

ANEXO I-A – ESPECIFICAÇÕES TÉCNICAS DAS SOLUÇÕES

Registro de Preços para aquisição de soluções de armazenamento de dados, contemplando storages de rede (NAS e Object Storage), e solução de backup de dados, incluindo software e appliances, além de serviços de operação assistida, treinamento e suporte especializado, com garantia integral de 60 (sessenta) meses, para atendimento das necessidades do Ministério da Justiça e Segurança Pública, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

GRUPO 1 – Soluções de Armazenamento de Dados e Serviços

ITEM	ESPECIFICAÇÃO	CATMAT/ CATSER	UNIDADE DE MEDIDA	QTDE.
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	160
5	Serviços de Treinamento Teórico/Prático (Turma)	3840	Unidade	2
6	Serviços de Suporte Especializado	27332	Horas	800

GRUPO 2 – Solução de Backup de Dados e Serviços

ITEM	ESPECIFICAÇÃO	CATMAT/ CATSER	UNIDADE DE MEDIDA	QTDE.
7	Software de orquestração de backup e replicação de dados, com garantia, manutenção e suporte técnico por 60 meses, instalação e implantação inclusos	27480	Unidade	1
8	Appliance para armazenamento de backup com capacidade útil de 400 TiB, garantia, manutenção e suporte técnico de 60 meses, instalação e implantação inclusos	404135	Unidade	2
9	Serviços de Operação Assistida	27332	Horas	160
10	Serviços de Treinamento Teórico/Prático (Turma)	3840	Unidade	2
11	Serviços de Suporte Especializado	27332	Horas	800

GRUPO 1 – SOLUÇÃO DE ARMAZENAMENTO DE DADOS E SERVIÇOS

1. REQUISITOS GERAIS PARA AS SOLUÇÕES DE ARMAZENAMENTO NAS E DE OBJETOS (ITENS 1 a 3)

- 1.1. Todas as capacidades e desempenho foram especificados em seu requisito mínimo, sempre podendo ser entregue capacidade e/ou desempenho superior.
- 1.2. Os valores de capacidade de armazenamento dos equipamentos neste documento estão expressos em *TebiBytes* (TiB), salvo menção em contrário. O *TebiByte* considera a expressão das grandezas relativas à capacidade de armazenamento em base 2, onde $1\text{TiB} = 2^{40} \text{ bytes} = 1.099.511.627.776 \text{ bytes} = 1024 \text{ GibiByte}$.
- 1.3. As soluções devem ser ofertadas na modalidade on-premises.
- 1.4. Os storages deverão ter garantia do fabricante para todos os seus componentes, hardware e software, conforme definido neste Termo de Referência. Todas as licenças de software fornecidas deverão estar atualizadas para a última versão e release liberado e comercializado para uso, incluindo software básico e operacional da solução de armazenamento. Deverão possuir os componentes de hardware e software de um mesmo fabricante, não sendo aceitas soluções com software baseado em regime de OEM.
 - 1.4.1. Na ocasião do fornecedor não ser o próprio fabricante da solução proposta, será aceita a garantia fornecida pela proponente, desde que ela seja oficialmente nominada pelo fabricante como uma assistência técnica autorizada a prestar suporte em seu nome.
 - 1.4.2. Os switches de rede necessários à implementação das soluções podem ser de fornecedores diversos, visto que a padronização deste tipo de rede é bastante solidificada. O fornecedor dos equipamentos de rede deve garantir junto ao fabricante dos switches e dos equipamentos de storage a total compatibilidade de toda a solução. Para tal pode-se comprovar por uma matriz de compatibilidade que certifique os dispositivos de rede de *backend* e/ou *frontend* fornecidos são certificados ou via carta dos fabricantes.
- 1.5. Os hardwares ofertados e seus componentes deverão ser novos, sem utilização anterior e em linha de fabricação na data da entrega.
- 1.6. Não serão aceitos equipamentos usados, de demonstração, que estejam em *end-of-sale*, *end-of-life*, remanufaturados, recondicionados nem qualquer instituto semelhante.
- 1.7. Todas as licenças de software necessárias para atendimento das especificações técnicas devem estar inclusas na solução entregue pelo fornecedor e devem funcionar, mesmo após o período de vigência e de garantia do contrato.
- 1.8. Todas as funcionalidades solicitadas deverão estar licenciadas e disponíveis para uso simultâneo e em toda capacidade contratada.
- 1.9. Deverão ser fornecidas, sem ônus adicional, todas as atualizações, upgrades, correções de software e patches de segurança durante o período de suporte contratual. As soluções de armazenamento deverão permitir a atualização do sistema operacional, seja por correção de erros ou implementação de novas funcionalidades, sem causar a indisponibilidade da solução.
- 1.10. O equipamento deve ser fornecido com *Power Distribution Units* (PDUs) redundantes e independentes para conexão à rede elétrica de tensão de 220V, no padrão das salas cofres deste MJSP, a serem instalados no rack. As PDUs devem possuir tomadas suficientes para energização dos equipamentos.

- 1.11. Cada *appliance*/controladora da solução deverá operar com pelo menos 2 (duas) fontes de energia redundantes e independentes, 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.
- 1.12. As fontes de alimentação deverão ser do tipo *hot swap* e deverão operar com tensão monofásica de entrada de 200VAC a 240VAC, com frequência de entrada de 60 Hz e com tolerância a uma variação mínima de 10%;
- 1.13. Os equipamentos deverão ser instalados na tensão da rede estabilizada disponíveis no Ministério da Justiça e Segurança Pública, de 220 V (bifásico ou trifásico), 60 Hz.
- 1.14. Os conectores “macho” e “fêmea”, necessários à conexão elétrica dos equipamentos aos quadros elétricos do Ministério da Justiça e Segurança Pública, deverão ser fornecidos pela CONTRATADA. Esses conectores deverão ser compatíveis entre si e atender a todos os requisitos técnicos dos equipamentos fornecidos. A adaptação dos plugues, caso necessário, será de responsabilidade da CONTRATADA.
- 1.15. Uma vez que os conectores “macho” e “fêmea” serão fornecidos pela CONTRATADA, o padrão a ser seguido fica a cargo da licitante, desde que dimensionado para a carga elétrica demandada pelo equipamento.
- 1.16. Deverá adaptar ou construir as tomadas elétricas dos equipamentos adquiridos, no momento da instalação, organizadas de forma que a alimentação elétrica seja feita por duas fontes de energia independentes, quando disponibilizadas.
- 1.17. O proponente fica obrigado, mediante solicitação do Ministério da Justiça e Segurança Pública, a certificar todas as condições físicas (elétricas e ambientais) de instalação dos equipamentos, conforme padrões estabelecidos pelo FABRICANTE.
- 1.18. Deverá ser fornecido todo o cabeamento de fibra óptica e UTPs necessários à instalação dos equipamentos, obedecidas as especificações técnicas que podem ser obtidas em visita técnica.
- 1.19. O cabeamento deverá ser fornecido no comprimento adequado para viabilização do projeto. As distâncias estimadas dos cordões ópticos e cabos UTPs variam de 3 a 15 metros. A aferição das metragens dos cabos poderá ser feita mediante vistoria nas unidades de instalação dos equipamentos.
- 1.20. As soluções de armazenamento devem 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, conectores, transceivers, PDU's, tampas frontais de fechamento, chaves e demais componentes necessários para seu perfeito funcionamento. A contratada deverá compor as soluções de *storage* de forma a suportar as métricas de desempenho definidas no TR.
- 1.21. A solução deverá ser instalada em rack próprio do órgão (Rittal – Modelo: TS IT RACK 600x2000x1000 R7035 PRT. Ventilador).
- 1.22. A empresa contratada deve fornecer todos os trilhos e componentes necessários para garantir uma instalação perfeita da solução. Esses trilhos e componentes devem ser compatíveis com o rack que já está presente nas instalações do órgão.

1.23. Gerenciamento e Automação

- 1.23.1. Deve possuir ferramenta para gerenciar e configurar a solução e expansões e todas suas funcionalidades requisitadas.
- 1.23.2. Deve possuir interface gráfica e linha de comando para administração e provisionamento de recursos de armazenamento, integrada com serviços de diretório padrão LDAP e Microsoft Active Directory para autenticação de usuários.
- 1.23.3. As funções de gerenciamento devem ser acessadas através de conexão IP e 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.
- 1.23.4. Deverá permitir a criação de usuários, grupos de usuário e perfis de acesso às interfaces de gerenciamento utilizando base interna e/ou integração com serviços de diretório padrão LDAP e Microsoft Active Directory.
- 1.23.5. Deverá implementar o protocolo NTP para sincronização de data e hora com os servidores NTP da CONTRATANTE.
- 1.23.6. Deverá implementar cliente de DNS para resolução de nomes nos servidores DNS da CONTRATANTE.
- 1.23.7. Deve gerar e permitir visualizar os eventos registrados relacionados à solução de armazenamento. Deverá gerar e permitir visualizar inclusive eventos de autoria dos usuários, a exemplo de registros de acesso e registros de alterações de configurações.
- 1.23.8. Deve permitir que os eventos gerados sejam encaminhados para servidor externo via protocolo *syslog*.
- 1.23.9. Deve prover acesso a dados históricos e de tempo real para avaliação de aspectos de capacidade e desempenho da solução de armazenamento, mantendo histórico de dados de no mínimo 60 (sessenta) dias.
- 1.23.10. Deve permitir a monitoração através de protocolo SNMP com o envio de *traps*.
- 1.23.11. Deve possuir monitoramento pró-ativo que permita a detecção de falhas antes mesmo que elas ocorram. Tal função abrangerá a auto monitoração e geração de log de erros e detecção de erros no disco, inclusive acionamento automático da reposição de discos pelo serviço de garantia.
- 1.23.12. Os produtos ofertados nos itens 1 a 3 deverão suportar todos os protocolos e funcionalidades descritos para cada um deles de forma global como um produto único, não sendo permitido composição de produtos para entrega da solução.
- 1.23.13. 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.
- 1.23.14. O sistema operacional dos módulos/nós dos sistemas de armazenamento *scale-out* deverão ser nativos 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.
- 1.23.15. As soluções não devem ser baseadas em softwares de clusterização de mercado, como Veritas Cluster, Microsoft cluster, Ceph Community, Minio ou similares.

- 1.23.16. As soluções não devem ser baseadas em gateways genéricos, baseados em servidores de rack comuns ou que não sejam de propósito específico.
- 1.23.17. Os equipamentos a serem ofertados pela contratada devem ser aderentes aos padrões de interoperabilidade do governo eletrônico (ePING - <https://eping.governoeletronico.gov.br/>), naquilo que lhes for aplicável.

2. REQUISITOS ESPECÍFICOS PARA AS SOLUÇÕES DE ARMAZENAMENTO DE ALTA PERFORMANCE (NAS) – TIPOS 1 e 2 (ITENS 1 e 2)

- 2.1. As Soluções Armazenamento de Alta Performance de *Storage* de rede (NAS) devem ser baseadas em *appliances* em arquitetura de cluster Scale-Out NAS, compostas por no mínimo 03 (três) módulos/nós/controladoras dispostos em 1 chassi e equipados com discos *all-flash*. As capacidades totais devem ser as seguintes:
- 2.1.1. **Storage (cluster) Tipo 1** – Possuir capacidade de sistema de armazenamento de dados escalável NAS com valor líquido total de, no mínimo, **412 TiB (quatrocentos e doze TebiBytes)**, para armazenamento de dados não-estruturados, fornecidos em discos *all-flash*, sem considerar ganhos com deduplicação, compactação, snapshot, clone e compressão de dados para o armazenamento de documentos digitais com formato não estruturado. Entende-se por capacidade líquida de armazenamento, a capacidade disponível para armazenamento de dados.
- 2.1.2. **Storage (cluster) Tipo 2** – Possuir capacidade de sistema de armazenamento de dados escalável NAS com valor líquido total de, no mínimo, **274 TiB (duzentos e setenta e quatro TebiBytes)**, para armazenamento de dados não-estruturados, fornecidos em discos *all-flash*, sem considerar ganhos com deduplicação, compactação, snapshot, clone e compressão de dados para o armazenamento de documentos digitais com formato não estruturado. Entende-se por capacidade líquida de armazenamento, a capacidade disponível para armazenamento de dados.
- 2.1.3. Entende-se por módulo, nó ou controladora, um conjunto autônomo contendo: CPUs, interfaces de comunicação, memórias, memória não volátil, controladora de discos de modo a permitir crescimento linear da capacidade de processamento, *throughput* e área de armazenamento de dados.
- 2.1.4. Entende-se por capacidade de armazenamento líquida: a capacidade de armazenamento subtraída das áreas utilizadas, entre outras, áreas utilizadas para reservas de *hot- spare*, nível de proteção com paridade, área destinada ao sistema operacional, metadados, áreas pré-alocadas para snapshots ou replicação, formatação e demais overheads (demais áreas dedicadas para o completo funcionamento da solução). É a capacidade disponível, dedicada e exclusiva para o armazenamento de dados de usuários e aplicações.
- 2.2. A capacidade entregue no cluster deverá ser expansível a, no mínimo, 30% da capacidade dimensionada inicialmente, para cada tipo de *storage* NAS (tipo 1 e 2). 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.
- 2.3. O equipamento fornecido deverá pertencer a linha exclusiva de discos all-flash do fabricante, não serão aceitos sistemas de armazenamento de dados híbridos.
- 2.4. Para efeito de definição do presente objeto, *appliances* são caracterizados segundo a convenção da Associação da Indústria de Redes de Armazenamento - SNIA (*Storage Networking Industry Association*).

2.5. Características de Hardware e Software

- 2.5.1. Cada controladora deve ser autônoma, contendo internamente todos os componentes tais como processamento, memória, discos e interfaces de rede. Não serão aceitas soluções que contenham componentes intermediários ou que possuam funções específicas de acesso ou armazenamento no cluster.
 - 2.5.1.1. A capacidade de processamento e de memória de cada controladora deve atender plenamente os requisitos de desempenho definidos nesse Termo de Referência.
 - 2.5.1.2. Cada controladora deverá possuir, no mínimo, 2 (duas) portas ethernet 25GbE SFP28 destinadas exclusivamente à conexão com switch de *frontend* a ser fornecido pela CONTRATANTE.
 - 2.5.1.3. Cada controladora deverá possuir, no mínimo, 2 (duas) portas ethernet 100GbE QSFP28 destinadas exclusivamente ao *backend*. Serão aceitas controladoras com conexão via RDMA e o uso de tecnologias como Infiniband e RoCE, desde que o desempenho não seja inferior ao solicitado.
 - 2.5.1.4. Cada controladora deverá possuir, no mínimo, 1 (uma) porta ethernet 1Gb/s (um gigabit por segundo) UTP dedicada para gerenciamento.
- 2.5.2. Os módulos/nós deverão se agregar em regime *scale-out* ao cluster, expandindo a sua área útil de acordo com a capacidade solicitada.
- 2.5.3. O sistema deve ser expansível para, no mínimo, 24 (vinte e quatro) módulos/nós em cluster.
- 2.5.4. Todos os discos fornecidos deverão ser do tipo SSD NVMe (*Non-Volatile Memory Express*), de tamanhos equivalentes, com as seguintes características:
 - 2.5.4.1. Tecnologia SLC, IBM® FlashCore Modules (FCM) ou enterprise Flash, incluindo eMLC e QLC, ou 3D TLC Nand ou superiores;
 - 2.5.4.2. Não serão aceitos SSDs com interface SATA sob quaisquer condições;
 - 2.5.4.3. Não serão admitidos SSDs do tipo cMLC, TLC planar ou similar.
- 2.5.5. O nível de proteção do cluster deverá ser ajustado para atender aos requisitos de melhores práticas recomendadas pelo fabricante. A área de proteção não deverá ser computada para o cálculo de área líquida ofertada e deverá suportar a falha de uma controladora sem afetar a disponibilidade dos dados armazenados. Para o cálculo da capacidade líquida ofertada deve-se considerar a tolerância à falhas de pelo menos 2 (dois) discos ou 1 (uma) controladora.
- 2.5.6. Deve estar licenciada para permitir posterior ativação e utilização de compressão e/ou deduplicação, entregando ganhos de redução de dados.
- 2.5.7. A área líquida deve estar disponível para aplicações, podendo ser disponibilizada e utilizada em sua totalidade sem prejuízo de desempenho, descontadas todas as reservas necessárias e permitindo que o volume seja disponibilizado para NAS (*Network Attached Storage*), sob os protocolos SMB/CIFS, NFS, S3 e REST API simultaneamente.

- 2.5.8. A solução deve permitir acesso para compartilhamento de arquivos, utilizando, no mínimo, os protocolos: NFSV3, NFSV4, NFSoRDMA, CIFS (SMBV2 e SMBV3) e S3. Estes protocolos devem ser nativos da solução e estar disponíveis para todo o conjunto de interfaces e para toda a capacidade líquida da solução, suportando inclusive a escalabilidade solicitada.
- 2.5.9. A solução deverá possuir uma taxa de operações (throughput) de no mínimo:
- 2.5.9.1. 36GB/s (trinta e seis gigabytes por segundo) com blocos de 512KB para operações de leitura no protocolo NFS3;
- 2.5.9.2. 9GB/s (nove gigabytes por segundo) com blocos de 512KB para operações de escrita no protocolo NFS3;
- 2.5.9.3. Taxas de no mínimo 210.000 OP/s (Operações por segundo) com latência de 10ms, considerando blocos de 512KB e protocolo NFS3.
- 2.5.9.4. As taxas de operações de leitura e escrita solicitadas nos itens anteriores devem ser comprovadas pelos relatórios obtidos através de ferramentas de modelagem/simuladores. Esses relatórios deverão fazer parte da Proposta apresentada pelo Licitante, contendo todo o detalhamento dos parâmetros utilizados, para análise, e eventual auditoria em fase de diligência, pela Equipe Técnica do Ministério da Justiça e Segurança Pública.
- 2.5.10. A indisponibilidade de uma controladora não poderá comprometer mais do 25% da capacidade de *throughput* do sistema de armazenamento.
- 2.5.11. Deverá suportar integração nativa com containers Kubernetes 1.25 ou superior, provendo armazenamento persistente através do protocolo NFS ou CIFS.
- 2.5.12. Possuir plugin de provisionamento dinâmico de volumes (Dynamic Volume Provisioning) para a plataforma de orquestração de contêineres Kubernetes.
- 2.5.13. Suportar no mínimo 20 bilhões de arquivos em um único file system ou namespace global.
- 2.5.14. A solução proposta em seu conjunto final, ainda que utilizando controladoras compatíveis superiores às ofertadas, deverá suportar uma escalabilidade mínima de 30PB (trinta petabytes) em um único cluster/sistema de arquivos/*namespace*.
- 2.5.15. A arquitetura da solução deve implantar, no mínimo, um único *namespace* com todo o volume disponível. Não será permitida a utilização de agregação de *namespaces* para atingir a escalabilidade solicitada.
- 2.5.16. As controladoras deverão operar com pelo menos 2 (duas) fontes de energia redundantes e independentes, 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.
- 2.5.16.1. As fontes de alimentação deverão ser do tipo hot swap e deverão operar com tensão monofásica de entrada de 220 VCA, com frequência de entrada de 60 Hz e com tolerância a uma variação mínima de 10%.

- 2.5.17. As controladoras deverão possuir redundância de fontes de alimentação, ventilação, barramento de interconexão de cluster, switches de rede para *backend* com portas suficientes para a escalabilidade requisitada, além de permitir a substituição de qualquer um destes componentes de maneira não disruptiva.
- 2.5.18. Deverá permitir o upgrade do sistema operacional entre versões de correção e de atualização global do sistema de armazenamento sem parada do global *namespace*.
- 2.5.19. Deverá ser permitida a troca de discos avariados, sem interrupção das operações de I/O das aplicações que estão acessando o subsistema de discos.
- 2.5.20. As atividades de administração do equipamento deverão ser realizadas por interfaces Ethernet. Estas interfaces podem ou não ser compartilhadas com acesso de usuários.
- 2.5.21. A rede interna de comunicação, que proporciona a sincronização do trabalho entre as controladoras do cluster, deverá ser exclusiva, especialmente desenhada e implantada e separada da rede de serviços de compartilhamento de áreas de armazenamento.
- 2.5.22. A solução deverá fornecer um mecanismo de balanceamento de acesso dos clientes em suas interfaces de rede de front-end.
- 2.5.23. Deverão ser fornecidos 02 (dois) *switches* de rede ethernet com portas 100GbE dedicados para interligação das portas de *backend* das controladoras. Deverão ser ofertados switches com número de portas suficientes para compor a solução integralmente, inclusive a fim de suportar uma eventual expansão conforme item 2.2. Caso as controladoras utilizem conexão via RDMA, não há a obrigatoriedade de entrega dos switches ethernet, mas deverá ser garantido pelo fornecedor que a conectividade de *backend* seja redundante e suficiente para suportar a solução e que a arquitetura da solução suporte uma eventual expansão conforme item 2.2, sem perda de desempenho.
- 2.5.24. Os switches deverão ainda possuir fontes de alimentação e ventilação redundantes e estar licenciado para suportar todas as funcionalidades previstas e necessárias para a correta interligação dos *appliances*/controladoras.
- 2.5.25. A rede de comunicação de backend entre os nós deverá ser implantada com velocidade mínima de 100 Gbps (cem gigabits por segundo) por porta, nos módulos/nós. A conectividade e os switches devem estar totalmente incluídos.
- 2.5.26. A rede de comunicação do *frontend* da solução NAS deve ser conectada aos switches ToR da solução de hiperconvergência, que estão sendo adquiridos por meio do processo 08006.000626/2023-72.
- 2.5.27. Esses switches topo de rack da solução de hiperconvergência serão equipados com portas de fibra de 25 Gigabit Ethernet SFP28. Portanto, a empresa contratada deve garantir que os nós do NAS sejam conectados aos switches topo de rack da solução de hiperconvergência com uma velocidade totalmente compatível e um padrão de conexão do tipo LCxLC.

2.6. Funcionalidades Avançadas

- 2.6.1. Os seguintes serviços de diretório deverão ser suportados pelo sistema de arquivos: Active Directory da Microsoft (AD), LDAP, NIS e autenticação local.
- 2.6.2. A solução deverá possibilitar integração com sistemas de antivírus, de forma que qualquer arquivo que seja manipulado pelo usuário seja verificado por um processo de procura e verificação de vírus. Caso a solução não possua essa integração, alternativamente, a solução deve permitir que seja possível instalar o agente de antivírus ou possibilitar que seja utilizado um servidor gateway com sistema operacional compatível para instalação do antivírus e montagem do volumes de arquivos para verificação em massa.
- 2.6.3. A solução deverá suportar monitoramento de utilização de seus componentes com armazenamento de dados históricos, de forma que os dados possam ser analisados e utilizados para provisionamento e upgrades futuros.
- 2.6.4. Deverá realizar gerenciamento de camadas, com movimentação automática de arquivos ou blocos entre diferentes camadas de armazenamento (*tiering*), se disponíveis no cluster, definidas por tipo e velocidade de acesso aos dados dos discos.
- 2.6.5. A solução deverá ter integração nativa e completa com solução de *storage* de objetos e suportar a expansão da sua capacidade para uma camada de armazenamento de objetos (tierização ou transbordo), necessitando suportar o padrão S3 (AWS), no mínimo, bem como suportar a expansão da capacidade para a solução de armazenamento de objetos.
 - 2.6.5.1. Deverá garantir, seja por uso de políticas definidas pelo administrador da solução, ou método equivalente, que dados e arquivos considerados frios, ou seja, sem acesso no decorrer de um período de tempo, sejam armazenados no *storage* de objetos de forma transparente ao usuário e com a finalidade de liberar área útil no *storage* NAS (*tiering* entre storages). Estes dados poderão retornar ao *storage* principal, a partir do momento que se forem acessados, desde que tenha disponibilidade de área; caso contrário deverá permanecer no *storage* de objetos, mesmo com aumento de latência no acesso, ou prover mecanismos que evitem a interrupção da solução de armazenamento NAS;
 - 2.6.5.2. A extensão de armazenamento para o *storage* de objetos deverá ser imperceptível para as aplicações e/ou usuários, onde os arquivos ou blocos, enviados para tal camada, deverão ser substituídos por stubs ou links automaticamente em suas localizações originais.
 - 2.6.5.3. Deverá ser possível criar regras/políticas para a movimentação de arquivos ou blocos para o *storage* de objetos.
- 2.6.6. A movimentação, (tierização) ou extensão de cache (aceleração), descritas nos subitens 2.6.1 e 2.6.2, deverá ocorrer com o uso de recursos internos da solução, sem softwares ou *appliances* externos. A movimentação deve ocorrer periodicamente, entre diferentes camadas de armazenamento existentes no equipamento, de acordo com políticas definidas pelo administrador. Já a extensão de cache (aceleração), deverá ser on-line.

- 2.6.7. Para a tierização, é mandatório que o administrador do sistema possa realizar a configuração das políticas que definirão em que camada de armazenamento o arquivo deve residir.
- 2.6.8. A solução deverá se integrar com serviços de diretório para promover a autenticação. Os seguintes serviços de diretório deverão ser suportados pelo sistema de arquivos: *Active Directory* da Microsoft, Open LDAP, NIS e autenticação local. A solução deve suportar a integração ao serviço *Active Directory* por mecanismo de single sign-on (SSO) que possibilite o acesso aos seus recursos por meio de tokens gerados pela plataforma de gerenciamento de identidade.
- 2.6.9. A solução deverá implementar mecanismo de controle de acesso baseado nas definições de modebits, conforme definido na RFC 1813 (página 22), para o protocolo NFSv3 e baseado em listas de controle de acesso (ACL) para os protocolos SMB e NFSv4. Deverá ser possível realizar o controle de acesso granular para as entidades existentes no serviço *Active Directory* (usuários e grupos), e mapear as permissões de pastas e arquivos de modo semelhante ao existente nos sistemas de arquivos para SOs Windows (NTFS) e Linux (EXT4/BRTFS).
- 2.6.10. A solução deverá suportar nativamente IPv4 e IPv6.
- 2.6.11. A solução deverá suportar monitoramento de utilização de seus componentes com armazenamento de dados históricos, de forma que os dados possam ser analisados e utilizados para provisionamento e upgrades futuros.
- 2.6.12. A solução deverá suportar cotas de armazenamento para usuários. As cotas deverão ser aplicadas em qualquer nível de profundidade da árvore de subdiretórios, aceitando-se atribuição de links dinâmicos ou *junction points* para alcançar qualquer nível de profundidade desejado.
 - 2.6.12.1. As cotas deverão ser implementadas através de políticas pré-definidas pelo administrador, aplicáveis a qualquer usuário ou grupo de usuários configurado no *namespace* global.
 - 2.6.12.2. A implementação de cotas deverá monitorar a utilização de espaço de armazenamento pelos usuários e garantir que eles não ultrapassem os limites configurados, permitindo que a solução tenha a opção de bloquear a escrita e/ou enviar alertas amigáveis para usuários.
 - 2.6.12.3. A política de cotas deverá possuir suporte ao provisionamento dinâmico, ou seja, deverá permitir que o administrador da solução entregue aos usuários uma capacidade de armazenamento maior do que a capacidade efetiva do equipamento.
- 2.6.13. A solução deverá registrar todas as atividades administrativas, eventos, falhas de componente sem um sistema unificado de registro de eventos.
- 2.6.14. A solução deverá implantar auditoria do sistema de arquivos, pelo menos para os protocolos SMB e NFS.
- 2.6.15. A solução deve possibilitar que os dados coletados pelo subsistema de auditoria sejam automaticamente exportados para sistemas centralizados de armazenamento de log de terceiros, através dos protocolos

padrões de mercado para este fim; e enviar as informações de auditoria das atividades administrativas para um servidor *syslog*.

- 2.6.16. A solução deverá suportar a funcionalidade de replicação remota de dados de forma assíncrona, permitindo a implantação de políticas de recuperação rápida em caso de desastre.
- 2.6.17. A solução deverá possibilitar a implantação de snapshots para os dados armazenados suficientes para atender capacidade a ser adquirida e suas eventuais expansões futuras.
 - 2.6.17.1. Deve ser permitida a criação de snapshots por volume ou *file system* (pasta).
 - 2.6.17.2. Deverá ser possível a integração do mecanismo de geração de snapshots com a funcionalidade de “*shadow copies*” do Windows, permitindo obter versões passadas das pastas armazenadas diretamente através do Sistema Operacional.
 - 2.6.17.3. A fim de fornecer pontos de restauração curtos para lidar com situações de ataques de *ransomware*, a solução deverá permitir a retenção de um ponto de restauração por hora por no mínimo 30 dias, para cada volume ou *file system*.
- 2.6.18. A solução deverá suportar os mecanismos de expansão da área útil de armazenamento de forma transparente para o cliente, ou seja, não serão aceitas soluções que exijam qualquer procedimento de reboot ou mesmo soluções que exijam o desmapeamento de unidades lógicas ou *mountpoints* de rede para reconhecimento da nova capacidade.
- 2.6.19. A solução deverá permitir o gerenciamento centralizado, através de interface web, para todos os componentes da solução, todos os componentes necessários para o perfeito funcionamento do gerenciamento devem ser fornecidos.
- 2.6.20. O gerenciamento deve permitir a criação de níveis de acesso de usuários (super usuário, administrador, operador, no mínimo).
- 2.6.21. A solução deverá permitir acesso via SSH para administração remota.
- 2.6.22. A arquitetura da solução deverá ser distribuída e composta por controladoras de armazenamento que atuem de forma paralela, com processamento simétrico, ou que utilize algoritmo que busque balancear a capacidade e o tráfego dos clientes da forma mais equitativa possível. Todas as controladoras que compõem a solução deverão ser ativas e em caso de falha de qualquer controladora, nenhum volume deve ficar indisponível.
- 2.6.23. A solução deverá balancear o armazenamento dos dados de forma automática entre todas as controladoras que compõem o cluster de alto processamento, sem utilização de nenhum componente externo.
 - 2.6.23.1. Em caso de adição de novas controladoras, a solução deve garantir que o balanceamento englobará a nova controladora, permitindo o rebalanceamento das informações armazenadas, de forma que a utilização de seus componentes seja equalizada com as demais. O rebalanceamento poderá acontecer de

maneira automática ou com a anuência do administrador, mas sempre sem que haja interrupção dos serviços de fornecimento de arquivos aos usuários e/ou sistemas.

- 2.6.23.2. A solução deverá fornecer um mecanismo de balanceamento de acesso dos clientes em suas interfaces de rede de *frontend*.
- 2.6.23.3. O mecanismo de balanceamento deverá ser nativo da solução, implantado sem que nenhum componente adicional de hardware e software sejam instalados e deverá ser capaz de identificar qual controladora do cluster encontra-se em melhores condições de prover os serviços de compartilhamento para o cliente. Para tal, deverá permitir integração aos serviços de DNS da contratante.
- 2.6.24. Deverá possuir funcionalidades de compressão e deduplicação *INLINE*, isto é, durante a gravação dos dados para a camada de armazenamento. Caso haja necessidade de licenciamento ou hardware adicional, deverá estar contemplado para toda a capacidade ofertada, sem prejuízo aos demais requisitos.
- 2.6.24.1. Caso a solução fornecida não implemente deduplicação *INLINE*, haverá necessidade de incremento da capacidade útil fornecida em 25% (cinquenta por cento), considerando que grande parte dos dados armazenados serão arquivos de usuário.
- 2.6.25. Deverá possuir recurso nativo que garanta que os dados (arquivos) não sejam alterados ou apagados durante o período pré-definido (imutabilidade), funcionalidade de *WORM (Write Once Read Many)* ou equivalente nativo da solução e do mesmo fabricante, não sendo aceitas soluções externas e de terceiros para o atendimento ao requisito.
- 2.6.25.1. O prazo de retenção da imutabilidade poderá ser atribuído ao volume, permitindo inclusive diferentes períodos de retenção para cada volume.
- 2.6.25.2. Deve ser compatível com a implementação de cofre para armazenamento de dados protegidos em uma área apartada, completamente isolada. Deve copiar todos os dados, metadados e demais para o cofre para garantir a rápida recuperação em caso de ataque no cluster de produção.
- 2.6.26. A solução deverá possibilitar integração com sistemas de antivírus, via protocolo *ICAP*, *CAVA*, *FPOLICY* ou integração própria, de forma que qualquer arquivo que seja manipulado pelo usuário seja verificado por um processo de procura e verificação de vírus. Caso a solução não possua essa integração, alternativamente, a solução deve permitir que seja possível instalar o agente de antivírus ou possibilitar que seja utilizado um servidor gateway com sistema operacional compatível para instalação do antivírus e montagem dos volumes de arquivos para verificação em massa.
- 2.6.27. Deve possuir integração com tecnologia de detecção e resposta automatizada contra ataques cibernéticos do tipo *ransomware*, definidas por política:
- 2.6.27.1. Este recurso deverá estar licenciado para toda a capacidade ofertada de forma perpétua ou modalidade de subscrição por todo período contratado.

- 2.6.27.2. Deve detectar comportamentos anômalos automaticamente, prover respostas automatizadas definidas por política com corte automático da conexão do usuário e interrupção imediata de replicação ou criação automática de ponto de restauração (*snapshot*);
- 2.6.28. A solução deverá possibilitar que compartilhamentos SMB criados possam ser compartilhados por meio de um “*Distributed File Share (DFS)*” disponibilizado por um servidor Windows Server.
- 2.6.29. A solução deverá permitir a implementação de técnicas de backup de filesystem/diretório/arquivos, utilizando-se o protocolo NDMP que deverá ser compatível com topologia 2-Way NDMP e 3-Way NDMP ou APIs proprietárias que permitam a integração nativa com as soluções de backup.
- 2.6.30. Deve realizar snapshots (cópias point-in-time). Deve suportar a criação de cópias independentes a partir dos snapshots, permitindo operações de leitura e escrita nessa cópia, sem que os dados originais sejam afetados.
- 2.6.31. Permitir que a criação de snapshots seja realizada através de agendamentos via interface gráfica, onde seja possível definir data e periodicidade, onde seja possível criar snapshots com intervalo mínimo de 5 minutos entre eles e seja possível configurar a retenção desses snapshots por, ao menos, 90 dias ou indefinidamente.
- 2.6.32. Permitir a criação de, no mínimo, 100 snapshots por filesystem ou subdiretório.
- 2.6.33. O uso simultâneo das funcionalidades especificadas: redução de dados, snapshot, clone, thin-clone e migração entre áreas de armazenamento internas ao storage devem ser possíveis de serem utilizadas sem restrições entre si.
- 2.6.34. Possuir criptografia nativa e habilitada dos dados armazenados nos dispositivos Flash, do tipo “*Data at Rest*”, via hardware ou software e utilizando algoritmo AES-256:
 - 2.6.34.1. Possuir conformidade com o padrão FIPS 140-2 (Federal Information Processing Standard (FIPS) Publication 140), que define requisitos mínimos de segurança para módulos criptográficos em produtos e sistemas.
 - 2.6.34.2. Caso seja necessário o fornecimento de hardware e/ou software para gerenciamento externo das chaves de criptografia em conformidade com o padrão FIPS 140-2, o mesmo deverá ser fornecido respeitando os níveis de redundância exigidos para o storage e as cláusulas de garantia e SLA do edital.
- 2.6.35. A solução deverá contemplar o licenciamento de software para atender todas as funcionalidades descritas no Termo de Referência, assim como as seguintes, de forma não exaustiva:
 - 2.6.35.1. Monitoração;
 - 2.6.35.2. Funcionalidade de gerenciamento e balanceamento de conexões;
 - 2.6.35.3. Gerenciamento e assinalamento de cotas;
 - 2.6.35.4. Gerenciamento de snapshots e/ou clones;

2.6.35.5. Gerenciamento de camadas (*tiering* ou tierização)

2.6.35.6. Funcionalidade de redução de dados;

2.6.35.7. Funcionalidades WORM ou similar, imutabilidade e detecção de anomalias.

2.7. Da Replicação

2.7.1. Deverá permitir a replicação dos objetos entre duas ou mais unidades da solução, de forma automática e assíncrona, no tempo mínimo permitido pela configuração proposta e não superior a 1 (uma) hora, independentemente de sua localização física.

2.7.2. Para atendimento desse item, considerar um link com velocidade mínima de 10 Gbps (dez gigabits por segundo) e com latência máxima de 100 ms (cem milissegundos).

3. REQUISITOS ESPECÍFICOS PARA A SOLUÇÃO DE ARMAZENAMENTO DE OBJETOS (ITEM 3)

- 3.1. A solução de Storage de Objetos (*Object Storage*) deverá ser composta por dois clusters do mesmo fabricante e devem ser baseadas em *appliances* em arquitetura de cluster *scale-out*. Cada cluster será instalado em um dos dois data centers do MJSP (primário, no MJSP; e contingência, no CICCEN) e deverá ser composta de, no mínimo, 04 módulos/nós/controladora dedicados em cada *cluster*.
 - 3.1.1. Entende-se por módulo, nó ou controladora, um conjunto autônomo contendo: CPUs, interfaces de comunicação, memórias, memória não volátil, controladora de discos de modo a permitir crescimento linear da capacidade de processamento, *throughput* e área de armazenamento de dados.
 - 3.1.2. Entende-se por capacidade líquida a capacidade disponível para efetivo armazenamento dos dados, desconsiderando a área adicional relacionada com os mecanismos de redundância e tolerância a falhas gerenciados internamente pelo *appliance*.
- 3.2. Possuir capacidade total líquida de, no mínimo, **420 TiB (quatrocentos e vinte Tebibytes)**. Para o cálculo líquido de armazenamento:
 - 3.2.1. Utilizar arquitetura RAID (*Redundant Array of Independent Disks*), RAIN (*Redundant Array of Independent Nodes*) ou similar, com seus respectivos algoritmos de paridade. Os dados armazenados nos discos devem ser protegidos por no mínimo tecnologia de dupla paridade: RAID6, *Erasure Coding* ou similar/superior;
 - 3.2.2. Subtrair as áreas utilizadas para algoritmos de paridade;
 - 3.2.3. Subtrair as áreas utilizadas para *dynamic-spare*;
 - 3.2.4. Subtrair as áreas utilizadas para *nodes-spare*;
 - 3.2.5. Subtrair as áreas utilizadas para uso interno da Solução;
 - 3.2.6. Subtrair as áreas utilizadas para metadados;
 - 3.2.7. Desconsiderar qualquer tipo de compactação ou compressão de dados;
 - 3.2.8. Desconsiderar qualquer tipo de deduplicação.
- 3.3. A capacidade entregue em cada *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.
- 3.4. Serão aceitas soluções baseadas em par de controladoras em alta disponibilidade e módulos de discos, desde que todas as demais características do conjunto sejam atendidas.
- 3.5. Para efeito de definição do presente objeto, *appliances* são caracterizados segundo a convenção da Associação da Indústria de Redes de Armazenamento - SNIA (*Storage Networking Industry Association*).
- 3.6. Não serão aceitas soluções de hardware commodity com software defined object storage montados especificamente para atender a este item.

3.7. Características de Hardware e Software

- 3.7.1. Os equipamentos de armazenamento de dados do tipo Objeto (*Object Storage*) são *appliances* que executam plataformas de armazenamento definidas por software, capazes de gerenciar e permitir o acesso a quantidades massivas de objetos organizados não de forma hierárquica através de estruturas de pastas, mas por coleções de metadados descritivos.
- 3.7.2. Cada controladora deve ser autônoma, contendo internamente todos os componentes tais como processamento, memória, discos e interfaces de rede. Não serão aceitas soluções que contenham componentes intermediários ou que possuam funções específicas de acesso ou armazenamento no cluster. Serão aceitas soluções que escalem horizontalmente em pares de alta-disponibilidade, com acesso compartilhado a disco, sendo cada controladora do par contabilizada de maneira individualizada. Neste caso, cada controladora do par deverá atender plenamente aos requisitos presentes no Termo de Referência.
 - 3.7.2.1. A capacidade de processamento e de memória de cada controladora deve atender plenamente os requisitos de desempenho definidos nesse Termo de Referência.
 - 3.7.2.2. Cada controladora deverá possuir, no mínimo, 2 (duas) portas ethernet 25GbE SFP28 destinadas exclusivamente ao *frontend*.
 - 3.7.2.3. Cada controladora deverá possuir, no mínimo, 2 (duas) portas ethernet 25GbE SFP28 destinadas exclusivamente ao *backend*. Serão aceitas controladoras com conexão via RDMA e o uso de tecnologias como Infiniband e RoCE, desde que o desempenho não seja inferior ao solicitado.
 - 3.7.2.4. Cada controladora deverá possuir, no mínimo, 1 (uma) porta ethernet 1Gb/s (um gigabit por segundo) UTP dedicada para gerenciamento.
 - 3.7.2.5. Deve conter discos SSDs suficientes para fins de aceleração e recuperação rápida dos metadados e/ou objetos mais acessados.
- 3.7.3. O sistema deve ser expansível para, no mínimo, 24 (vinte e quatro) módulos/nós em cluster.
- 3.7.4. Ser dimensionada para comportar no total, no mínimo, 2.000.000.000 (dois bilhões) de objetos líquidos de 1MB cada. Para o cálculo de capacidade líquida de endereçamento deve-se:
 - 3.7.4.1. Subtrair todos os arquivos/objetos que sejam metadados;
 - 3.7.4.2. Subtrair todos os arquivos/objetos relativos às políticas de armazenamento;
 - 3.7.4.3. Subtrair todos os arquivos/objetos que sejam cópias de um objeto original;
 - 3.7.4.4. Subtrair todos os arquivos/objetos que sejam fragmentos de um objeto original.
 - 3.7.4.5. Suportar escalabilidade para endereçar a capacidade líquida total de, no mínimo, 18.874.368.000 (dezoito bilhões e oitocentos e setenta e quatro milhões e trezentos e sessenta e oito mil) objetos de 1MB cada, após uma possível expansão.
 - 3.7.4.6. Para o cálculo da capacidade líquida de endereçamento, considerar o descrito no item 3.2 e seus subitens.

- 3.7.5. A solução deverá prover mecanismo de proteção dos dados armazenados, seja através de RAID (*Redundant Array of Independent Disks*) ou em nível de arquivos (*Erasure Coding*), permitindo falhas em até dois discos de um agregado ou de até 1 nó do cluster ou controladora sem interrupção do funcionamento, mantendo a capacidade líquida e a performance de armazenamento.
- 3.7.6. 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.
- 3.7.7. Deve suportar o armazenamento de objetos de, no mínimo, 100 GB (cem gigabytes). Em concordância com o padrão Amazon S3, a gravação de objetos maiores que 5GB (cinco gigabytes) deverá ser feita através de *multipart uploads*.
- 3.7.8. A solução ofertada deverá possuir recursos de *multi-tenancy* de forma a permitir a segregação lógica da área de armazenamento.
- 3.7.9. 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.
- 3.7.9.1. A característica de *Global Namespace* deverá ser aplicada ao escopo de abrangência dos dois cluster, considerando a funcionalidade de replicação. Ou seja, os dois clusters deverão ser vistos como um único *namespace*, caso replicados.
- 3.7.10. Deverá possuir capacidade para armazenar dados não estruturados e seus metadados, denominados objetos, conforme descrito abaixo:
 - 3.7.10.1. Dados não estruturados: arquivos em geral, que podem ser de diversos tipos (XML, PDF, TXT, Microsoft Office, OpenOffice, arquivos de sistema operacional Linux, etc.);
 - 3.7.10.2. Metadados: dados internos à solução de armazenamento de objetos que descrevem os objetos armazenados na solução.
 - 3.7.10.2.1. Cada metadado deve conter informações relativas a um único objeto e com essas informações deve ser possível recuperar: o objeto original, data e hora da criação, referências ao conteúdo do objeto de forma a possibilitar a implementação de mecanismo de busca avançada, tamanho e suas políticas de autenticação, retenção, proteção e segurança;
 - 3.7.10.2.2. Cada metadado deverá possuir as mesmas políticas (autenticação, retenção, proteção e segurança) do objeto que descreve.
 - 3.7.10.3. Metadados Customizados: dados que podem ser inseridos pela aplicação para descrever os objetos armazenados na solução de forma a possibilitar a implementação de mecanismo de busca avançada mais refinada.
- 3.7.11. Os módulos deverão possuir redundância de fontes de alimentação, ventilação, barramento de interconexão de cluster, além de permitir a substituição de qualquer um destes componentes de maneira não disruptiva.

- 3.7.12. As fontes de alimentação deverão possuir tensão de entrada de 200VAC a 240VAC em 60Hz, deverão ser acompanhadas do cabo de alimentação compatível com o PDU para cada fonte de alimentação fornecida, e cada fonte deve ter potência mínima dimensionada para suportar a configuração máxima do conjunto entregue.
- 3.7.13. O equipamento deve ser fornecido com *Power Distribution Units* (PDUs) que tenham um número suficiente de portas e potência para atender às necessidades da solução.
- 3.7.14. A solução ofertada deverá vir com equipamentos para prover a comunicação interna entre todos os nós ou controladora que compõem a solução de maneira totalmente redundante, incluindo todos os switches de rede, transceptores, cabos e licenças que forem necessários para a intercomunicação.
- 3.7.15. As redes de *frontend* e *backend* devem ser compostas de equipamentos (switches) redundantes e completamente independentes, não sendo permitido o compartilhamento de switches para as redes de *frontend* e *backend*.
- 3.7.16. A solução deverá ser ofertada com todos os itens necessários, incluindo os switches de *frontend*/ToR.
- 3.7.17. A rede de *frontend* deverá ser interconectada com a infraestrutura SPINE-LEAF já existente no órgão. Os equipamentos existentes são do fabricante Cisco Nexus 9336C-FX2, PART NUMBER N9K-C9336C-FX2 e não possuem *transceivers* sobressalentes. Diante disso, a contratada deverá prever todos os *transceivers* necessários (tanto do lado do *frontend*, quanto do lado dos equipamentos existentes) para a perfeita conexão entre os switches de *frontend* dos storages de objetos e os switches existentes no órgão, devendo manter totalmente a compatibilidade com os equipamentos do órgão.
- 3.7.18. A solução deverá ser instalada em rack próprio do órgão (Rittal – Modelo: TS IT RACK 600x2000x1000 R7035 PRT. Ventilador).
- 3.7.19. A empresa contratada deve fornecer todos os trilhos e componentes necessários para garantir uma instalação perfeita da solução. Esses trilhos e componentes devem ser compatíveis com o rack que já está presente nas instalações do órgão.
- 3.7.20. A solução ofertada deverá ser capaz de prover acesso aos objetos armazenados através de um único namespace para toda a capacidade ofertada.
- 3.7.21. Os nós ou controladoras deverão possuir redundância de fontes de alimentação, ventilação, barramento de interconexão de cluster, bem como tolerar a falha completa de um nó ou controladora.
- 3.7.22. Os switches devem possuir o mínimo de 8 conexões para realizar tráfego “Norte-Sul” ou “*uplink*” para a rede principal do MJSP em portas SFP+ ou SFP28.
- 3.7.23. Deve permitir a agregação de portas Ethernet utilizando LACP IEEE 802.3ad.
- 3.7.24. Cada nó do cluster deve possuir, pelo menos, uma interface de 1Gbps Ethernet adicional dedicada para gerenciamento remoto OOB (*Out-Of-Band*).

- 3.7.25. Cada conexão da solução ofertada deverá possuir, de forma nativa, a capacidade de autodeterminar a velocidade de transmissão dos dados, para o caso de conectar-se a dispositivos que operem em outras velocidades, para auto negociar entre velocidades de 10Gbps (dez gigabits por segundo) ou 25Gbps (vinte e cinco gigabits por segundo), de acordo com o *transceiver* utilizado na interface de rede dos módulos/nós (10Gbps ou 25Gbps).
- 3.7.26. A solução deverá permitir que os dois clusters possam ser reconfigurados como um único cluster geograficamente disperso entre dois datacenters. Este único cluster geograficamente disperso deve fornecer um *namespace* global.
- 3.7.27. Deverão ser fornecidos 02 (dois) switches de rede ethernet, por site, com portas 25GbE dedicados para interligação das controladoras (*frontend*) com portas suficientes para suportar toda solução e as expansões previstas. Cada switch deverá possuir 4 (quatro) interfaces 100/40GbE QSFP28. Para cada switch deverão ser fornecidos 4 (quatro) *transceivers* (GBICS) no padrão 40-Gbase-SR-BIDI ou QSFP-40G-SR, além de 4 (quatro) *transceivers* extras, todos compatíveis com o switch do fabricante CISCO, modelo Nexus 9336C-FX2, PART NUMBER N9K-C9336C-FX2, atualmente instalados nos Data Centers do MJSP. A compatibilidade com o switch do fabricante CISCO e qualquer ônus ou problema decorrente do *transceiver* é responsabilidade da contratada. Todos os cabos e insumos para a correta implantação dos switches deverá ser fornecido pela contratada conforme item 1.20.
- 3.7.28. Deverão ser fornecidos 02 (dois) *switches* de rede ethernet, por site, com portas 25GbE dedicados para interligação das portas de *backend* dos *appliances*. Deverão ser ofertados switches com número de portas suficientes para compor a solução integralmente, inclusive a fim de suportar uma eventual expansão conforme item 3.3.
- 3.7.29. Caso as controladoras utilizem conexão via RDMA, não há a obrigatoriedade de entrega dos switches ethernet, mas deverá ser garantido pelo fornecedor que a conectividade de *backend* seja redundante e suficiente para suportar a solução e que a arquitetura da solução suporte uma eventual expansão conforme item 3.3, sem perda de desempenho.
- 3.7.30. Os switches deverão ainda possuir fontes de alimentação e ventilação redundantes e estar licenciado para suportar todas as funcionalidades previstas e necessárias para a correta interligação dos *appliances*/controladoras e todos os cabos e conectores deverão ser fornecidos pela contratada para o pleno funcionamento e comunicação da solução com a rede do Ministério da Justiça e Segurança Pública.
- 3.7.31. A solução deverá balancear o armazenamento dos dados de forma automática entre todos as controladoras que compõem o cluster de alto processamento, sem utilização de nenhum componente externo.
- 3.7.32. Na adição de novas controladoras, a solução deve garantir que o balanceamento englobará a nova controladora, permitindo o rebalanceamento das informações já armazenadas, de forma que a utilização de seus componentes seja equalizada com as demais. O rebalanceamento poderá acontecer de maneira

automática ou com a anuência do administrador, mas sempre sem que haja interrupção dos serviços de fornecimento de arquivos aos usuários e/ou sistemas.

- 3.7.33. Deverá possuir, de forma nativa, as seguintes capacidades de proteção:
 - 3.7.33.1. Deverá proteger os dados distribuindo em grupos de discos ou *chunks* com no máximo 16 (dezesesseis) discos ou fragmentos, incluindo os discos de paridade;
 - 3.7.33.2. Permitir automaticamente que um objeto original possua múltiplas cópias, de forma que cada cópia seja armazenada em servidores e discos diferentes do objeto original;
 - 3.7.33.3. Recuperar de forma automática um objeto original;
- 3.7.34. Deverá possuir de forma nativa as seguintes capacidades de segurança:
 - 3.7.34.1. 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.
 - 3.7.34.2. 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.
 - 3.7.34.3. 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.
 - 3.7.34.4. Garantir que um objeto não seja acessado por usuário ou aplicação não autorizados.
- 3.7.35. Deverá possuir de forma nativa os seguintes controles de retenção:
 - 3.7.35.1. 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;
 - 3.7.35.2. 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;
 - 3.7.35.3. O prazo de retenção deverá ser atribuído a cada objeto armazenado, ou a uma classe de retenção ao qual o objeto esteja associado.
 - 3.7.35.4. Possuir funcionalidade que permita que os objetos sejam mantidos mesmo após a expiração do seu prazo de retenção;
 - 3.7.35.5. Permitir definição do tempo de retenção de, no mínimo, 25 (vinte e cinco) anos.
- 3.7.36. Deverá possuir uma taxa de operações (*throughput*) de:
 - 3.7.36.1. No mínimo 1000 MB/s (um mil megabytes por segundo) para operações de escrita utilizando objetos com tamanho médio de 1 MB (um megabyte).
 - 3.7.36.2. No mínimo 3000 MB/s (três mil megabytes por segundo) para operações de leitura utilizando objetos com tamanho médio de 1 MB (um megabyte).
 - 3.7.36.3. As taxas de operações de leitura e escrita solicitadas nos itens anteriores devem ser comprovadas pelos relatórios obtidos através de ferramentas de modelagem/simuladores. Esses relatórios do fabricante deverão fazer parte da Proposta apresentada pelo Licitante, contendo todo o detalhamento dos parâmetros utilizados, para análise e eventual auditoria em fase de diligência pela Equipe Técnica do Ministério da Justiça e Segurança Pública.

3.8. Funcionalidades Avançadas

- 3.8.1. A solução deverá permitir a integração com o *Active Directory* para definição de usuários e grupos com permissões administrativas na plataforma.
- 3.8.2. A solução deverá ser passível de federação a provedores externos de identidade (IAM) para controle de acesso por meio dos protocolos SAML ou OAUTH2, em especial para os acessos via protocolo http(s)/S3.
- 3.8.3. A autenticação para acesso aos serviços por http(s) deverá ser feita utilizando no mínimo os protocolos HMAC SHA- 1 e HMAC-SHA256.
- 3.8.4. A solução deverá garantir que um objeto seja único no sistema.
- 3.8.5. A solução deverá implementar protocolos de acesso seguro.
- 3.8.6. A solução deve permitir que se efetue pesquisa de objetos através de índices específicos configuráveis, definindo campos-chave e/ou através da indexação completa dos metadados dos objetos; ou permitir integração com soluções de mercado homologadas pelo fabricante do *storage* que realizem a função de indexação (exemplo: *Elasticsearch*).
- 3.8.7. Permitir que as aplicações clientes executem operações com as seguintes finalidades: leitura, gravação, deleção, configuração de retenção, busca e recuperação de objetos.
- 3.8.8. A solução ofertada deverá fazer uso de discos do tipo SSD para aceleração das buscas e recuperação dos metadados e/ou objetos.
- 3.8.9. Possuir interface com as aplicações através do protocolo S3.
- 3.8.10. Deverá possibilitar a aplicação de listas de controle de acesso (ACL's) permitindo o gerenciamento do acesso a objetos e *buckets* para o protocolo S3.
- 3.8.11. A solução deverá permitir a reutilização do espaço liberado para otimizar os recursos de armazenamento.
- 3.8.12. A solução deve possuir a capacidade de gerenciar cotas de armazenamento definidas por políticas determinadas pelo administrador, aplicáveis no *namespace*. A implementação de quotas deve permitir a monitoração de sua utilização, garantindo que não sejam ultrapassados os limites determinados.
- 3.8.13. Deve possuir funcionalidade de criptografia de dados nativa, possuindo suporte ao algoritmo AES-256 e ao padrão FIPS 140-2.
 - 3.8.13.1. A criptografia poderá ser habilitada para todos os dados armazenados ou por *bucket*;
 - 3.8.13.2. Quando a criptografia estiver habilitada para todos os dados armazenados não deve causar uma queda superior à 10% (dez por cento) do desempenho de *throughput* do cluster.
 - 3.8.13.3. A criptografia deverá ocorrer por meio do uso de discos do tipo *Self-Encrypting Drives* (SEDs) ou equivalente.
 - 3.8.13.4. Serão aceitas outras formas de criptografia dos dados (sem uso de discos SED ou equivalentes), desde que os relatórios de desempenho da solução de objetos ou declaração da fabricante atestem que a solução

de armazenamento de objetos consegue atingir o desempenho solicitado, com a criptografia habilitada para todos os dados armazenados.

- 3.8.14. O acesso aos objetos via protocolo S3, assegurado o uso de todas as funcionalidades solicitadas, deve ser suportado por fabricantes de solução para operação com softwares de backup do mercado que operam com S3.
- 3.8.15. A solução ofertada deverá permitir a atualização do sistema operacional, seja por correção de erros ou implementação de novas funcionalidades, sem causar a indisponibilidade da solução.
- 3.8.16. A solução ofertada deverá possuir os componentes de hardware e software de um mesmo fabricante, não sendo aceitas soluções com software baseado em regime de OEM.
- 3.8.17. A solução deverá ser passível de utilização como destino (target) de backup de longa retenção por meio das suas capacidades de *cloud storage*, sem a necessidade de adaptadores ou softwares adicionais, com compatibilidade por meio da utilização do protocolo S3, considerando as soluções de backup (software de orquestração e *appliance* de curta retenção) licitadas neste grupo.
- 3.8.17.1. Compete ao fornecedor garantir a compatibilidade entre as soluções de backup e o *storage* de objetos descrito neste item, a fim de viabilizar o seu uso como tier de armazenamento do backup primário com deduplicação.
- 3.8.18. A solução deverá ter capacidade nativa para armazenamento de snapshots de clusters *ElasticSearch*, bem como para funcionar como tier cold/freeze de armazenamento de índices do *ElasticSearch* por meio das suas capacidades de *cloud storage*.
- 3.8.19. A solução deve ser capaz de manter várias versões do mesmo objeto dentro de um mesmo *bucket*, de modo a prevenir sobrescritas ou remoções não intencionais, e possibilitar a aplicação de políticas de retenção e arquivamento aos objetos, além de permitir a recuperação de qualquer uma das versões anteriores dos objetos armazenados.
- 3.8.20. A solução deverá ser capaz de realizar a tierização do conteúdo do *storage* NAS *scale-out* definido nas especificações técnicas dos itens 1 e 2.
- 3.8.21. A solução deverá permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, de maneira perpétua, irrestrita e sem necessidade de licenciamentos ou ônus adicionais.
- 3.8.22. O equipamento deve possuir funcionalidade de monitoramento proativo que permita a detecção, o isolamento e o registro de falhas em discos, bem como a reconstrução dos dados sem intervenção humana.
- 3.8.23. A solução deve possuir monitoramento proativo e reativo por meio de uma conexão VPN via Internet, a uma central de assistência técnica do fabricante ou de um representante autorizado, que opere em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. Esse monitoramento deve permitir a abertura automática de chamados de suporte para reposição de componentes defeituosos ou de

componentes que apresentem indícios de falha iminente. Os chamados abertos deverão ser confirmados pelo contratante antes de serem efetivados.

3.9. Da Replicação

- 3.9.1. Deverá permitir a replicação dos objetos entre duas ou mais unidades da solução, de forma automática e assíncrona, no tempo mínimo permitido pela configuração proposta e não superior a 1 (uma) hora, independentemente de sua localização física.
- 3.9.2. Para atendimento desse item, considerar um link com velocidade mínima de 10 Gbps (dez gigabits por segundo) e com latência máxima de 100 ms (cem milissegundos).
- 3.9.3. O método de replicação entre unidades da solução deverá ser Ativo-Ativo.
- 3.9.4. Em caso de parada, programada ou não-programada, da solução principal no sítio primário, a solução localizada no sítio de replicação deverá assumir imediatamente as operações de leitura e estar apta a assumir as operações de gravação em um intervalo máximo de 5 (cinco) minutos.
- 3.9.5. Deverá fazer replicação e recuperação de forma automática de objetos entre soluções geograficamente distantes, sem envolvimento de aplicações e suportar, ao menos, 3.000km (três mil quilômetros) de distância.
- 3.9.6. Deverá permitir a replicação em nível de *bucket*, *namespace* ou granularidade similar.

GRUPO 2 – SOLUÇÃO DE BACKUP DE DADOS E SERVIÇOS

4. SOFTWARE DE ORQUESTRAÇÃO DE BACKUP E REPLICAÇÃO DE DADOS (ITEM 7)

4.1. Características gerais

- 4.1.1. A solução ofertada deverá atender integralmente os requisitos especificados neste Termo Referência devendo ser fornecida com todas as licenças necessárias para entrega funcional da solução e completo funcionamento dos recursos contratados, inclusive os softwares básicos, com suporte para *backup*, *restore* e tecnologia de deduplicação de dados, onde o licenciamento deverá possuir capacidade ilimitada de retenções, cópias dos dados protegidos, replicações para outros ambientes para fins de recuperação de desastres e suportar toda a infraestrutura detalhada. As funcionalidades podem ser providas tanto pelo software quanto pelo *appliance* de backup.
- 4.1.2. A solução ofertada não pode ser do tipo comunidade, software livre, ou possuir componentes e módulos sem suporte oficial do fabricante. Todos os componentes de software descritos deverão ser de um único fabricante.
- 4.1.3. A solução ofertada deverá possuir todos os softwares na versão estável mais atual.
- 4.1.4. As funcionalidades aqui descritas poderão ser fornecidas por meio de um único software ou por softwares que operem de forma integrada, devendo ser fornecido todo o licenciamento integral que preencha todas as funcionalidades, sendo admitido que cada uma das ferramentas possua o seu próprio catálogo.
- 4.1.5. Para facilitar o processo de verificação de pré-requisitos e compatibilidade, o fabricante deverá possuir mecanismo público de geração de lista de checagem que, através da informação do pacote a ser instalado, do sistema operacional alvo da instalação, gere uma lista que contenha:
- 4.1.5.1. Patches do Sistema Operacional e de dispositivos de hardware que necessitem estar instalados;
 - 4.1.5.2. Componentes do produto suportados para instalação ou uso no Sistema Operacional em questão;
 - 4.1.5.3. Requerimentos de Hardware para instalação do produto no Sistema Operacional em questão;
 - 4.1.5.4. Componentes de Hardware compatíveis;
 - 4.1.5.5. Compatibilidade com aplicações, bancos de dados e sistemas de arquivos (*File System*).

4.2. Características de licenciamento da solução

- 4.2.1. Todas as licenças do software de backup deverão ser fornecidas de acordo com um dos seguintes modelos de licenciamento:
- 4.2.1.1. Por capacidade de Frontend;
 - 4.2.1.2. Por socket;
 - 4.2.1.3. Por capacidade armazenada em Appliance.
- 4.2.2. Para estimativa do licenciamento foi previsto o seguinte volume licenciado por modelo de licenciamento:

Modelo de licenciamento		Volume Licenciado
1	Por capacidade de Frontend (em TiB)	152
2	Por socket	64
3	Por capacidade armazenada em Appliance (TiB)	400

- 4.2.3. Conforme Tabela do item 4.2.2, a solução fornecida deve prover licenciamento do software de backup para 152 TiB (Terabytes em base 2) de dados de frontend (volume total de dados protegidos considerando

a somatória de todas as fontes de dados de backup) ou para 64 processadores (socket) ou para 400 TiB de capacidade armazenada em appliance, permitindo utilizar em quantidade ilimitada os agentes e módulos do software de backup, enquanto mantendo-se o limite da quantidade contratada.

- 4.2.3.1. O licenciamento de software no modelo de capacidade frontend (terabytes) deve considerar o volume máximo de dados medidos na origem que devem ser protegidos.
- 4.2.3.2. No modelo de licenciamento por processador (socket) deve ser considerada a quantidade de processadores físicos (socket) dos servidores que devem ser protegidos.
- 4.2.3.3. Deverão ser fornecidas licenças para processadores físicos encontrados na origem para o ambiente virtual, incluindo todas as funcionalidades solicitadas neste Termo de Referência, com suporte para backup, restore e tecnologia de deduplicação de dados, onde o licenciamento deve possuir capacidade ilimitada de retenções, cópias dos dados protegidos, replicações para outros ambientes para fins de recuperação de desastres.
- 4.2.3.4. Dos 64 sockets contratados, 16 poderão ser utilizados para proteção de dados em nuvem, na seguinte proporção: 1 socket = 1 TiB.
- 4.2.3.5. No modelo de licenciamento por capacidade armazenada em appliance, deve ser considerada toda a capacidade útil fornecida para os appliances de backup.
- 4.2.4. Deverá prover licenciamento de software baseado na modalidade caráter perpétuo ou de subscrição, devendo todas as funcionalidades solicitadas neste documento estarem operacionais e disponíveis durante 60 meses, inclusive no que diz respeito ao suporte, atualizações e garantia dos componentes.
- 4.2.5. No caso do licenciamento por subscrição, o funcionamento do software de backup deverá ser mantido após o período de vigência contratual, ainda que sem os serviços de suporte, atualização de versão e correção de bugs.
- 4.2.6. Todas as licenças de software que compõem a solução entregue deverão ser ofertadas na modalidade licença de uso perpétuo ou de subscrição, ou seja, o Ministério da Justiça e Segurança Pública se reserva ao direito de continuar utilizando o software, mesmo após o fim do período de garantia, onde apenas o suporte técnico e direito de atualização poderão ser interrompidos.
- 4.2.7. A solução deve possuir capacidade ilimitada de retenções, cópias dos dados protegidos e replicações para outros ambientes para fins de recuperação de desastres.
- 4.2.8. Não poderão ser cobrados quaisquer valores adicionais para a recuperação dos dados já protegidos – durante e após o término do contrato. O licenciamento deverá estar em nome da CONTRATANTE.
- 4.2.9. A solução utilizada deverá estar habilitada para permitir a instalação de quantos servidores/gateways de dados e de gerência do backup físicos ou virtualizados forem necessários para configuração do ambiente da CONTRATANTE, de acordo com as melhores práticas propostas pelo fabricante, desde que respeitando o volume total licenciado e sem custos adicionais.
- 4.2.10. Independentemente da métrica de licenciamento empregada, entende-se que todas as funcionalidades descritas neste documento estarão habilitadas e disponíveis para uso, de acordo com a necessidade da CONTRATANTE.

4.3. Arquitetura do Software

- 4.3.1. Possuir arquitetura em múltiplas camadas permitindo desempenho e escalabilidade horizontal:
 - 4.3.1.1. Camada de gerência.
 - 4.3.1.2. Camada do serviço de mídia/unidade de disco de retenção dos dados.
 - 4.3.1.3. Camada de clientes/agentes multiplataforma de backups.
- 4.3.2. Deve possuir catálogo ou banco de dados contendo as informações sobre todos os dados e mídias onde os backups foram armazenados, esse banco de dados ou catálogo deve ser próprio e fornecido em conjunto com o produto.
- 4.3.3. Deve possuir mecanismo de verificação e checagem de consistência da base de dados no intuito de garantir a integridade dos dados. Podendo ser provida tanto pelo software quanto pelo *appliance* de backup.
- 4.3.4. Possuir mecanismo de reconstrução do catálogo ou banco de dados centralizado em caso de perda do mesmo, sem a necessidade de recatálogo as imagens de backup.
 - 4.3.4.1. É necessário que a solução possua mecanismos para garantir a alta disponibilidade da solução (backup e restore), mesmo que algum servidor ou componentes da solução fique indisponível. A solução deve possuir réplica do servidor de gerência/catálogo no site secundário e alta disponibilidade dos servidores movimentadores de dados e/ou *appliance* de backup.
- 4.3.5. Deve fazer uso de banco de dados relacional para guardar o catálogo de Jobs, arquivos e mídias dos backups.
- 4.3.6. Deve suportar servidor de gerência e catálogo nas seguintes plataformas: Linux e Windows.
 - 4.3.6.1. Para soluções que utilizam o modelo Scale-Out ou Appliances, poderão ser aceitos sistemas operacionais proprietários baseados em arquitetura Linux, desde que não traga nenhum prejuízo técnico ao MJSP (Atualizações de Sistema Operacional, Correções e Aplicação de "Fixes").
- 4.3.7. Deverá permitir a configuração de servidores de gerência de catálogo em cluster ou réplica, para promover alta disponibilidade dos serviços de gerenciamento, em pelo menos as seguintes plataformas:
 - 4.3.8. Red Hat Enterprise Linux;
 - 4.3.9. Windows.
- 4.3.10. Deve suportar servidores movimentadores de dados nas seguintes plataformas: Linux e Windows.
- 4.3.11. Os servidores movimentadores de dados devem suportar balanceamento de carga para distribuir a carga entre eles de forma automática.
- 4.3.12. Os servidores movimentadores de dados devem suportar configuração de recurso automático de failover, ou seja, permitir a configuração de mais de um servidor movimentador de dados em uma política de proteção, de forma que a indisponibilidade de um servidor seja suprida por outro servidor movimentador de dados disponível de forma automática. Esta funcionalidade deverá ser nativa do produto, e não pode ser construída com o uso de soluções baseadas em softwares de cluster de terceiros.
- 4.3.13. Deve permitir o backup e restore de arquivos abertos, garantindo a integridade do backup.
- 4.3.14. Possuir a capacidade de dividir o fluxo de dados proveniente de um servidor em vários dispositivos de gravação (*multiple streams*).

- 4.3.15. Executar backup de logs transacionais, possibilitando a criação de rotina de backup para que ocorra em intervalos mínimos de 1 (uma) hora para pelo menos bancos de dados Oracle (RMAN), Microsoft SQL, Postgres e MySQL.
- 4.3.16. Suportar os métodos de backup Full e Incremental. No método Incremental, suporte ao modo Incremental Forever, ou seja, as cópias de segurança devem consistir em apenas de um backup Full e todos os demais incrementais até o término do período de retenção. Será facultado a utilização de deduplicação na origem.
- 4.3.17. Permitir a geração de cópias de longa retenção full, tanto no modo ativo - executando uma nova cópia de segurança Full no cliente - quanto no modo sintético - utilizando os backups já salvos anteriormente. Deverá permitir o agendamento para geração automática destas cópias.
- 4.3.18. Possuir a capacidade de reiniciar backups a partir do ponto de falha, após a ocorrência da mesma.
- 4.3.19. Deve possuir mecanismo de atualização de clientes e agentes de backup de forma remota, por intermédio da interface de gerenciamento ou via script, permitindo a instalação de múltiplos clientes de backup simultaneamente.
- 4.3.20. Possuir a capacidade de realizar instalação de atualizações no servidor de backup e clientes.
- 4.3.21. Possuir ambiente de gerenciamento de backup e restore via interface gráfica.
- 4.3.22. Possuir função de agendamento do backup através de calendário.
- 4.3.23. Possuir interface gráfica para gerenciamento, monitoramento e criação de políticas de backup e restore.
- 4.3.24. Possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades de administração e operação do software de backup.
- 4.3.25. Possuir função para definição de prioridades de execução de Jobs de backup ou clientes.
- 4.3.26. Deverá permitir o agendamento de jobs de backup, sem utilização de utilitários de agendamento dos hosts.
- 4.3.27. Deverá permitir a programação de jobs de backup automatizadas em que sejam definidos prazos de retenção das imagens/backups.
- 4.3.28. Possuir a função de Backup sintético que permite a criação de uma única imagem de backup a partir de um backup full e qualquer quantidade de backups incrementais. O restore será efetuado da nova imagem full sintética.
- 4.3.29. Possuir políticas de ciclo de vida nativas, gerenciar camadas de armazenamento e transferir automaticamente os dados de backup entre camadas através do seu ciclo de vida.
- 4.3.30. Permitir a recuperação granular, possibilitando a restauração de arquivos individuais ou conjuntos de dados.
- 4.3.31. Permitir o controle da banda de tráfego ou otimização da rede durante a execução do backup e/ou do restore.
- 4.3.32. Ser capaz de recuperar dados para servidores diferentes do equipamento de origem.
- 4.3.33. Realizar backup e restore de file systems montados em dispositivos Network-Attached Storage (NAS) através do suporte ao protocolo NDMP ou de API que se integre diretamente com o dispositivo NAS. O

- suporte ao NDMP deve estar licenciado para toda a capacidade da solução, de acordo com o licenciamento utilizado pelo fornecedor (frontend terabyte, socket ou volume armazenado em appliance).
- 4.3.34. Possuir Interface única para gerenciamento de todos os servidores independente do S.O que hospeda esse serviço (Windows, Linux) ou ao menos com a separação entre estrutura de backup da Central de Serviços e estrutura de backup das Unidades remotas.
 - 4.3.35. Deverá implementar monitoramento e administração remotos da solução de backup a partir de qualquer servidor ou estação de trabalho.
 - 4.3.36. A Solução de Backup deverá, a partir de uma única interface, gerenciar operações de Backup e Restore de diferentes sistemas operacionais (clientes).
 - 4.3.37. Deverá permitir a verificação da integridade dos dados armazenados através de algoritmos de *checksum* e/ou autocorreção. A funcionalidade poderá ser atendida pelo *appliance*.
 - 4.3.38. Deverá possuir a funcionalidade de backup com duplicação dos dados entre mídias ou *appliances* de deduplicação distintos.
- 4.4. Desduplicação por Software ou Appliance**
- 4.4.1. Deverá suportar deduplicação de blocos na origem (*client-side*), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir do último backup full, podendo ser provida tanto pelo software quanto pelo *appliance* de backup.
 - 4.4.2. Deverá suportar deduplicação de blocos de tamanho fixo ou variável, podendo ser provida tanto pelo software quanto pelo *appliance* de backup.
 - 4.4.3. A solução de backup deverá ser capaz de gerenciar a réplica do backup deduplicado entre *appliances* de deduplicação.
 - 4.4.4. Deverá possuir a capacidade de deduplicação global de dados no nível de segmentos ou blocos de dados repetidos, entre ambientes físicos e virtuais, mesmo em localidades remotas, podendo ser provida tanto pelo software quanto pelo *appliance* de backup.
 - 4.4.5. Permitir o envio de dados deduplicados para a nuvem, caso seja necessário fornecer licenciamento adicional deverá constar na proposta.
 - 4.4.6. Deverá possuir a capacidade de deduplicação de dados no nível de segmentos ou blocos de dados repetidos de ambientes Oracle, podendo ser provida tanto pelo software quanto pelo *appliance* de backup.
 - 4.4.7. Deverá suportar deduplicação de blocos na origem (*client-side*), para ambientes Oracle, podendo ser provida tanto pelo software quanto pelo *appliance* de backup.
 - 4.4.8. Deverá possuir a capacidade de Replicação de Dados entre “pools” ou *Appliances* de deduplicação de maneira otimizada, enviando somente blocos únicos, podendo ser provida tanto pelo software quanto pelo *appliance* de backup.
 - 4.4.9. Deverá possuir a capacidade de realizar balanceamento de carga automático entre servidores ou *appliances* de deduplicação, podendo ser provida tanto pelo software quanto pelo *appliance* de backup.
 - 4.4.10. Deverá possuir a capacidade de criptografar os dados armazenados de forma deduplicada, podendo ser provida tanto pelo software quanto pelo *appliance* de backup.

- 4.4.11. Não serão aceitas soluções de deduplicação global parciais, aplicadas por *jobs*, políticas de backup independentes ou apenas para cenários de replicação de dados via WAN.

4.5. Controle de Acesso

- 4.5.1. Deverá possuir e implementar o fator duplo de autenticação - 2FA para o console de administração gráfica por meio do provedor de identidade baseado em SAML ou cartões inteligentes CAC / PIV ou certificados de usuário. Será aceito também autenticação da console de administração via SSO com token para verificação de usuário, até que o token expire ou MFA.

4.6. Criptografia

- 4.6.1. Deverá permitir escolher se a criptografia será realizada no agente, com o tráfego de dados via rede já criptografado ou no servidor de backup. A funcionalidade pode ser provida tanto pelo software quanto pelo *appliance* de backup.
- 4.6.2. Deverá possuir capacidade nativa de efetuar criptografia dos backups em no mínimo 256 bits nos Clientes de Backup e em dispositivos de mídia que suportem criptografia. A funcionalidade pode ser provida tanto pelo software quanto pelo *appliance* de backup.
- 4.6.3. Deverá implementar criptografia TLS 1.2 ou superior durante o tráfego dos dados (*in-transit*) e no armazenamento (*at-rest*) em todos os backups, restaurações, replicação automática de imagens e deduplicação. A funcionalidade pode ser provida tanto pelo software quanto pelo *appliance* de backup.
- 4.6.4. Deverá implementar criptografia (*in-transit*) para os metadados de catálogo de backup. A funcionalidade pode ser provida tanto pelo software quanto pelo *appliance* de backup.

4.7. Monitoramento

- 4.7.1. Deverá possibilitar enviar notificações, quando configurado, dos eventos por e-mail;

4.8. Virtualização

- 4.8.1. A solução ofertada deverá ser compatível nativamente e deverá oferecer soluções de backup em nível de hypervisor (sem agente) para máquinas virtuais nas seguintes tecnologias de virtualização:
 - 4.8.1.1. vSphere ESXi versões 6.7 ou superiores;
 - 4.8.1.2. Microsoft Hyper-V 2012 ou superiores.
- 4.8.2. Deverá ser compatível com o VADP (*vStorage API for Data Protection*) para realizar operações de Backup e Restore de ambientes VMware.
 - 4.8.2.1. Deverá permitir a criação de políticas de replicação contínua considerando grupos relacionados com a afinidade dos recursos ao serviço a ser protegido (ex.: máquinas virtuais de aplicação e de bancos de dados relacionadas com uma única aplicação ou workload).
- 4.8.3. A solução deve permitir descobrir e adicionar automaticamente as máquinas virtuais VMware em rotinas de backup, com capacidade de realizar filtros avançados com critérios que incluam pelo menos:
 - 4.8.3.1. *Host*;
 - 4.8.3.2. *Cluster*;
 - 4.8.3.3. *Resource Pool*;
 - 4.8.3.4. *VM Tags*;
 - 4.8.3.5. *Datastore*;

- 4.8.3.6. *vApp*.
- 4.8.4. Permitir a recuperação de máquina virtual instantaneamente no ambiente virtualizado VMware, com inicialização rápida a partir de seus arquivos de backup, sem a necessidade de esperar o término do processo de restauração.
- 4.8.5. Permitir adicionar automaticamente as máquinas virtuais descobertas em rotinas de backup predefinidas, baseado no domínio de proteção que estão contidas.
- 4.8.6. Permitir adicionar automaticamente as máquinas virtuais que não foram incluídas em domínios de proteção a um grupo padrão, de forma a evitar que essas máquinas fiquem sem proteção após a sua criação.
- 4.8.7. Permitir redirecionar a restauração de uma da máquina virtual para um *datastore* ou rede alternativos.
- 4.8.8. Permitir a restauração granular a nível de arquivos das máquinas virtuais protegidas, sem a necessidade de se restaurar a máquina virtual inteira.
- 4.8.9. Permitir a restauração no nível de objetos das aplicações que rodem em ambientes virtualizados para um ambiente de *staging* em que possam ser examinados e validados.

4.9. Nuvem

- 4.9.1. Deverá suportar armazenamento em pelo menos um dos cloud storages: Amazon S3, Microsoft Azure e Oracle Cloud Infrastructure (OCI).
- 4.9.2. Especificamente para armazenamento em nuvem, será permitido o uso de virtual appliance (OVA), desde que devidamente licenciado e com suporte a *storage object*.
- 4.9.3. Deverá suportar deduplicação de dados a fim de reduzir o consumo de rede e armazenamento em nuvem, caso seja necessário, o licenciamento deverá ser fornecido com suporte a 100TB de appliance virtual com deduplicação ou licenciamento integral para permitir armazenamento e deduplicação para recebimento de replicação do site principal para algumas das cloud listadas (Amazon S3 ou Microsoft Azure).
- 4.9.4. Deverá possuir a capacidade de gravar informações de catálogo nos backups enviados para os provedores de nuvem, Microsoft Azure ou Amazon S3, diretamente ou via appliance virtual para deduplicação.
- 4.9.5. Deverá permitir a orquestração de sistemas virtuais VMWare de forma automatizada para recuperação de desastres com no mínimo:
 - 4.9.5.1. Prover meios de automatizar e garantir a consistência do backup a nível de aplicação ou máquina virtual, ou seja, ser capaz de automatizar a restauração de uma máquina virtual ou grupo de consistência e executar ações de testes automatizado para aquela determinada aplicação ou grupo de consistência de forma a garantir que o backup está consistente.
- 4.9.6. A solução deverá permitir o transporte de dados de backup em infraestrutura de objetos, como S3.
- 4.9.7. Solução deverá estar licenciada para realizar o transporte dos dados para infraestruturas de objetos em nuvem pública e privada.
 - 4.9.7.1. Não se faz necessária a entrega dessa infraestrutura;
- 4.9.8. Deverá ser compatível com, no mínimo um, dentre os provedores de nuvem pública, tal qual:
 - 4.9.8.1. Microsoft Azure;

- 4.9.8.2. AWS;
- 4.9.8.3. Oracle Cloud Infrastructure (OCI).
- 4.9.9. Deve permitir que seja configurado a execução de scripts customizados no plano de continuidade.
- 4.9.10. Permitir o controle da banda de tráfego de rede ou otimização durante a execução do backup para nuvem.
- 4.9.11. Deverá permitir e estar licenciado o envio de dados desduplicados para a nuvem.
- 4.10. Auditoria**
- 4.10.1. Possuir mecanismo de auditoria, permitindo a emissão de relatórios onde constem, no mínimo, as seguintes informações:
 - 4.10.1.1. Data e hora da operação, Usuário que realizou a operação, Operação realizada (em caso de modificação de configurações, informar qual a configuração anterior e a modificação realizada);
 - 4.10.1.2. Auditoria e controle de acesso devem ser funcionais para operações realizadas via interface gráfica;
 - 4.10.1.3. Deverá prover monitoramento via interface gráfica e em tempo real dos Jobs sendo executados, incluindo visão de nível hierárquico dos Jobs;
 - 4.10.1.4. Deverá suportar operações de backup e restore em paralelo;
 - 4.10.1.5. Ser capaz de enviar traps SNMP (*Simple Network Management Protocol*) com o objetivo de reportar eventos ocorridos na operação da solução.
- 4.11. Suporte a Plataformas/Sistemas de Arquivos**
- 4.11.1. Deverá suportar o backup e o restore de diferentes sistemas operacionais tais como:
 - 4.11.1.1. Microsoft Windows Server 2012 ou superiores;
 - 4.11.1.2. Microsoft Windows 10 ou superiores;
 - 4.11.1.3. CentOS Linux 7 ou superiores;
 - 4.11.1.4. Debian Linux 10.13 ou superiores;
 - 4.11.1.5. Red Hat Enterprise Linux 7 ou superiores;
 - 4.11.1.6. Oracle Linux 7 ou superiores;
 - 4.11.1.7. SUSE Linux Enterprise Server 15 ou superiores;
 - 4.11.1.8. Ubuntu 16.04 LTS ou versões LTS superiores;
 - 4.11.1.9. VMware ESX/ESXi 6.5 ou superiores;
- 4.11.2. Microsoft Active Directory, com recurso de cópia online.
- 4.11.3. Possibilitar as seguintes opções de recuperação:
 - 4.11.3.1. Recuperação de um objeto;
 - 4.11.3.2. Recuperação de um atributo deletado de um objeto.
- 4.11.4. Suportar a recuperação granular dos dados dos seguintes sistemas de arquivos do tipo: Btrfs, ext3, ext4, XFS, NTFS e ReFS.
- 4.11.5. Permitir os backups e restore do "system state" do Windows de forma nativa e sem a utilização de software de terceiros.
- 4.12. Suporte a Bancos de Dados**
- 4.12.1. Deverá suportar no mínimo os seguintes bancos de dados, utilizando agente específico:
 - 4.12.1.1. Oracle/Oracle RAC versões 11g, 12c, 18c, 19c e 21c.

- 4.12.1.2. MySQL 8 ou superiores;
- 4.12.1.3. PostgreSQL 11, 12 e 13 ou superiores;
- 4.12.1.4. Microsoft SQL Server 2014 ou superiores (incluindo cluster Always-on);
- 4.12.1.5. Microsoft Exchange 2013 ou superiores;
- 4.12.1.6. Microsoft Active Directory.
- 4.12.2. Para os bancos listados abaixo deve possuir as seguintes características:
 - 4.12.2.1. Oracle
 - 4.12.2.1.1. Deverá suportar backup de logs transacionais;
 - 4.12.2.1.2. Deverá suportar backup do Oracle Database, também na arquitetura Oracle RAC, através da integração com RMAN;
 - 4.12.2.1.3. Deverá manter a sincronia entre os catálogos de backups do Oracle RMAN e da solução ofertada.
 - 4.12.2.2. Suporte a MySQL
 - 4.12.2.2.1. Deverá suportar backup de logs transacionais;
 - 4.12.2.2.2. Executar proteção e recuperação de base de dados MySQL Server com as seguintes características nativas ou não:
 - 4.12.2.2.3. Cópia online do banco de dados;
 - 4.12.2.2.4. Permitir a recuperação completa;
 - 4.12.2.2.5. Restaurar a base de dados ou seus arquivos no mesmo servidor em caminho diferente;
 - 4.12.2.2.6. Restaurar uma instância ou seus arquivos em um outro servidor.
 - 4.12.2.3. Suporte a SQL Server:
 - 4.12.2.3.1. Deverá suportar backup de logs transacionais;
 - 4.12.2.3.2. Executar backup de bases de dados do SQL Server de forma “online”, ou seja, sem a parada do banco;
 - 4.12.2.4. Suporte a PostgreSQL
 - 4.12.2.4.1. Deverá suportar backup de logs transacionais;
 - 4.12.2.4.2. Executar proteção e recuperação de base de dados PostgreSQL Server com as seguintes características nativas:
 - 4.12.2.4.3. Cópia online do banco de dados;
 - 4.12.2.4.4. Permitir a recuperação completa;
 - 4.12.2.4.5. Restaurar a base de dados ou seus arquivos no mesmo servidor em caminho diferente;
 - 4.12.2.4.6. Restaurar uma instância ou seus arquivos em um outro servidor.
 - 4.12.2.5. Suporte a SQL Server:
 - 4.12.2.5.1. Deverá suportar backup de logs transacionais;
 - 4.12.2.5.2. Executar backup de bases de dados do SQL Server de forma “online”, ou seja, sem a parada do banco;
 - 4.12.2.5.3. Permitir a montagem de uma base de dados SQL Server a partir dos arquivos de backup, sem necessidade de restauração completa da base para produção, permitindo executar procedimentos e visualizar dados através do SQL Server Management Studio;
 - 4.12.2.5.4. Permitir recuperação granular de objetos ou bases de dados do SQL Server para o local original, ou para um servidor alternativo.

4.12.2.6. Suporte a Microsoft Exchange:

- 4.12.2.6.1. Suportar backups originados de infraestrutura de servidores Exchange organizados por meio de arquitetura DAG (*Database Availability Group*).
- 4.12.2.6.2. Permitir a montagem e restauração granular de backups do Microsoft Exchange a nível de caixas e pastas. Caso a solução necessite de licenciamento para o fornecimento deste recurso, deve estar incluso no fornecimento da solução.

4.13. Relatórios e Gerenciamento

- 4.13.1. A solução deverá permitir a visualização em sua console gráfica ou geração de relatórios de backup, os quais permitam obter minimamente as seguintes informações:
 - 4.13.1.1. Horário de início e término de uma rotina de backup;
 - 4.13.1.2. Tempo de duração de uma rotina de backup;
 - 4.13.1.3. Status das cópias de segurança (situação);
 - 4.13.1.4. Relação dos objetos incluídos na rotina de backup;
 - 4.13.1.5. Horário de início e término das cópias de segurança de cada objeto;
 - 4.13.1.6. Tempo de duração das cópias de segurança de cada objeto;
 - 4.13.1.7. Volume de dados na origem durante a rotina de backup;
 - 4.13.1.8. Volume de dados com compressão e deduplicação;
 - 4.13.1.9. Taxa de deduplicação e de compressão de dados;
 - 4.13.1.10. Relatórios sobre o consumo de licenças.
- 4.13.2. Suportar a geração de relatórios de máquinas virtuais protegidas, contendo:
 - 4.13.2.1. Quantidade total de máquinas virtuais na infraestrutura virtual;
 - 4.13.2.2. Relação das máquinas virtuais, com quebra entre as que possuem backup e aquelas que não possuem backup;
 - 4.13.2.3. Quantidade de versões de backup armazenadas nas cópias de segurança de cada máquina virtual protegida;
 - 4.13.2.4. Data da última execução da rotina de backup com sucesso;
 - 4.13.2.5. Repositório no qual a cópia de segurança do objeto está armazenada.
- 4.13.3. Possuir relatórios e alertas padrões e customizáveis, contendo minimamente as seguintes características:
 - 4.13.3.1. Permitir a segregação de acesso de acordo com o perfil do usuário, para monitorar a infraestrutura conectada;
 - 4.13.3.2. Permitir o envio automático e programado de relatórios por e-mail;
 - 4.13.3.3. Permitir exportar os relatórios gerados em um dos formatos: Microsoft Excel, CSV ou PDF;
 - 4.13.3.4. Suportar a geração de relatórios de charge-back para o ambiente de backup ou prover informações, gráficos e relatórios que subsidiem os referidos relatórios.
 - 4.13.3.5. Suportar a geração e envio de alarmes automaticamente relacionados à infraestrutura virtual e da solução de proteção.
- 4.13.4. Deverá ser possível reter os dados operacionais da plataforma de gerenciamento por período mínimo de 12 meses.

5. REQUISITOS PARA OS APPLIANCES DE BACKUP (ITEM 8)

5.1. Características Gerais

- 5.1.1. Sistema de armazenamento de backup em disco baseado em *appliance*, equipamento desenvolvido com o propósito específico para armazenamento de backup com compactação, deduplicação e replicação.
- 5.1.2. O *appliance* deverá ser composto de conjunto integrado de hardware e software com a finalidade específica de armazenamento de backup em disco, devendo ser um produto desenvolvido e mantido pelo fabricante do software de orquestração de backup ou, caso seja de um fabricante diferente, ser um produto completamente integrado ao software de orquestração e relacionado em sua matriz de compatibilidade.
- 5.1.3. Não serão aceitas soluções definidas por Software (Virtual *Appliance*).
- 5.1.4. Caso haja necessidade de licenciamento para uso do *appliance*, este deverá estar licenciado para toda a sua capacidade de armazenamento líquida.
- 5.1.5. O *appliance* deverá ser novo, de primeiro uso e estar em linha de fabricação na data da abertura da licitação. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração.
- 5.1.6. Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, irrestrita e sem necessidade de licenciamentos ou ônus adicionais.
- 5.1.7. Deve ser composto, de processamento, portas de conectividade e armazenamento integrado, dedicado única e exclusivamente, à execução das atividades ingestão, deduplicação e replicação dos dados.

5.2. Características de Hardware

- 5.2.1. Cada *appliance* deverá ter a capacidade mínima total de armazenamento, conforme especificado a seguir:
 - 5.2.1.1. **Appliance para armazenamento de backup (item 8):** capacidade útil de **400 TiB (TebiBytes)** de dados líquidos em RAID-6, Erasure Coding ou similar, sem considerar ganhos com deduplicação e compressão de dados.
- 5.2.2. Os valores de capacidade de armazenamento dos equipamentos neste documento estão expressos em TebiBytes (TiB), salvo menção em contrário. O TebiByte considera a expressão das grandezas relativas à capacidade de armazenamento em base 2, onde $1\text{TiB} = 2^{40} \text{ bytes} = 1.099.511.627.776 \text{ bytes} = 1024 \text{ GibiByte}$.
- 5.2.3. O *appliance* deverá realizar a deduplicação dos dados de forma inline ou de forma pós-processada a partir de uma área de armazenamento em stage (*staging área*). A área de *staging* de armazenamento não deve ser computada para o armazenamento líquido do *appliance* e deverá ser fornecida em acréscimo ao volume líquido solicitado para o equipamento.
 - 5.2.3.1. Caso a solução fornecida não possua recurso de deduplicação de dados inline, deverá ser fornecida capacidade extra de armazenamento de 25% da capacidade líquida prevista, totalizando 500 TiB (Tebibytes).
- 5.2.4. Capacidade de realizar a ingestão de pelo menos **26 Terabytes/hora**, considerando deduplicação no destino e **54 Terabytes/hora**, considerando deduplicação na origem (cliente-side), a ser comprovada por meio de documento público que comprove essa capacidade.
- 5.2.5. A solução deve permitir escalabilidade à no mínimo 50% extra da capacidade líquida prevista.

- 5.2.6. Possuir pelo menos 04 (quatro) portas SFP28 de 25 Gbps para a realização de backups e replicações de dados, além de uma porta de gerência padrão 1000BaseT de 1Gbps. Se, para atingir o desempenho requerido no projeto, as melhores práticas do fabricante indicar pelo fornecimento de mais portas, essas devem ser adicionadas.
- 5.2.7. A rede de comunicação do *frontend* da solução de backup deve ser conectada aos switches topo de rack (ToR) da solução de hiperconvergência, que serão adquiridos por meio do processo 08006.000626/2023-72. Serão fornecidas no máximo 04 (quatro) portas SFP28 de 25 Gbps para cada appliance no switch ToR retromencionado.
 - 5.2.7.1. Soluções que demandem de mais de 4 portas SFP+/SFP28 25 Gbps por site no total, deverão obrigatoriamente fornecer switches ToR para sua conectividade com redundância, ou seja, no mínimo 2 (dois) equipamentos por site.
- 5.2.8. Esses switches topo de rack da solução de hiperconvergência serão equipados com portas de fibra de 25 Gigabit Ethernet SFP28. Portanto, a empresa contratada deve garantir que os nós do appliance de backup sejam conectados aos switches topo de rack da solução de hiperconvergência com uma velocidade totalmente compatível e um padrão de conexão do tipo LCxLC.
- 5.2.9. Deve obrigatoriamente fazer uso de sistemas de armazenamento de backup em disco, baseado em “*Appliance*”, que se entende como um subsistema com o propósito específico de console de gerenciamento central com base de dados de catálogo independentes, movimentadores de dados de backup, também conhecidos como gerenciadores de mídia, ingestão dos dados de backup com deduplicação e replicação. Caso a solução faça uso de servidores para movimentação de dados, catálogo, este deverá ser entregue junto com a solução completa de backup.
- 5.2.10. O “*Appliance*” deve ser composto, de processamento e armazenamento integrado, dedicado única e exclusivamente, à execução das atividades de console de gerenciamento, gerenciadores de mídia, ingestão, deduplicação e replicação dos dados. Caso a solução faça uso de servidores para movimentação de dados, catálogo, este deverá ser entregue junto com a solução completa de backup.
- 5.2.11. O hardware do “*Appliance*” não poderá ser compartilhado com nenhum outro software.
- 5.2.12. Deve ser novo, sem uso, e constar no site do fabricante como um *appliance* de backup em disco em linha de produção atual.
- 5.2.13. Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, irrestrita e sem necessidade de licenciamentos ou ônus adicionais.
- 5.2.14. Deve ser composto, de processamento, portas de conectividade e armazenamento integrado, dedicado única e exclusivamente, à execução das atividades ingestão, deduplicação e replicação dos dados.
- 5.2.15. Ser homologada pelo software de proteção ofertado.
- 5.2.16. Constar no site do fabricante (documento oficial e público) como um sistema de armazenamento de backup em disco, em linha de produção.
- 5.2.17. O hardware do módulo de armazenamento de cópias em disco não poderá ser compartilhado com nenhum outro software para operar.

- 5.2.18. Estar licenciada para toda sua capacidade e funcionalidade, incluindo replicação.
- 5.2.19. Deverá suportar a gerência em porta específica por meio do protocolo IPMI.
- 5.2.20. A solução deverá ser instalada em rack próprio do órgão padrão 19" (Rittal – Modelo: TS IT RACK 600x2000x1000 R7035 PRT. Ventilador).
- 5.2.21. A empresa contratada deve fornecer todos os trilhos e componentes necessários para garantir uma instalação perfeita da solução. Esses trilhos e componentes devem ser compatíveis com o rack que já está presente nas instalações do órgão. Os equipamentos devem ser fornecidos com tampas frontais e chaves de abertura/fechamento da solução.
- 5.2.22. Deverá utilizar alimentação elétrica de 220V, monofásica, devendo possuir fontes internas ao equipamento, redundantes e *hot-swappable*.
- 5.2.23. O equipamento deve ser fornecido com *Power Distribution Units* (PDUs) que tenham um número suficiente de portas e potência para atender às necessidades da solução.
- 5.2.24. Deverá possuir no próprio hardware do equipamento função de "*call-home*" ou e-mail para seus componentes de hardware e software, tais como: CPU, disco, fonte, ventiladores, temperatura, capacidade de utilização, firmware, entre outros para notificar de forma automática quaisquer problemas para a central do fabricante.
- 5.2.25. Os componentes de FAN e *power supply* devem ser redundantes.
- 5.2.26. Os equipamentos deverão ser instalados na tensão da rede estabilizada disponíveis no Ministério da Justiça e Segurança Pública, de 220 V (bifásico ou trifásico), 60 Hz.
- 5.2.26.1. Os conectores "macho" e "fêmea", necessários à conexão elétrica dos equipamentos aos quadros elétricos do Ministério da Justiça e Segurança Pública, deverão ser fornecidos pela CONTRATADA. Esses conectores deverão ser compatíveis entre si e atender a todos os requisitos técnicos dos equipamentos fornecidos. A adaptação dos plugues, caso necessário, será de responsabilidade da CONTRATADA.
- 5.2.26.2. Uma vez que os conectores "macho" e "fêmea" serão fornecidos pela CONTRATADA, o padrão a ser seguido fica a cargo da licitante, desde que dimensionado para a carga elétrica demandada pelo equipamento.
- 5.2.26.3. Deverão ser fornecidos todos os cabos e conexões necessários ao funcionamento do *appliance*, bem como seus conectores elétricos macho e fêmea para conexão à rede elétrica da CONTRATANTE.
- 5.2.26.4. Deverão permitir a substituição dos componentes redundantes sem interrupção do serviço (*hot swapping*).
- 5.2.27. Possuir suporte a mecanismo de segurança, através de RAID (*Redundant Array of Independent Disks*) ou tecnologia similar como *Erasure Coding*, de forma a suportar a falha simultânea de no mínimo dois discos, sem interrupção dos serviços de ingestão, restauração e replicação de dados.
- 5.2.28. Para soluções em RAID, deve possuir discos de *Hot Spare* para o *appliance* e gavetas de expansão de disco da solução, sem necessidade de intervenção prévia manual.
- 5.2.29. Para *Appliances* baseados em Controladora + Gavetas de Disco, os mesmos devem ser oferecidos com pelo menos 2 Controladoras (*High Availability*).

- 5.2.30. A replicação de dados de backup entre *appliances* deverá ocorrer de forma otimizada, seja através do uso de um otimizador WAN embutido, ou transmitindo somente os blocos modificados com deduplicação visando economia de largura de banda do link.
- 5.2.31. Deverá suportar replicação dos dados em disco para outro *appliance*. A replicação deverá ser assíncrona e ocorrer em horário pré-determinado.
- 5.2.32. Deverá ser fornecido licenciamento para replicação dos dados armazenados no dispositivo de armazenamento para outro dispositivo de mesma categoria e nuvem em formato deduplicado.
- 5.2.33. A solução deve possuir no próprio hardware do equipamento função de “*call-home*” ou email para notificar de forma automática quaisquer problemas para a central do fabricante.
- 5.2.34. Possuir todos os acessórios necessários para a plena configuração, operacionalização, utilização e gerenciamento do equipamento.

5.3. Características de Software e de Interface de Gerenciamento

- 5.3.1. O Sistema Operacional do equipamento deverá ser licenciado. Não serão aceitas soluções que usem sistemas operacionais não corporativos, que não possuem suporte do fabricante.
- 5.3.2. Não serão aceitas soluções definidas por Software (Virtual Appliance).
- 5.3.3. Permitir replicar os dados através de rede IP (WAN/LAN).
- 5.3.4. Suportar os protocolos IPv4 e IPv6.
- 5.3.5. Deverá ter suporte ao protocolo de monitoramento SNMP v2 ou superior, ou possuir API's abertas que possibilitam o monitoramento.
- 5.3.6. Deverá possuir interface de administração gráfica GUI.
- 5.3.7. A interface GUI deverá permitir a visualização de status todos os componentes de hardware, bem como de todos os alertas gerados pelo sistema.
- 5.3.8. Prover “software” para total gerenciamento, administração e configuração do sistema de forma local ou remota, que permitam também a análise de desempenho e implementação das políticas de segurança física, lógica, e de acesso de usuários.
- 5.3.9. Os *softwares*, *drives* e *firmwares* necessários devem estar em suas últimas versões.

5.4. Características de Deduplicação

- 5.4.1. Possuir tecnologia de deduplicação de dados, ou seja, não armazenar mais de uma vez dados que sejam duplicados.
- 5.4.2. A deduplicação deve segmentar automaticamente os dados em blocos de tamanho fixo ou variável.
- 5.4.3. A deduplicação deve ser global, ou seja, identificar dados duplicados tanto do mesmo servidor-cliente de origem do backup como outros servidores-cliente armazenados no mesmo dispositivo de backup, armazenando na solução somente blocos de dados únicos.
- 5.4.4. Permitir o envio de dados deduplicados para a nuvem ou replicação para o Appliance virtual. Caso seja necessário fornecer licenciamento adicional deverá constar na proposta.
- 5.4.5. Permitir suporte à replicação dos dados no formato deduplicado, com controle do catálogo do aplicativo de backup.

- 5.4.6. A deduplicação deverá acontecer ao nível de bytes ou de blocos de dados de tamanho fixo ou variável, de forma a atingir melhores taxas de deduplicação com menor consumo de espaço em disco.

5.5. Características de Segurança

- 5.5.1. Deve possuir recursos de com as seguintes características:
 - 5.5.1.1. Imutabilidade dos dados armazenados;
 - 5.5.1.2. Duplo Fator de Autorização;
 - 5.5.1.3. Air-gap.
- 5.5.2. Deve possuir integração com o Microsoft Active Directory, para autenticação e definição de perfis de acesso.
- 5.5.3. Deverá suportar armazenamento seguro imutável, WORM (Write Once Read Many) ou similar, para evitar que os dados sejam criptografados, modificados ou excluídos. Todos os dados salvos nessas instâncias deverão estar protegidos, segundo o padrão SEC 17a-4, garantindo que os atributos de imutabilidade não possam ser modificados por nenhum usuário com qualquer tipo de credencial.
- 5.5.4. Deve possuir criptografia dos dados armazenados em padrão FIPS 140-2, utilizando no mínimo os algoritmos 256-bits AES.
- 5.5.5. Caso a solução proposta não suporte a replicação dos dados criptografados, deverão ser fornecidos adicionalmente a solução proposta, um *appliance* baseado em hardware que possibilite a implementação de TUNNELING entre os dados de origem e destino, garantindo a segurança dos dados.
- 5.5.6. Deverá possuir suporte a TLS, SSH e Kerberos.
- 5.5.7. Deverá implementar criptografia segura TLS 1.2 ou superior, durante o tráfego dos dados (in-transit) e no armazenamento (at-rest) em todos os backups, restaurações, replicação automática de imagens e deduplicação.
- 5.5.8. Deverá permitir a implementação da função de segurança RBAC.
- 5.5.9. Deverá implementar a conformidade ao Guias Técnicos de Implementação de Segurança (STIGs) que fornecem orientações técnicas para aumentar a segurança dos sistemas e software para ajudar a prevenir ataques malicioso com no mínimo os seguintes requisitos:
- 5.5.10. Deverá implementar conformidade de senhas seguras, não permitindo utilização de senhas fáceis ou sequenciais.
- 5.5.11. Deverá reduzir os privilégios da conta do usuário root.
- 5.5.12. Deverá desativar a opção de reinicializar Ctrl-Alt-Delete.
- 5.5.13. Deverá desabilitar o login root para SSH.
- 5.5.14. As rotinas internas de manutenção dos dados de backup armazenados tais como: Processo de limpeza (*Garbage Collector ou housekeeping*) e validação de integridade (*data integrity*), devem ser executados em paralelo com as rotinas de backup e recuperação, ou seja, a solução ofertada não deve exigir parada ou interrupção (*blackout window*) das atividades de backup/restore para tarefas internas do equipamento.
- 5.5.15. O appliance deverá implementar mecanismos de validação da consistência dos dados deduplicados armazenados, garantindo que eles estejam íntegros durante backups, restaurações e replicações. A

tecnologia deverá reparar, automaticamente, dados que não estejam consistentes com as rotinas executadas;

- 5.5.16. Deverá permitir a implementação de topologias de replicação, como 1 para 1, 1 para N. A solução deverá permitir a criação de topologias de nuvem privada e híbrida.

GRUPOS 1 E 2

6. GARANTIA, MANUTENÇÃO E SUPORTE TÉCNICO (ITENS 1 a 3, 7 e 8)

- 6.1. A CONTRATADA deve fornecer garantia do fabricante com assistência técnica 24x7 e vigência de 60 (sessenta) meses, a partir da assinatura contratual.
- 6.1.1. A vigência do Contrato não exonera a CONTRATADA do período de garantia mínima exigida ou ofertada na proposta, a qual consiste na prestação, pela CONTRATADA, de todas as obrigações previstas na Lei nº 8.078, de 11/09/90, e alterações - Código de Defesa do Consumidor.
- 6.1.2. Devem ser fornecidas garantias técnicas do fabricante para todos os hardwares e softwares necessários ao funcionamento de cada solução pelo período de 60 (sessenta) meses.
- 6.2. Os serviços de suporte técnico aos produtos fornecidos deverão contemplar as atividades de assistência técnica e suporte on-site para atendimento em casos de problemas na Solução, esclarecimentos de dúvidas técnicas (por telefone e e-mail), atualização de firmware e software, sem limites de chamados técnicos em qualquer modalidade.
- 6.3. Durante o prazo de garantia, deverá ser prestado serviço de assistência técnica presencial por meio de manutenção corretiva e preventiva com fornecimento de peças novas e originais, fornecidas pelo fabricante, a serem repostas no local onde ele encontra-se instalado, sem ônus adicional para o Ministério da Justiça e Segurança Pública, respeitando o Acordo de Nível de Serviço estabelecido.
- 6.4. A CONTRATADA deverá contratar garantia do fabricante e descrever em sua proposta os termos da garantia técnica oferecida, incluindo o *part number* da garantia ofertada, e a deverá apresentar comprovante inequívoco da contratação da garantia do fabricante para os equipamentos fornecidos, como requisito para o recebimento definitivo.
- 6.4.1. A garantia é contada a partir do recebimento definitivo da respectiva solução de armazenamento, pela equipe técnica da STI/SE/MJSP.
- 6.5. Os serviços de reparo dos equipamentos serão executados somente e exclusivamente onde se encontram (on-site).
- 6.6. A CONTRATANTE poderá abrir o equipamento sem prévia autorização para efetuar instalação de módulo de memória, discos e outros periféricos sem prejuízo da garantia, desde que seguindo as boas práticas do fabricante do equipamento.
- 6.7. A garantia do fabricante deve possuir, no mínimo, as seguintes características, durante todo seu período de vigência:
 - 6.7.1. Reposição de peça/equipamento defeituoso; o substituto deverá ser novo, de primeiro uso e de modelo igual ou superior ao danificado, e deverá ser enviado pelo fabricante, às expensas da CONTRATADA, para o endereço registrado do CONTRATANTE, passando à propriedade desta e imediatamente sendo incluído no contrato de manutenção vigente em substituição ao equipamento ou peça danificados. Adicionalmente, o equipamento ou peça substituído deverá ser enviado ao fabricante à expensa da CONTRATADA, em até 5 (cinco) dias úteis; ou retirados pela CONTRATADA;
 - 6.7.2. Garantia da atualização do sistema operacional/firmware, provendo o fornecimento de novas versões por necessidade de correção de problemas ou por implementação de novas funcionalidades;

- 6.7.3. Acesso ao serviço de assistência técnica 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; os chamados deverão ser atendidos por engenheiros certificados e especializados do quadro de funcionários do fornecedor credenciado ou fabricante, em inglês ou português;
- 6.7.4. Acesso seguro 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, por parte da CONTRATANTE, utilizando-se de código individual, a ferramentas de autosserviço no sítio do fabricante, que permitam o diagnóstico e sugestões de solução de problemas quando possível.
- 6.8. Deverá haver prestação de assistência técnica por parte da CONTRATADA, durante a vigência dos contratos, contemplando, no mínimo, o serviço de atendimento telefônico gratuito (0800), com atendimento no idioma português, e suporte remoto via web, ambos em regime de 7 (sete) dias por semana, 24 (vinte e quatro) horas por dia; esse serviço poderá ser usado para abrir solicitações de informações, reportar incidentes ou esclarecer dúvidas quanto à utilização dos produtos e soluções fornecidos.
- 6.8.1. O atendimento de chamadas telefônicas por meio de central de atendimento a ser provida pela CONTRATADA deve estar disponível através de serviço de Discagem Direta Gratuita – DDG (0800).
- 6.9. Os chamados deverão ser registrados e deverão estar disponíveis para acompanhamento pela(s) equipe(s) da CONTRATANTE, e deverão conter data e hora da chamada, descrição do problema ocorrido, descrição da resolução e data e hora de conclusão.
- 6.10. O registro do horário da abertura do chamado será feito através do número do protocolo de atendimento que deverá ser informado pela Contratada ou através do horário de envio do e-mail com a solicitação da Contratante.
- 6.11. Entende-se por término do atendimento a disponibilidade do equipamento para uso em perfeitas condições de funcionamento no local onde está instalado, estando condicionado à aprovação da equipe técnica do Ministério da Justiça e Segurança Pública.
- 6.12. Entende-se por tempo de solução o prazo compreendido entre o horário de abertura do chamado na Central de Atendimento da Contratada até a solução do incidente/problema, com a entrega e instalação do equipamento/peça (hardware) em pleno funcionamento, quando for o caso.
- 6.13. O chamado aberto junto à Contratada, após fechado, poderá ser reaberto, se necessário, a qualquer momento fazendo referência ao número original de identificação da chamada.
- 6.14. O tempo de solução de problema poderá ser suspenso, reavaliado ou aceito somente para os casos em que a Contratada justificar que não deu causa ao atraso e que tenha sido analisada e julgada procedente pela equipe de fiscalização do contrato.
- 6.15. O atendimento deverá ser realizado, de acordo com a SEVERIDADE do problema, nos seguintes prazos, após a solicitação formal:
- 6.15.1. **SEVERIDADE BAIXA**: o equipamento, acessório, periférico ou produto apresenta pane, falha ou não conformidade técnica que causa restrições de operação de funções acessórias. Aplicado para instalação, configuração, manutenção preventivas, aplicações de firmwares e esclarecimento técnico relativo ao uso dos equipamentos ou solução. O primeiro retorno telefônico da CONTRATADA deve ser realizado em no

máximo 4 (quatro horas) e a solução técnica, definitiva ou de contorno, não poderá exceder a 72 (setenta e duas horas), contadas do chamado técnico;

- 6.15.2. **SEVERIDADE MÉDIA:** o equipamento, acessório, periférico ou produto apresenta pane, falha ou não conformidade técnica que prejudica a operação, uso ou acesso de função básica. Aplicado quando há falha no uso dos equipamentos ou solução, estando ainda disponíveis, porém apresentando problemas ou instabilidade. O primeiro retorno telefônico da Contratada deve ser realizado em no máximo 4 (quatro horas) e a solução técnica, definitiva ou de contorno, não poderá exceder a 24 (vinte e quatro horas), contadas do chamado técnico;
- 6.15.3. **SEVERIDADE ALTA:** o equipamento, acessório, periférico ou produto apresenta pane, falha ou não conformidade técnica que o torna total ou parcialmente inoperante. Aplicado para os casos em que a solução encontra-se operante, mas com redução importante de desempenho e/ou funcionalidade. O primeiro retorno telefônico da Contratada deve ser realizado em no máximo 2 (duas horas) e a solução técnica, definitiva ou de contorno, não poderá exceder a 12 (doze horas), contadas do chamado técnico;
- 6.15.4. **SEVERIDADE CRÍTICA:** o equipamento, acessório, periférico ou produto apresenta pane, falha ou não conformidade técnica que o torna total ou parcialmente inoperante. Aplicado para os casos em que a solução encontra-se indisponível e/ou inoperante. O primeiro retorno telefônico da Contratada deve ser realizado em no máximo 1 (uma hora) e a solução técnica, definitiva ou de contorno, não poderá exceder a 8 (oito horas), contadas do chamado técnico.
- 6.16. As tabelas a seguir representam as relações entre o tempo, em horas, para resolução do chamado e as respectivas sanções administrativas aplicáveis para cada caso de acordo com a gravidade do problema, nos seguintes prazos, após a solicitação formal:

GRAU	CORRESPONDÊNCIA
BAIXO	0,2% por hora acima do previsto sobre o valor do item afetado no chamado.
MÉDIO	0,4% por hora acima do previsto sobre o valor do item afetado no chamado.
ALTO	0,8% por hora acima do previsto sobre o valor do item afetado no chamado.
CRÍTICO	1,6% por hora acima do previsto sobre o valor do item afetado no chamado.
	1,6% por dia de atraso acima do previsto sobre o valor da OSFB, até o limite de 15 (quinze)

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

- 6.18. Caso a CONTRATADA verifique a necessidade de encaminhar equipamento para assistência técnica, deverá providenciar o imediato empréstimo de outro equipamento à CONTRATANTE, em perfeito estado de funcionamento e com características técnicas idênticas ou superiores às daquelas do equipamento defeituoso, o qual o substituirá até a conclusão de seus reparos. É responsabilidade da CONTRATADA a instalação e configuração do novo equipamento, garantindo o funcionamento da solução dentro das mesmas condições anteriores ao problema. A partir do pleno estado de funcionamento do novo equipamento, ficará suspensa a contagem do prazo de solução definitiva. Cabe lembrar que a CONTRATADA é responsável pela garantia do sigilo das informações configuradas no equipamento.
- 6.19. Os equipamentos substitutos deverão ser instalados e ativados no ambiente do MJSP, de modo a garantir que todas as funções e atividades providas pelo equipamento original estejam totalmente operacionais e ambientadas de acordo com as necessidades do Ministério da Justiça e Segurança Pública.
- 6.20. Se, em razão da complexidade dos reparos, for necessária a remoção do equipamento das instalações da CONTRATANTE, observar-se-á o seguinte:
- 6.20.1. A remoção somente será possível mediante justificativa, por escrito, sobre a situação técnica ao servidor responsável pelo acompanhamento dos serviços, que, após constatar tal necessidade, autorizará a saída também por escrito, desde que não prejudique a segurança dos dados produzidos ou sob guarda do Ministério da Justiça e Segurança Pública.
- 6.20.2. É responsabilidade da CONTRATADA a realização de toda e qualquer atividade necessária para o transporte, ativação, ambientação e adaptação dos equipamentos (incluindo a instalação e customização de softwares e migrações de dados), assim como a sua posterior desinstalação e remoção com reinstalação dos itens definitivos, em razão de atividades de garantia e manutenção.
- 6.20.3. Todas as despesas referentes ao transporte e ao seguro do equipamento correrão por conta da CONTRATADA, sendo sua exclusiva responsabilidade reparar quaisquer avarias decorrentes deste transporte.
- 6.21. O equipamento colocado em substituição ficará instalado nas dependências da CONTRANTE até a devolução do equipamento consertado, que deverá ocorrer no prazo de até 30 (trinta) dias corridos após a sua retirada para reparos.
- 6.22. Quando constatada a impossibilidade do conserto ou passados 30 (trinta) dias corridos, a substituição passará a ser definitiva.
- 6.23. As peças e componentes substituídos deverão ser entregues à CONTRANTE, juntamente com o equipamento consertado, salvo definição contrária pela Equipe de Fiscalização do Contrato. Qualquer substituição deverá ser acompanhada por técnico designado pela CONTRATANTE.
- 6.24. Os componentes instalados em substituição aos danificados deverão ter características, no mínimo, iguais aos originais do equipamento. Caso sejam utilizados componentes com características superiores, não haverá ônus adicional para a CONTRATANTE. Os componentes instalados em substituição a componentes defeituosos passarão a fazer parte do equipamento, sendo, portanto, de propriedade da CONTRATANTE.
- 6.25. Todas as peças, dispositivos ou mesmo unidades que forem substituídas durante o período de garantia terão, a partir de sua entrega, todas as garantias descritas neste item.

- 6.26. Correrá por conta exclusiva da Contratada a responsabilidade pelas manutenções nos endereços do MJSP, bem como pelo deslocamento de seus técnicos ao local de instalação do equipamento, pela retirada e entrega do mesmo e por todas as despesas de transporte, estada, frete e seguro correspondentes ou quaisquer outras necessárias ao cumprimento do serviço de manutenção.
- 6.27. A Contratada apresentará ao Ministério da Justiça e Segurança Pública, em cada manutenção realizada, um Relatório de Visita Técnica, nele constando a descrição clara do(s) problema(s) identificado(s) e os procedimentos adotados para a sua resolução.
- 6.28. Os chamados somente poderão ser fechados após concordância e autorização da CONTRATANTE.
- 6.29. Deverá ser possível a Contratada gerar relatórios contendo as informações de data e hora de abertura e fechamento do chamado, nome do responsável pela abertura, nome do responsável pelo atendimento, número de controle (protocolo), nível de severidade, descrição sucinta do chamado, Nível de Serviço alvo e Nível de Serviço atingido.
- 6.30. Aplicar-se-á, no que couber, as disposições do Código de Proteção e Defesa do Consumidor, instituído pela Lei nº 8.078, de 11 de setembro de 1990.
- 6.31. A solução deverá possuir função de acesso remoto para diagnóstico pela CONTRATADA em caso de falhas ou defeitos. A função deve estar disponível de modo integral (servidores, armazenamento e software). Os dispositivos necessários para a implementação dessa funcionalidade são de responsabilidade da CONTRATADA, à exceção de eventual linha telefônica comum, ou conexão à internet, que será fornecida pela CONTRATANTE.
- 6.32. O acesso remoto será controlado pela CONTRATANTE e só poderá ser habilitado com autorização expressa da CONTRATANTE.
- 6.33. A CONTRATADA deve informar antecipadamente à CONTRATANTE qualquer necessidade de acesso remoto.
- 6.34. Todas as intervenções realizadas remotamente são de responsabilidade da CONTRATADA, cabendo ao mesmo responder por quaisquer danos porventura decorrentes dessas intervenções.
- 6.35. Os equipamentos, se aplicável, deverão possuir função de *call-home*, através de linha VPN (Virtual Private Network) ou acesso seguro, e diagnóstico remoto para a central da CONTRATADA, em caso de erros/defeitos.
- 6.36. A proponente deverá considerar em sua proposta de preços final todos os insumos que porventura sejam necessários para o pleno atendimento dos serviços contratados.
- 6.37. A garantia legal ou contratual do objeto tem prazo de vigência própria e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.
- 6.38. Os serviços deverão ser executados sem impacto na utilização do ambiente de TI da CONTRATANTE, de forma que os serviços mais críticos deverão ser executados em horário noturno e finais de semana, com agendamento prévio de janela para evitar qualquer risco de paralisação dos ativos.
- 6.39. A CONTRATADA deverá instalar e configurar todos os componentes das soluções descritas neste Termo de Referência e seus Anexos, bem como prestar serviço de suporte técnico às atividades operacionais

para o atendimento de demandas da CONTRATANTE referentes aos equipamentos e softwares adquiridos, envolvendo as seguintes atividades:

- 6.39.1. Substituição de equipamento defeituoso;
- 6.39.2. Atualização de firmware de hardware;
- 6.39.3. Aplicação de patches de segurança em todos os ativos envolvidos;
- 6.39.4. Recebimento e acompanhamento de alertas dos equipamentos;
- 6.39.5. Sustentação de rotinas operacionais, com 32h mensais remotas e limitado a solução contratada nesse instrumento;
- 6.39.6. Suporte na resolução de problemas;
- 6.39.7. Atualização de versões, releases e patches aplicados nos ativos, com o devido histórico.
- 6.40. Os serviços de instalação, assistência técnica, suporte e garantia deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

7. SERVIÇO DE INSTALAÇÃO E IMPLANTAÇÃO (ITENS 1 a 3, 7 e 8)

- 7.1. A CONTRATADA deve fornecer serviços de instalação e implantação das soluções dos grupos 1 e 2 (itens 1, 2, 3, 11 e 12), inclusos na aquisição dos itens referenciados.
- 7.2. Entende-se como serviço de instalação todos os serviços pertinentes ao completo funcionamento da solução, compreendendo a montagem, instalação física (inclusive a passagem de cabos e energização), lógica e configuração inicial dos componentes do sistema e/ou software.
- 7.2.1. A CONTRATADA é responsável por montar, instalar, ativar e configurar, visando o melhor desempenho possível, os equipamentos (hardware) e/ou softwares fornecidos e seus componentes, com o acompanhamento da equipe técnica do Ministério da Justiça e Segurança Pública, visando ao repasse de tecnologia e conhecimentos, em data e horário a serem determinados pela STI/SE/MJSP, em dia útil ou não.
- 7.2.2. A CONTRATANTE poderá solicitar que equipamentos sejam montados apenas dentro dos sítios onde serão implantadas as soluções de armazenamento. Isto se justifica devido ao piso até adentrar os respectivos locais não suportarem cargas elevadas de peso.
- 7.3. 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 e/ou softwares, nos dois sítios. Todas as condições da execução dependerão de aprovação da CONTRATANTE.
- 7.3.1. O cluster primário da solução dos itens 1 e 5, a solução de orquestração de backup do item 11 e uma unidade da solução de *appliance* de backup ou equivalente do item 12 deverão ser entregues e instalados no data center primário do MJSP localizado no endereço Esplanada dos Ministérios, Bloco T, Anexo II, Brasília/DF – CEP: 70.064-900.
- 7.3.2. O cluster secundário da solução dos itens 1 e 5 e uma unidade da solução de *appliance* de backup ou equivalente do item 12 deverão ser entregues e instalados no data center secundário do MJSP localizado no Prédio da sede da PRF – Complexo do MCTI - Setor Policial Sul, Área 5 - Quadra 3 – Bloco H (CICCN Nacional), Brasília/DF – CEP: 70.610-909.
- 7.3.3. A CONTRATADA deverá submeter para aprovação por parte da CONTRATANTE, em até 30 (trinta) dias antes da entrega das soluções, plano de entrega, instalação e configuração dos equipamentos e/ou software da solução ofertada nos ambientes mencionados.
- 7.3.4. O Plano de Entrega, Instalação e Configuração deverá conter, no mínimo:
- 7.3.4.1. Descrição da equipe do projeto de instalação, contendo nomes, contatos e papéis desenvolvidos por cada um;
- 7.3.4.2. Plano de comunicação;
- 7.3.4.3. Descrição das fases da instalação e configuração, atividades desenvolvidas em cada uma, metas, entregáveis e cronograma;

- 7.3.4.4. Detalhamento dos ativos necessários em cada etapa do processo;
- 7.3.4.5. Análises de risco e possíveis impactos das atividades para a infraestrutura da CONTRATANTE;
- 7.3.4.6. Detalhamento da topologia e configurações propostas. Deve-se englobar as especificidades de clientes e políticas atualmente implantadas atualmente na CONTRATANTE;
- 7.3.4.7. No caso do Grupo 2, deverá abranger as três camadas da arquitetura de backup da solução, contando com: Gerência e controle, Operação de mídia e Clientes.
- 7.4. O prazo para finalização da instalação e configuração será de 60 (sessenta) dias, contados a partir da data de aceitação dos respectivos Planos por parte da CONTRATANTE;
- 7.5. A CONTRATADA deverá prestar atualizações do estado da instalação e configuração. As atualizações devem evidenciar o percentual concluído, entregáveis, problemas e quaisquer outras questões que possam estar afetando o andamento do serviço.
- 7.6. Após a instalação, a CONTRATADA deverá proceder a configuração dos componentes de forma que toda a capacidade relativa ao item seja disponibilizada para uso.
- 7.7. 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.
- 7.8. A certificação dos técnicos deverá contemplar a habilitação para instalar, configurar e customizar todas as funcionalidades demandadas no Termo de Referência.
- 7.9. A instalação, montagem e configuração deve seguir sempre as melhores práticas levando em consideração as recomendações dos fabricantes dos equipamentos.
- 7.10. 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.
- 7.11. 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.
- 7.12. 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.
- 7.13. As configurações deverão seguir fielmente a padronização previamente estabelecida pela CONTRATANTE.
- 7.14. 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;

- 7.15. 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.

8. SERVIÇO DE OPERAÇÃO ASSISTIDA (ITENS 4 e 9)

- 8.1. O Serviço de Operação Assistida compreende o período pós-implantação das soluções, ao qual a CONTRADATA aloca uma equipe especializada, de preferência aquela responsável pela implantação, para o apoio à operação e monitoramento das soluções em produção e propiciar repasse contínuo de conhecimento e rápida solução de dúvidas à equipe técnica da STI/SE/MJSP.
- 8.2. Será dedicado o quantitativo de 80 horas contínuas, com início após o aceite do Serviço de Instalação e Implantação, para cada solução de armazenamento ou backup implantada.
- 8.3. Abrange as seguintes atividades:
 - 8.3.1. Auxiliar a STI/SE/MJSP na formulação da customização e parametrização do ambiente de produção, de acordo com as diretrizes e necessidades do MJSP;
 - 8.3.2. Apoiar o monitoramento dos eventos gerados pelos módulos de administração e gerenciamento da Solução;
 - 8.3.3. Apoiar o monitoramento de alertas dos módulos de administração e gerenciamento da Solução;
 - 8.3.4. Refinar e melhorar o processo de administração e gerenciamento da solução contratada nesse instrumento;
 - 8.3.5. Realizar e orientar testes de novas versões do software de Gerenciamento da Solução;
 - 8.3.6. Apoiar na geração de informações para a gestão da capacidade e do desempenho;
 - 8.3.7. Ao término da checagem geral deverá ser realizado um workshop de no mínimo 4 horas para repasse da arquitetura e topologia do das soluções implantadas. Deve ainda entregar documentação contendo, no mínimo:
 - 8.3.7.1. Mapa atualizado com arquitetura com a topologia;
 - 8.3.7.2. Descritivo do estado gerado da infraestrutura recém implementada de softwares e serviços, contemplando, no mínimo, configuração, versão, desempenho e status do ciclo de vida.
- 8.4. Transferência de Conhecimento**
 - 8.4.1. A Contratada deverá fornecer transferência de conhecimento da tecnologia implantada.
 - 8.4.2. A transferência de conhecimento deverá ter como base o acompanhamento da operação e monitoramento da solução implantada pela equipe técnica da STI/SE/MJSP para a plena operação do equipamento, bem como solução de dúvidas, capacitando a equipe técnica da STI/SE/MJSP a respeito da arquitetura (física e/ou lógica), configurações, modos de operação, monitoramento, procedimentos de abertura de chamados e outros requisitos básicos operacionais da solução adquirida.
 - 8.4.3.** Será adotado como índice de reajuste do Contrato o Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, a cada 12 meses de execução contratual.

9. SERVIÇO DE TREINAMENTO TEÓRICO/PRÁTICO (ITENS 5 e 10)

- 9.1. A CONTRATADA deverá providenciar treinamento teórico e prático (*hands-on*) para solução ofertada conforme melhores práticas na operação dos equipamentos e/ou softwares das soluções adquiridas.
- 9.2. A capacitação terá caráter teórico-prático dirigido, principalmente, para o contexto de atuação da equipe técnica e dos colaboradores da CONTRATANTE. Os serviços de treinamento deverão ser realizados de segunda a sexta-feira entre 8h e 18h, nas dependências da CONTRATANTE ou de forma remota.
- 9.3. Os instrutores do repasse deverão ter pleno conhecimento da arquitetura e configurações da solução instalada, bem como serem certificados pelo fabricante da solução.
- 9.4. A carga horária mínima de capacitação de tecnologia para as soluções de armazenamento é de 20 horas e da solução de backup é de 40 horas.
- 9.5. As turmas terão quantidade máxima de 6 alunos.
- 9.6. Os treinamentos deverão ser realizados, preferencialmente, em um único período do dia (manhã ou tarde), totalizando carga horária de 4h diárias mínima.
- 9.7. Os treinamentos deverão ser baseados em material e ementa oficial do fabricante.
- 9.8. O conteúdo programático da capacitação para as soluções de armazenamento (NAS e/ou Storage de Objetos) deverá abordar, no mínimo:
 - 9.8.1. Visão geral dos componentes dos equipamentos;
 - 9.8.2. Arquitetura física e lógica;
 - 9.8.3. Modos de operação;
 - 9.8.4. Configuração e operação básica e avançada;
 - 9.8.5. Comandos básicos;
 - 9.8.6. Atualização de firmware e diagnóstico dos equipamentos/software;
 - 9.8.7. Melhores práticas de configuração e uso;
 - 9.8.8. Uso dos componentes NAS e/ou storage de objetos e seus protocolos, incluindo S3;
 - 9.8.9. Snapshots;
 - 9.8.10. Desduplicação e Compressão de dados, caso se aplique;
 - 9.8.11. Gerência e monitoramento contínuo da solução;
 - 9.8.12. Replicação de dados.
- 9.8.13. O conteúdo programático da capacitação para a solução de backup deverá abordar, no mínimo:
 - 9.8.14. Apresentação da arquitetura da solução e dos conceitos fundamentais;
 - 9.8.15. Aspectos sobre instalação da solução;
 - 9.8.16. Configuração e gerenciamento da solução em níveis básicos e avançados;
 - 9.8.17. Operação completa da solução;
 - 9.8.18. Melhores práticas de backup da solução;
 - 9.8.19. Análise de logs e problemas;

- 9.8.20. Geração e customização de relatórios, caso aplicável;
- 9.8.21. Verificação de alertas e tomada de ações;
- 9.8.22. Desduplicação e compressão de dados da solução, caso se aplique;
- 9.8.23. Segurança da Informação da solução;
- 9.8.24. Otimizações ou desempenho (performance);
- 9.8.25. Troubleshooting.
- 9.9. Todo material didático deverá ser fornecido pela CONTRATADA e deverá estar incluso no escopo do treinamento.
- 9.10. Ao final do treinamento, deverá ser emitido o certificado de conclusão a cada participante, devidamente assinado pela empresa promotora, especificando o conteúdo programático completo do curso, corpo docente, data de início, data de fim e carga horária do treinamento.
- 9.11. Todo e qualquer custo envolvido na transferência de conhecimento tecnológico deverá correr por conta da CONTRATADA, sem nenhum ônus para o MJSP.
- 9.12. Após o treinamento inicial na entrega da solução, poderão ser requeridas novas turmas, para fins de capacitação e atualização dos colaboradores da CONTRATANTE, em virtude de turnover (rotatividade) e atualização tecnológica.
- 9.13. Este serviço será utilizado sob demanda, somente turmas aprovadas por Ordens de Serviço (OS) poderão ser executadas e posteriormente faturadas.
- 9.14. A vigência deste serviço é de 12 meses a partir do recebimento definitivo da respectiva solução, podendo ser renovado por igual período, até o limite máximo de 60 meses.
- 9.14.1. Será adotado como índice de reajuste do Contrato o Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, a cada 12 meses de execução contratual.

10. SERVIÇO DE SUPORTE ESPECIALIZADO (ITENS 6 e 11)

- 10.1. Tendo em vista a modernização da operação de infraestrutura de TIC do MJSP com recursos de armazenamento de rede por *storage* NAS e *storage* de objetos, solução de backup e de proteção de dados para backup, faz-se necessário contratar os respectivos serviços de suporte especializado.
- 10.2. O suporte especializado deverá apoiar na definição da melhor utilização dos recursos disponibilizados, inclusive para a adaptação de dados e de funcionalidades dos sistemas corporativos do Ministério da Justiça e Segurança Pública.
- 10.3. O suporte especializado deverá:
 - 10.3.1. Orientar na melhoria de métodos, procedimentos e técnicas utilizadas pela área de Infraestrutura, Segurança e de Desenvolvimento de Sistemas;
 - 10.3.2. Avaliar o desempenho do ambiente, com indicação das medidas recomendadas para sua otimização.
 - 10.3.3. Orientar e apoiar quanto à integração com:
 - 10.3.4. Soluções de segurança e de gestão de identidade e de acesso;
 - 10.3.5. Soluções de orquestração de ambientes em nuvem;
 - 10.3.6. Soluções de *Data Analytics*, caso aplicável;
 - 10.3.7. Ferramentas de *Backup* e *Restore* suportadas pelo produto;
 - 10.3.8. APIs de ferramentas de terceiros, entre outras tecnologias.
- 10.4. Orientar e apoiar na implementação de novas plataformas de desenvolvimento e/ou novas versões das plataformas existentes.
- 10.5. Orientar e apoiar quanto a métodos e procedimentos para a migração de objetos para outros equipamentos.
- 10.6. Este serviço será utilizado sob demanda, solicitadas com no mínimo 10 dias de antecedência e alocação mínima de 8h e somente horas previamente aprovadas por Ordens de Serviço (OS) poderão ser utilizadas/executadas, e posteriormente faturadas.
- 10.7. A vigência deste serviço é de 60 meses a partir do recebimento definitivo da solução implantada.
 - 10.7.1. Faz-se necessário um contrato de 60 meses considerando a necessidade de o serviço estar disponível durante todo o período de garantia do equipamento a ser fornecido.
 - 10.7.2. Será adotado como índice de reajuste do Contrato o Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, a cada 12 meses de execução contratual.