as funcionalidades de Tecnologia da Informação e Comunicação do Ministério.

9.4. ARMAZENAMENTO DE DADOS E BACKUP

9.4.1. Solução 1 - Manutenção dos equipamentos atuais, com adoção de software livre

9.4.1.1. O presente cenário tem o objetivo de analisar a possibilidade de manutenção e expansão da atual solução de armazenamento.

9.4.1.2. Conforme detalhado no item 3.2 deste ETPC os equipamentos que fazem parte do ambiente de armazenamento dos Data Centers do Ministério foram adquiridos nos anos de 2012 (EMC VNX 7500), 2013 (EMC VNX 5300) e 2014 (NETAPP FAS 8080), operando portanto, em sua grande maioria, há mais de 10 (dez) anos de forma ininterrupta, acima do tempo de vida útil dos equipamentos, que costuma ser de 5 (cinco) anos em média. A obsolescência dos equipamentos gera elevados custos de manutenção corretiva e pode impactar em não atender a alta disponibilidade requerida para o ambiente computacional.

9.4.1.3. Outro fator crucial, quando se fala em manutenção de equipamentos de infraestrutura, é o *End-Of- Life* (fim da vida útil ou descontinuação) por parte dos fabricantes, o que aumenta o risco de manutenção na medida em que se torna cada vez mais difícil a aquisição de peças de reposição, mesmo com a contratação de manutenção e suporte de terceiros.

9.4.1.4. Os equipamentos atuais não possuem capacidade plena para suportar todas as necessidades de armazenamento e backup de dados presentes e os projetadas para um futuro próximo, incluindo performance aquém do demandado pelas aplicações e suporte a novas tecnologias. A solução para isso tem sido movimentar alguns workloads e dados para a nuvem, o que nem sempre é a melhor alternativa do ponto de vista econômico. A expansão necessária da capacidade de armazenamento e backup de dados, considerando as projeções realizadas neste ETP, iria requerer a contratação de módulos de expansão para os equipamentos atuais, o que não se mostra uma alternativa tecnicamente válida em função do limitado tempo de vida e suporte para estes equipamentos, sendo que alguns casos as opções de expansão não estão sequer mais disponíveis.

9.4.1.5. Um fator que impacta a administração e a manutenção dos componentes da infraestrutura em seu último nível de atualização (recomendação para manutenção da segurança) é a dificuldade de compatibilização das versões devido à obsolescência do hardware. O software evolui rapidamente, demandando que o hardware esteja alinhado tecnologicamente ao seu desenvolvimento a fim de suportar suas novas versões. Quando há uma desassociação entre a evolução desses dois componentes, hardware e software, gera-se uma grande dificuldade em se manter a compatibilidade do ambiente, impedindo seu crescimento (inclusão de novos componentes e discos), e gera-se outra grande dificuldade em atualizar sistemas operacionais e aplicativos para funcionarem com as correções mais recentes de segurança, acarretando um ambiente vulnerável ciberneticamente, sujeito a ataques e vazamentos de informações sensíveis e importantes para o Ministério.

9.4.1.6. A análise até aqui demonstra a inviabilidade por si só no que se refere a possibilidade de manutenção e expansão do atual parque da forma como está. No entanto, outro fator a ser considerado no presente cenário é a necessidade de atualização tecnológica da camada de armazenamento. Atualmente, o Ministério não possui nenhum repositório local para armazenamento de objetos. Ao contrário do que estamos acostumados a ver nos equipamentos tradicionais de armazenamento, nos quais o armazenamento é feito em blocos ou arquivo, o armazenamento de objetos é totalmente voltado à escalabilidade, disponibilidade e eficiência máxima para leitura. Isso significa que ao armazenar os dados em um object storage, esses serão automaticamente distribuídos de forma segura por toda infraestrutura da cloud privada, de forma a garantir sua disponibilidade e durabilidade. Hoje o Ministério não possui nenhum object storage em seu parque, utilizando para sanar essa falta os recursos da nuvem pública.

9.4.1.7. No que diz respeito aos equipamentos e software de backup, ao optar por esse cenário, teríamos como vantagem o aproveitamento de alguns dos investimentos já feitos anteriormente, exclusivamente com relação ao licenciamento, já que os appliances alcançaram o período de *end of life*. Diferentemente de outras ferramentas, a troca de um software gerenciador de backup pode ser mais complexa e demorada, pois implica na necessidade de manter 02 (duas) soluções em funcionamento ou de efetuar a migração de todo o legado através da nova solução e mesmo nesse caso, todo o histórico de *metadados* do banco de dados (catálogo) teria que ser refeito na nova solução. Na última contratação realizada pelo Ministério, tínhamos como vantagem a possibilidade de manter os appliances da Veritas, o que não se aplica atualmente.

9.4.1.8. Com relação ao licenciamento, conforme mencionado anteriormente, a atual solução de backup está licenciada por volumetria (FETB) e socket. Quando um software de backup é alterado, existem duas possibilidades mais usuais:

- a) Manter a solução antiga em funcionamento até que todos os backups expirem a data de proteção, ou;
- b) Restaurar todos os backups da solução antiga e refazê-los na nova solução.

9.4.1.9. No caso do cenário "a", o órgão trabalharia com suas soluções de backup simultâneas, até a expiração da data de proteção, conforme política interna de backup de dados. No caso do cenário "b", seria necessário a previsão de um item para a migração dos dados legados de backup em fita para a nova solução, o que acarretaria maiores custos para a adoção deste cenário, além das dificuldades técnicas de migração de tecnologias distintas de soluções de backup.

9.4.1.10. Temos hoje os seguintes direitos ativos de produtos Netbackup Veritas em nome do Ministério, conforme dados extraídos do portal <https://vems.community.veritas.com/vems/entitlements>:

Product Name	Entitled Quantity	Entitlement Status	Service Expiration	Service Status
NETBACKUP PLATFORM DATA PROTECTION OPTIMIZATION ADDON XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE	5	ACTIVE	2014-12-31	Expired
NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE	20	ACTIVE	2015-12-31	Expired
NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE	30	ACTIVE	2019-11-25	Expired
NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE	30	ACTIVE	2018-11-26	Expired
NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE	30	ACTIVE	2022-02-28	Expired
NETBACKUP ENTERPRISE VIRTUAL CLIENT WLS CPU HARDWARE TIER 4 ONPREMISE STANDARD PERPETUAL LICENSE	48	ACTIVE	2022-02-28	Expired

Tabela 18 - Licenciamento atualmente contratado (Veritas Netbackup).

9.4.1.11. Conforme já explanado anteriormente, a atual solução tem se mostrado insuficiente e não mais atende aos requisitos do Ministério, tanto no aspectos quantitativo, como qualitativo:

- a) Os appliances estão com a utilização acima do permitido, tendo sido necessário a criação de appliances virtuais para suprir a necessidade por armazenamento;
- b) Os appliances encontram-se na última versão suportada, porém estão com o End of Life anunciado pelo fabricante;
- c) Necessidade de uma solução mais moderna e eficiente para armazenamento e recuperação do backup e longa retenção;
- d) Detecção e proteção de ataques do tipo *ransomware*.

9.4.1.12. Nesse cenário, poderíamos ainda, se fosse possível utilizar o hardware já adquirido, manter os equipamentos atuais e adotar uma solução de software livre. Esta alternativa traria uma série de riscos relacionados à capacidade de sustentação da infraestrutura de backup, incompatíveis com a criticidade dos negócios suportados por meio dos sistemas providos a partir dos data centers do MJSP.

9.4.1.13. Ainda, conforme levantamento de softwares disponíveis no portal do Software Público, não foi encontrado nenhuma solução que atendesse aos requisitos do Ministério por completo (site: <http://www.softwarepublico.gov.br>, acessado em 05/09/2023 às 13:14, palavra-chave "backup").

CATÁLOGO DE SOFTWARE PÚBLICO

Resultado da pesquisa

PESQUISAR CATÁLOGO DE SOFTWARE

☒ Todos ☐ Software Público

BACKUP

FILTRO

MAIS OPÇÕES

0 Software(s)

Exibir: 15 Ordenar por: Avaliação

Nenhum software encontrado. Tente outros filtros

Figura 19 - Catálogo do Software Público.

9.4.1.14. Dessa forma, seguindo o Guia de Boas Práticas da STI/MP, o acórdão TCU *n. 2400/2006*, e considerando ainda a necessidade de expansão e atualização da camada de armazenamento e backup, a equipe de planejamento da contratação entende que a aquisição do serviço de garantia e suporte técnico **não é uma solução viável**, pois não resolveria as limitações de capacidade atual ou demandaria a contratação de expansões para equipamentos em fim de vida e implicaria em risco elevado para a operação dos serviços críticos de tecnologia da informação providos pelo Ministério, devido à indisponibilidade de suporte aos equipamentos por parte do fabricante e a desatualização tecnológica da atual solução.

9.4.2. Solução 2 - Contratação de nova solução de mercado

9.4.2.1. Este cenário tem por objetivo avaliar a aquisição de uma nova solução de armazenamento do tipo Storage NAS e Object Storage, bem como uma solução de backup, para substituir os atuais equipamentos. Nesse cenário, teríamos dois storages do tipo NAS (Tipo 1 e Tipo 2) para uso do file server e armazenamento NFS, nos dois sites do Ministério. Esses dois equipamentos operariam de forma redundante, com replicação de parte dos dados para o site secundário. A principal diferença entre o tipo 1 e o tipo 2 seria basicamente com relação a capacidade de armazenamento, que no storage secundário seria de 2/3 do primário.

9.4.2.2. Um aspecto importante com relação aos equipamentos de armazenamento é a sua capacidade de armazenar dados (evidentemente), e em segundo lugar, como ampliar essa capacidade de forma rápida, simples e sustentável, em caso de necessidade. Considerando esse requisito, é mandatório, nesse projeto, que o equipamento a ser adquirido seja escalável e do tipo scale-out.

9.4.2.3. Outro aspecto é o quesito de performance dos storages NAS. A necessidade de disponibilização de performance às aplicações corporativas, que tem sido impactadas com o nível de iops disponíveis nos equipamentos atuais, conforme apresentado na sessão 1, tem gerado problemas e impactos aos níveis mínimos necessários para atendimento das necessidades do MJSP. Atualmente os equipamentos disponíveis no mercado atual possuem dois tipos de tecnologia: all-flash e híbrida. Notoriamente, a performance dos equipamentos all-flash é maior, mas também com custo acima daqueles equipamentos com tecnologia híbrida. Esta EPC, tendo em vista que a atual tecnologia adotada nos equipamentos é a híbrida e que não tem atendido as necessidades de usuários e das aplicações, entende que a adoção da mesma tecnologia híbrida para os novos equipamentos continuaria a trazer impactos negativos aos objetivos e necessidades do órgão. Desta forma, a tecnologia escolhida foi a all-flash, para os fins de ganhos de performance e recursos tecnológicos para a nova infraestrutura a ser adquirida.

9.4.2.4. Com relação ao object storage, a proposta é que os dois equipamentos sejam idênticos e que cada um deles fique em um dos sites. Conforme já mencionado nos tópicos anteriores, eles terão, basicamente, duas finalidades: camada para proteção do NAS e hospedagem de objetos.

9.4.2.5. Há alguns aspectos importantes com relação ao storage objeto que merecem ser destacados. O storage objeto tem uma diferença fundamental em relação ao NAS. Ele se comporta como sendo um serviço de nuvem. Não é preciso estar fisicamente ligado ao mesmo data center para acessá-lo. Na verdade, replicação, se houver, será a

nível de conteúdo e não do storage. Então, podemos, por exemplo, dizer o seguinte: temos dois storages, um em cada data center, que são vistos pelas aplicações como único storage lógico. Não há a preocupação se quem está acessando o storage, no caso do storage objeto, é uma máquina que está no mesmo data center do local onde está gravado. Isso não é um pré-requisito para o storage objeto. Podemos ter perfeitamente um workload que está rodando em um determinado data center, acessar um conteúdo que está no storage objeto fisicamente, armazenado em um outro data center, sem nenhum problema. Se houver necessidade de criar resiliência com o storage objeto, será no nível do conteúdo. Poderíamos, por exemplo, criar uma política e informar o seguinte: pra esse repositório eu tenho uma política interna de replicação que garante que iremos ter esse mesmo conteúdo gravado nos dois storage objeto. A nível de aplicação isso é transparente. Daí a diferenciação em relação a outros storages tradicionais.

9.4.2.6. Este cenário implica na aquisição de novo hardware de Storage, com todo o licenciamento de software no modelo de licença perpétua. Não se aplica ao presente cenário o licenciamento de software por subscrição, dado que o mercado não comercializa storage com camada de software por subscrição.

9.4.2.7. No que tange ao backup, ao optar por esse cenário, o Ministério se propõe a contratar uma nova solução de backup de forma aberta, sem especificar fabricante. Esse cenário pode se mostrar favorável com relação a ampliação da competitividade, além da liberdade de incluir novas tecnologias e arquiteturas previstas em soluções de outros fabricantes.

9.4.2.8. A esse respeito, é muito importante citar os recentes ataques do tipo *ransomware* às organizações. Recentemente, devido a relevância do tema, o Tribunal de Contas da União, através do Acórdão 1.109/2021 – Plenário, ressaltou a importância dos procedimentos de backup nas organizações públicas federais. Entre os principais pontos de atenção elencados pelo órgão de controle, citamos:

- a) Realize cópias de segurança (backups) de todos os dados da organização, de forma regular e automática;
- b) Realize cópias de segurança (backups) integrais dos sistemas críticos da organização, de modo a permitir sua rápida recuperação em caso de necessidade;
- c) Realize, periodicamente, testes de restauração (restore) das cópias de segurança (backups) da organização, de modo a atestar seu funcionamento em caso de necessidade;
- d) Proteja adequadamente as cópias de segurança (backups) da organização, por meio de mecanismos de controle de acesso físico e lógico;
- e) Armazene as cópias de segurança (backups) da organização em ao menos um destino não acessível remotamente.

9.4.2.9. Ainda nesse contexto, a Secretaria de Governo Digital do Ministério da Economia, publicou em maio de 2022 um Modelo de Política de Backup, com o objetivo de fornecer aos gestores de TIC orientações para mitigação de possíveis riscos ligados às temáticas de privacidade e segurança da informação relativos aos seus sistemas informacionais.

9.4.2.10. Entre as recomendações está a de manter uma infraestrutura de backup apartada, lógica e fisicamente, dos sistemas críticos da organização.

9.4.2.11. Diante do exposto, a equipe de planejamento da contratação entende que esse cenário é o mais adequado nesse momento, por possibilitar o reposicionamento do Ministério diante das novas tecnologias, além da remodelagem da atual arquitetura de armazenamento.

9.4.3. Solução 3 - Adoção exclusiva de armazenamento em nuvem

9.4.3.1. O presente cenário tem o objetivo de analisar a possibilidade de adotar a computação em nuvem pública para todos os serviços e aplicações do Ministério.

9.4.3.2. Conforme já exposto no item 3.2 deste ETPC, o Ministério centraliza seus serviços baseados em Tecnologia da Informação em data centers com infraestrutura local (on-premises), que se destinam à hospedagem de sistemas legados e sistemas com grau de restrição, além de contratos de nuvem (on-cloud) com a Microsoft (Azure) e com a Oracle (Oracle Cloud).

9.4.3.3. Importante destacar que o modelo de infraestrutura de nuvem pretendido no âmbito do MJSP, se baseia no conceito de nuvem híbrida (inciso IV, Art. 3º da INSTRUÇÃO NORMATIVA Nº 5, DE 30 DE AGOSTO DE 2021), composta pela nuvem privada (Salas Cofres on-premises) e nuvem pública (Microsoft Azure e Oracle Cloud).

9.4.3.4. Cabe destacar que a STI/MJSP vislumbra benefícios na adoção de serviços de computação em nuvem nas modalidades infraestrutura e plataforma como serviço, sendo esta uma tendência a médio e longo prazo. No entanto, deve ser considerado que já foram feitos investimentos consideráveis em infraestrutura própria de TIC, justamente por acreditar que o modelo de nuvem híbrida oferece um conjunto único e contínuo de recursos que atendem às estratégias e iniciativas de transformação digital do Ministério.

9.4.3.5. Destaca-se que existem algumas estratégias iniciais no MJSP para adoção de serviços de computação em nuvem. Atualmente o Ministério conta com o contrato nº 46/2021 (SEI nº 15305041), que disponibiliza créditos na Azure Public Cloud, da Microsoft. No entanto, mesmo considerando o uso atual das soluções de IaaS e PaaS do fornecedor, a estratégia do MJSP para a sustentação de serviços de TIC não permite prescindir de infraestrutura on-premise, por considerar que ainda há grande risco para a sustentação e operação de serviços críticos caso seja feita a opção pela adoção de infraestrutura puramente em nuvem, pois, neste caso, não existiria uma alternativa para manter a sustentação dos sistemas corporativos caso houvesse alterações nas previsões orçamentárias ou na política de preços dos fornecedores. É dentro desse contexto que a instituição considera ser necessário dotar a infraestrutura de data center local de recursos mínimos capazes de garantir a alta disponibilidade dos serviços.

9.4.3.6. Além disso, não se vislumbra a computação em nuvem como alternativa técnica viável para a operacionalização de sistemas legados que permanecem sendo utilizados no âmbito da instituição, e tampouco há alternativa para a sustentação segura desses sistemas on-premise sem que haja um reforço das condições de infraestrutura hoje existentes, além do fato que o reforço dessa infraestrutura atua no sentido de preservar os investimentos já realizados.

9.4.3.7. Dessa forma, a equipe de planejamento contratação entende que a adoção de computação em nuvem pública para todos os serviços e aplicações do Órgão, não é uma solução viável, por considerar que ainda há grande risco para a sustentação e operação de serviços críticos caso seja feita a opção pela adoção de infraestrutura puramente em nuvem.

10. Análise comparativa de custos (TCO)

11.1. Não se aplica, pois apenas 1 (uma) solução se mostrou viável não sendo possível realizar comparação com outra, conforme previsto no art. 11, § 1º da INSTRUÇÃO NORMATIVA SGD/ME Nº 94, DE 23 DE DEZEMBRO DE 2022.

11. Registro de soluções consideradas inviáveis

11.1. Conforme § 1º do art. 11, da INSTRUÇÃO NORMATIVA SGD/ME Nº 94, DE 23 DE DEZEMBRO DE 2022, as soluções identificadas no inciso II consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação, dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

11.2 - ARMAZENAMENTO DE DADOS E BACKUP

11.2.1. Solução 1 - Foi analisada a possibilidade de manutenção e expansão da atual solução com aproveitamento dos investimentos já efetuados. De forma resumida, esse cenário foi considerado inviável pelos seguintes motivos:

- a) Equipamentos alcançaram o end-of-life;
- b) Licenciamento por socket descontinuado pela Veritas;
- c) Licenciamento por FETB insuficiente para as atuais necessidades do Ministério;
- c) Necessidade de atualização tecnológica no que se refere a mudança de arquitetura, com inclusão de uma camada de proteção contra ataques do tipo ransomware.
- d) A adoção de uma solução de Software Livre foi considerada inviável pela indisponibilidade uma solução que atendesse por completo as necessidades do Ministério. E mesmo se houvesse uma solução de Software Livre, seria imprescindível a customização, evolução e manutenção dessa solução, o que não se mostra um cenário favorável.

11.2.2. Solução 3 - Foi analisada a possibilidade de adoção exclusiva de armazenamento em nuvem. A possibilidade de adotar exclusivamente o armazenamento em nuvem foi considerada na análise. No entanto, concluiu-se que essa abordagem não é viável devido ao alto risco envolvido na ampla implementação da computação em nuvem pública para todas as atividades e sistemas do Órgão.

11.2.2.1. A principal razão para essa conclusão é a avaliação de que adotar uma infraestrutura baseada apenas na nuvem traria consigo um nível significativo de risco quando se trata de manter e operar os serviços críticos do Órgão. Isso implica que a dependência exclusiva da nuvem poderia comprometer a estabilidade e a disponibilidade desses serviços essenciais, o que é inaceitável para o funcionamento adequado da organização. Portanto, a equipe de planejamento de contratação considerou que é prudente buscar uma abordagem mais equilibrada e flexível em relação à infraestrutura de TI, levando em conta a natureza crítica de certos serviços.

12. Descrição da solução de TIC a ser contratada

12.1. Trata-se da aquisição de solução de armazenamento de dados e solução de backup, para fins de reestruturação de infraestrutura dos data centers do MJSP, para fins de substituir o parque atual de infraestrutura de armazenamento e backup obsoleto, limitado e sem suporte, além de suprir as demandas corporativas do MJSP com novas soluções tecnológicas modernas e atualizadas. As soluções a serem contratadas fazem parte do projeto de instalação e implantação de nuvem privada do MJSP.

12.2. Além dos equipamentos de armazenamento e de backup, com garantia, suporte técnico e instalação inclusos, também serão contratados serviços de operação assistida para monitoramento do funcionamento das soluções e repasse de conhecimento, serviço de treinamento para capacitação da equipe técnica e de colaboradores da STI/SE /MJSP e serviços de suporte especializado para apoio na implantação de projetos.

12.3. As soluções a serem adquiridas serão implantadas nos data centers do MJSP, de acordo com cronograma de contratação e de implantação das soluções.

12.4. A solução escolhida encontra-se detalhada no item 9.4.2 e as especificações técnicas das soluções de armazenamento encontram-se detalhadas nas seções 3 e 5.

12.5. Após os estudos realizados tem-se na tabela a seguir os itens que seriam os objetos relativos a esta contratação:

GRUPO 1 – Soluções de Armazenamento de Dados e Serviços

ITEM	ESPECIFICAÇÃO	CATMAT/ CATSER	UNIDADE DE MEDIDA	QUANTIDADE
1	Solução de Armazenamento NAS de alta performance Scale-Out (Storage All Flash NVMe) – Tipo 1, com capacidade útil de 412 TiB, garantia, manutenção e suporte técnico de 60 meses, instalação e implantação inclusos	404135	Unidade	1
2	Solução de Armazenamento NAS de alta performance Scale-Out (Storage All Flash NVMe) – Tipo 2, com capacidade útil de 274 TiB, garantia, manutenção e suporte técnico de 60 meses, instalação e implantação inclusos	404135	Unidade	1

3	Solução de Armazenamento de Objetos Scale-Out, com capacidade útil de 420 TiB, garantia, manutenção e suporte técnico de 60 meses, instalação e implantação inclusos	404135	Unidade	2
4	Serviços de Operação Assistida	27332	Horas	320
5	Serviços de Treinamento Teórico/Prático (Turma)	3840	Turma	4
6	Serviços de Suporte Especializado	27332	Horas	800

GRUPO 2 – Solução de Backup de Dados e Serviços

ITEM	ESPECIFICAÇÃO	CATMAT/ CATSER	UNIDADE DE MEDIDA	QUANTIDADE
11	Software de orquestração de backup e replicação de dados (152TiB de front end ou), com garantia, manutenção e suporte técnico por 60 meses, instalação e implantação inclusos	27464	Unidade	1
12	Appliance para armazenamento de backup com deduplicação e capacidade útil de 400 TiB, garantia, manutenção e suporte técnico de 60 meses, instalação e implantação inclusos	404135	Unidade	2
13	Serviços de Operação Assistida	27529	Horas	160
15	Serviços de Treinamento Teórico/Prático	16837	Turma	4
17	Serviços de Suporte Especializado	27332	Horas	800

13. Estimativa de custo total da contratação

Valor (R\$): 17.358.114,40

13.1. Conforme o "Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação" V 3.0 do SISP, o orçamento informado nesse momento é preliminar. Ele deverá ser suficiente na análise de custo total de propriedade para a escolha da solução. **O orçamento detalhado será realizado na confecção do Termo de Referência.**

13.2 Tendo em vista durante esse estudo optarmos por separar as contratações uma vez que tratam-se e objetos distintos, os custos serão apresentados de forma separada por grupos. Os valores foram baseados em pesquisas

preliminares de editais, contratos e com fornecedores, conforme levantamento realizado em planilha (SEI 29171334) anexa.

13.3 GRUPO 1

Valor: R\$ 8.726.411,20

Item	Descrição	Quantidade	Volumetria (TiB) ou unidade	Custo Unitário	Valor Unitário Máximo (60 meses)	Valor Total Máximo
1	Solução de Armazenamento NAS de alta performance Scale-Out (Storage All Flash NVMe) – Tipo 1, com capacidade útil de 412 TiB, garantia, manutenção e suporte técnico de 60 meses, instalação e implantação inclusos	1	412 TiB	R\$ 109,65	R\$ 2.710.548,00	R\$ 2.710.548,00
2	Solução de Armazenamento NAS de alta performance Scale-Out (Storage All Flash NVMe) – Tipo 2, com capacidade útil de 274 TiB, garantia, manutenção e suporte técnico de 60 meses, instalação e implantação inclusos	1	274	R\$ 109,65	R\$ 1.802.646,00	R\$ 1.802.646,00
3	Solução de Armazenamento de Objetos Scale-Out, com capacidade útil de 420 TiB, garantia, manutenção e suporte técnico de 60 meses, instalação e implantação inclusos	2	420	R\$ 81,91	R\$ 2.064.132,00	R\$ 4.128.264,00
4	Serviços de Operação Assistida	160	Horas	R\$ 276,56	R\$ 276,56	R\$ 44.249,60
5	Serviços de Treinamento Teórico/Prático	4	Unidade	R\$ 2.035,18	R\$ 40.703,60	R\$ 40.703,60
6	Serviços de Suporte Especializado	800	Horas	R\$ 322,17	R\$ 322,17	R\$ 257.736,00

Tabela 19 - Estimativa de Custo Preliminar: Grupo 1.

13.3 GRUPO 2

Valor: R\$ 8.631.703,20

Item	Descrição	Quantidade	Volumetria (TiB) ou unidade	Custo TB/Mês Pesquisa	Valor Unitário Máximo (60 meses)	Valor Total Máximo (60 meses)
7	Software de orquestração de backup e replicação de dados, com garantia, manutenção e suporte técnico	1	152	R\$ 191,42	R\$ 1.745.750,40	R\$ 1.745.750,40

	por 60 meses, instalação e implantação inclusos					
8	Appliance para armazenamento de backup com deduplicação e capacidade útil de 400 TiB, garantia, manutenção e suporte técnico de 60 meses, instalação e implantação inclusos	2	400	R\$ 135,47	R\$ 3.251.280,00	R\$ 6.502.560,00
9	Serviços de Operação Assistida	160	Horas	R\$ 276,56	R\$ 276,56	R\$ 44.249,60
10	Serviços de Treinamento Teórico/Prático	4	Unidade	R\$ 2.035,18	R\$ 81.407,20	R\$ 81.407,20
11	Serviços de Suporte Especializado	800	Horas	R\$ 322,17	R\$ 322,17	R\$ 257.736,00

Tabela 20 - Estimativa de Custo: Grupo 2.

13.1. Desse modo, o valor previsto para a presente contratação é de **R\$ 8.726.411,20 (oito milhões, setecentos e vinte e seis mil, quatrocentos e onze reais e vinte centavos)** para a solução de armazenamento e **R\$ 8.631.703,20 (oito milhões, seiscentos e trinta e um mil, setecentos e três reais e vinte centavos)** para solução de backup.

13.2 Totaliza-se assim o valor global de **R\$ 17.358.114,40 (dezessete milhões, trezentos e cinquenta e oito mil, cento e quatorze reais e quarenta centavos)**.

14. Justificativa técnica da escolha da solução

14.1. Diante de todo o exposto, a equipe de planejamento da contratação entende que o cenário de "Contratação de nova solução de mercado" é o mais adequado nesse momento, por possibilitar o reposicionamento do Ministério diante das novas tecnologias, além da remodelagem da arquitetura de backup e armazenamento de dados com o acréscimo de tecnologias para proteção das cópias de segurança contra ataques de ransomware. Além disso, este cenário contempla plenamente as necessidades de expansão da capacidade de armazenamento e backup de dados e o aumento da performance de acesso a dados e de recuperação no caso de desastres, através da modernização dos equipamentos.

14.2. A solução adquirida engloba serviços de instalação e implantação, configuração, suporte técnico, transferência de conhecimento na Tecnologia e suporte especializado.

14.3. As principais soluções do objeto, assim como os respectivos serviços de instalação, suporte e garantia do fabricante, incluindo apoio em configurações, e os serviços de repasse de conhecimento são dependentes entre si e devem ser executados por empresa que possui expertise no provimento de solução de armazenamento e backup, logo o parcelamento da aquisição desses serviços em grupos separados comprometeria o conjunto da solução por separar serviços com alto grau de interdependência.

14.4. Conforme explicita o item 3.8, alínea a, do Anexo III da IN 05/2017 da SEGES/MPOG:

"O parcelamento da solução é a regra devendo a licitação ser realizada por item, sempre que o objeto for divisível, desde que se verifique não haver prejuízo para o conjunto da solução ou perda de economia de escala, visando propiciar a ampla participação de licitantes, que embora não disponham de capacidade para execução da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas;"

14.5. Conforme preconizado na alínea “b” do Art. 40 da Lei 14.133/2021, “do parcelamento, quando for tecnicamente viável e economicamente vantajoso”. Tal conceito foi estritamente observado no presente processo, procedendo-se o agrupamento dos equipamentos, em virtude da interdependência entre eles.

14.6. Os equipamentos e serviços de instalação, configuração e manutenção são interdependentes, sendo inviável, no quesito técnico, a contratação de empresas distintas para execução dos mesmos, sob o risco de inexecução do objeto como um todo.

14.7. O ambiente cujos serviços serão implementados configuram um conjunto indissociável, razão por que, qualquer inconformidade ou eventual indisponibilidade de quaisquer conjuntos de conexões podem comprometer o andamento das atividades internas administrativas e/ou operacionais, necessitando sempre de sua disponibilidade e completa solução.

14.8. Por tal fato, somente a contratação de forma integrada dos equipamentos, ou seja, com adjudicação por preço global para cada item (Solução de Armazenamento, Solução de Backup de Dados e Solução de Proteção de Dados para Backup), e com a garantia da interoperabilidade e fornecimento dos mesmos durante a execução dos serviços, mitiga os riscos a preservação do cenário ideal, uma vez que asseguram a conservação das características originais da solução integrada, além da operação ininterrupta do ambiente, evitando transferência de responsabilidade, no caso de eventuais problemas causados por erro nas execuções ou vícios ocultos, que inviabilizem uma imediata definição de responsabilidades, ou até mesmo a deserção de eventual componente.

14.9. Por tais razões, é inadequada e inviável, sob o ponto de vista técnico e do interesse público, a contratação individual dos equipamentos e serviços, bem como a divisão do objeto da presente licitação em parcelas maiores. Há a necessidade de execução integral para que possa estar em condições de funcionamento.

14.10. Quanto ao parcelamento da contratação decorrente de aspectos técnicos, tem-se a informar que o estudo de dimensionamento foi realizado criteriosamente para atender as demandas de todas as unidades do MJSP. As soluções de armazenamento NAS e de objetos são interdependentes entre si, de forma que tanto a tierização quanto as funções de replicação precisam funcionar em harmonia e só é possível garantir essa relação com o fornecimento em conjunto. Não há garantia para a Administração, caso a solução fosse contratada com adjudicação por itens separados, de compatibilidade entre as soluções a serem contratadas, causando danos aos objetivos do projeto em andamento.

14.11. Por outro lado, o objeto foi dividido em tantos itens quanto possíveis para fins de individualização das suas partes e para clareza quanto à classificação orçamentário-financeira, entretanto, não é viável tecnicamente a adjudicação individualizada em itens, dada a interdependência citada. Também no caso em comento, a centralização da responsabilidade em uma única empresa contratada, para implantação da solução e para acompanhamento de problemas e soluções, facilitaria a verificação das suas causas e atribuição de responsabilidade, aumentando o controle sobre a execução do objeto (crítico para o órgão). Contudo, vê-se a possibilidade de aquisição parcelada no tempo das soluções de armazenamento e backup, tendo em vista que é possível a segmentação da implantação da infraestrutura para o data center principal e data center secundário.

14.12. Os Termo de Referência foram definidos de acordo com a natureza de cada objeto, contendo a seguinte disposição:

a) Grupo 1: Solução de armazenamento de dados e serviços;

b) Grupo 2: Solução de backup de dados e serviços.

14.13. Desse modo, a adjudicação em grupos visa:

a) promover o ganho em escala, no que se refere ao preço ofertado;

b) reduzir o risco de incompatibilidade entre equipamentos;

c) Diante do exposto, entende-se que a contratação dos produtos e serviços que a princípio compõem a demanda em atendimento deve ser feita em quatro grupos.

15. Justificativa econômica da escolha da solução

15.1. Não se aplica, pois apenas 1 (uma) solução se mostrou viável não sendo possível realizar comparação com outra, conforme previsto no art. 11, § 1º da INSTRUÇÃO NORMATIVA SGD/ME Nº 94, DE 23 DE DEZEMBRO DE 2022.

16. Benefícios a serem alcançados com a contratação

16.1. Espera-se alcançar os seguintes benefícios com a presente contratação:

- a) Amplificação da camada de armazenamento e disponibilidade da informação;
- b) Gerar meios de economia de espaço de armazenamento por meio de técnicas de arquivamento;
- c) Adequação das licenças e serviços às necessidades atuais do Ministério da Justiça e Segurança Pública;
- d) Possibilitar a otimização das rotinas de backup e de restauração de dados, de maneira que tais operações sejam realizadas em períodos menores e com maior confiabilidade, visando o restabelecimento de sistemas, banco de dados e serviços do Ministério;
- e) Reduzir o risco de indisponibilidades e perda de integridade de dados, relacionados à falta de garantia e suporte especializado no software atualmente em produção na infraestrutura da rede do Ministério;
- f) Atendimento ao período de retenção de dados pessoais previstos na Política de Backup do MJSP e na LGPD;
- g) Modernização dos data centers do MJSP, com implantação de infraestrutura hiperconvergente e nuvem privada, com soluções de armazenamento performáticas e especializadas, bem como solução de backup com segurança avançada para os dados corporativos.

17. Providências a serem Adotadas

17.1. Providências decorrentes desta contratação:

Tipo de Adequação	Descrição
Infraestrutura Tecnológica	O ambiente de TIC do Ministério já se encontra em condições adequadas para receber a solução requisitada.
Infraestrutura Elétrica	Os data centers do Ministérios já possuem todos os requisitos elétricos para atender a solução
Logística	A solução será baseada em máquinas do tipo Appliance, portanto, é aderente e totalmente adaptável ao ambiente do Ministérios. A logística envolve apenas a entrega do equipamento e a definição do local de instalação. Neste caso, os data centers já estão preparados para receber os equipamentos.
Espaço físico	Deverá ser oferecido ambiente para alocação de pessoal que realizará o serviço no órgão.
Mobiliário	Não necessita de adequações.
Outros	Viabilizar a entrada e a permanência dos técnicos no data center para instalação da solução
Acompanhamento Contratação	Acompanhar o andamento da contratação de hiperconvergência (SEI nº 08006.000626/2023-72), uma vez que existe um relacionamento da solução proposta naquela contratação e nesta, visando o objetivo maior de reestruturar toda a capacidade de processamento, armazenamento e backup de dados do Ministério da Justiça e Segurança Pública.

Tabela 21 - Tipos de Adequação.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

18.1. O Estudo Técnico Preliminar desta contratação enfatiza que a abordagem mais eficaz para alcançar os resultados desejados, minimizar riscos e aderir aos princípios de economia, eficácia e eficiência é conduzir um processo de aquisição que inclua uma solução de armazenamento de dados, contemplando storages de rede (NAS/Object Storage) e solução de backup de dados, incluindo softwares e appliances, além de serviços. Essa solução deve ter uma garantia integral de 60 meses para atender às necessidades do Ministério da Justiça e Segurança Pública.

18.2. Diante do exposto, a equipe de planejamento declara ser viável a contratação da solução pretendida.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

RODRIGO ALBERNAZ BEZERRA

Integrante Técnico



Assinou eletronicamente em 10/01/2025 às 17:15:32.

LEONARDO GARCIA GRECO

Integrante Requisitante



Assinou eletronicamente em 13/01/2025 às 13:19:47.

SOLANGE BERTO DE MEDEIROS

Autoridade Máxima de TIC



Assinou eletronicamente em 15/01/2025 às 11:38:26.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Pesquisa_Preco_ETP.xlsx (117.8 KB)