ANEXO I – ESPECIFICAÇÃO TÉCNICA

O documento Especificação Técnica traz o conjunto de informações necessárias para a especificação da parceria comercial, bem como as principais responsabilidades de cada uma das partes para a composição da solução objeto da parceria comercial. A solução proposta para estabelecimento da Parceria deve ser entregue com os requisitos abaixo:

1. CONDIÇÕES GERAIS DA PARCERIA COMERCIAL

Para composição da parceria comercial para oferta da solução BaaS GovCloud, as seguintes condições deverão ser atendidas pela potencial parceira, descrita a seguir como PARCEIRA, juntamente à DATAPREV:

1.1. A composição da solução BaaS GovCloud será realizada por meio da modalidade de Parceria Comercial. Nesse sentido, todos os riscos envolvidos para operacionalização da solução serão compartilhados entre DATAPREV e PARCEIRA através do atendimento dos requisitos listados nos próximos tópicos e seções do presente documento;

1.2. A PARCEIRA deverá disponibilizar HARDWARES, SOFTWARES, CAPACITAÇÃO, SUPORTE, MANUTENÇÕES CORRETIVAS E EVOLUTIVAS e demais itens necessários à composição da solução conforme especificado nesta seção do documento;

1.3. Sob nenhuma hipótese a DATAPREV arcará com custos relacionados ao direito de uso dos *softwares*, *hardwares* bem como os custos relacionados à futuras atualizações, garantias, manutenção e suporte, sendo estes de inteira responsabilidade da PARCEIRA;

1.4. A DATAPREV não ficará responsável pela instalação, manutenção e suporte continuado de tais softwares, hardware e ferramentas, devendo essa ser uma das responsabilidades da PARCEIRA.

1.5. O ANS (Acordo de Nível de Serviço) de disponibilidade do armazenamento de dados deve ser igual ou superior a 98% para cada período de 1 mês.

1.6. A DATAPREV fará uso e efetuará pagamento apenas aos serviços efetivamente consumidos e/ou solicitados à PARCEIRA, pagamento sob consumo;

1.7. A DATAPREV deverá indicar quais data centers possuem os requisitos necessários para implantação de equipamento fornecida pela PARCEIRA, que viabilizará a oferta da solução;

1.8. A DATAPREV deverá alocar time especializado para a operação e a manutenção de equipamentos em data centers em conformidade com os padrões técnicos necessários para operacionalização de serviço mantendo todos os padrões atuais da DATAPREV, Tier III;

1.9. Todos os serviços descritos deverão ser executados em ambiente local (DATA CENTER) da DATAPREV sendo este obrigatoriamente em território nacional brasileiro;

1.10. A DATAPREV e a PARCEIRA deverão estabelecer metas de comercialização e realizar a prospecção ativa de clientes de forma a perseguir o superávit na operação comercial da solução;

1.11. A operacionalização da solução deverá garantir a prevalência da legislação brasileira, isto é, quaisquer contratos eventualmente assinados relacionados ao consumo de tecnologias, infraestruturas, serviços ou ações de qualquer natureza relacionadas ao provisionamento da solução devem garantir que a legislação brasileira é soberana;

1.12. Deverá ser disponibilizado pela PARCEIRA um portal contendo informações sobre:

1.12.1. Relatório de Faturamento: relatórios com consumo de serviços e métricas de bilhetagem compatíveis aos padrões de mercado;

1.12.2. Relatórios e/ou *dashboards* de avaliação e otimização de performance;

1.12.3. Os relatórios e/ou *dashboards* deverão ser disponibilizados pelo portal de gestão, com periodicidade em horas, diária, semanal e/ou mensal. O serviço estará dentro das responsabilidades da PARCEIRA, não sendo cobrado como serviço adicional;

1.13. A plataforma de gerenciamento de serviços citada atuará como plataforma de governança, provisionamento de serviços, gerenciamento de políticas, gerenciamento de custos e gerenciamento de operações;

1.14. A DATAPREV não ficará responsável pela instalação, manutenção técnica e suporte técnico continuado de tais *softwares*, *hardwares* e ferramental, nem emitirá ordens de serviço para esses fins, devendo essa ser uma das responsabilidades da PARCEIRA;

1.15. No caso de encerramento da parceria comercial por qualquer razão, a PARCEIRA deverá fornecer soluções que permita a DATAPREV integração com solução externa de forma a viabilizar a continuidade do serviço em conformidade com os requisitos elencados no presente termo de referência;

1.16. Todos os serviços de armazenamento de dados prestados pela PARCEIRA devem ser realizados de modo que os dados da DATAPREV provisionados na solução em nuvem privada ou comunitária, sejam portáveis para outros provedores e soluções, sem nenhuma possibilidade de aprisionamento tecnológico (*lock in*) de qualquer natureza;

1.17. A composição do modelo de comercialização da solução a ser composto com a PARCEIRA deve incluir os principais elementos relacionados à comercialização de soluções no modelo de nuvem computacional elencados no Plano Diretor de Tecnologia da Informação (PDTI) 2022 – 2026 da DATAPREV, a saber:

1.17.1. Os serviços disponibilizados na plataforma de nuvem da Empresa devem seguir cinco premissas: autosserviço, pagamento sob consumo, alta disponibilidade, escalabilidade e desempenho;

1.17.2. As parcerias comerciais com os fabricantes de tecnologias devem ser abrangentes, englobando o maior número possível de *softwares* e plataformas, o que oferece maior capacidade de escolha aos clientes;

1.17.3. Os contratos a serem firmados dentro de um processo de parceria estratégica devem: ser faturados em Reais (R$); privilegiar a contratação direta do detentor da patente, fabricante e/ou desenvolvedor; e dar preferência à contratação de serviços por pagamento sob uso e a ausência de franquia mínima, com bilhetagem orientada a métricas usuais de mercado;

1.17.4. Os modelos de negócio para os produtos de nuvem devem considerar a preparação da empresa para suportar o movimento de transferência dos *workloads* da TI tradicional para a nuvem.

1.18. A PARCEIRA deverá ser responsável pela aquisição e todo investimento financeiro em equipamentos (*appliances*) que estejam diretamente relacionados à oferta da solução objeto da parceria comercial;

1.19. A PARCEIRA deverá ser responsável tecnicamente e financeiramente pela ativação dos serviços, que pode envolver, mas não se limita a atividades relacionadas a licenciamento de software, customizações dos equipamentos e do *software* necessário para composição da solução e todas as ações necessárias para garantir que a solução estará de acordo com as características da solução (ver seção 2 do presente documento).

1.20. A DATAPREV realizará o pagamento da parte combinada com a PARCEIRA apenas do que for contratado pelo cliente final (de forma que o requisito de pagamento sob consumo seja viabilizado para os clientes finais da solução);

1.21. A PARCEIRA deverá atuar em conjunto com a DATAPREV para garantir a operacionalização da solução, envolvendo (mas não se restringindo) às seguintes atividades:

1.21.1. Manutenção física dos equipamentos, garantindo um SLA compatível com a oferta desse serviço com as principais nuvens públicas;

1.21.2. Expansão física dos equipamentos quando necessária;

1.21.3. Realizar o suporte para os times da DATAPREV envolvidos com a operação da solução;

1.21.4. Realizar a substituição de partes e peças do equipamento quando necessário;

1.21.5. Apoiar a execução do ciclo-de-vida dos equipamentos e softwares envolvidos com a operacionalização da solução, incluindo a realização de procedimentos relacionados ao *End-of-Line* (EOL) da solução;

1.21.6. Adicionar componentes relacionados à novas tecnologias quando necessário;

1.21.7. Realizar a migração dos equipamentos físicos quando necessário;

1.21.8. Atualização de *firmware* quando necessário;

1.21.9. Manutenção evolutiva e corretiva do *software* da solução.

1.22. A PARCEIRA deverá ser responsável pela instalação dos equipamentos em DATACENTER da DATAPREV. A quantidade de equipamentos necessários à prestação dos serviços ficará a critério da PARCEIRA.

1.23. Os serviços descritos deverão ser executados em ambiente local (datacenter) da DATAPREV. Os locais de instalação ficarão a critério da DATAPREV;

1.24. A PARCEIRA deverá fornecer solução que permita a DATAPREV realizar backup das aplicações e cópias dos dados armazenados nos dispositivos de armazenamento em nuvem privada, através do catálogo de serviços.

2. Das características da composição da Parceria Comercial

A solução proposta deve ser entregue em um modelo de computação em nuvem, com agregação dos seguintes valores:

2.1. A solução deve endereçar, no mínimo, os seguintes requisitos funcionais:

2.1.1. Atender o escopo abrangendo o conjunto de dados digitais que devem ser salvaguardados, restrito aos sistemas e soluções suportados pela solução BaaS GovCloud;

2.1.2. A realização de backup deve obedecer às frequências diária, semanal, mensal e anual;

2.1.3. O período de retenção deve ser customizado pelo usuário cliente em conformidade com a política de backup estabelecida em sua organização;

2.1.4. Deve viabilizar a realização de procedimento de recuperação de dados (*restore*)

2.2. Deve ter mecanismos para viabilizar o requisito de imutabilidade dos dados;

2.3. Deve possuir portal de gerenciamento centralizado para todas as instancias de armazenamento instaladas nos data centers Dataprev e de seus clientes;

2.4. Deve permitir o crescimento de espaço de armazenamento de forma ilimitada;

2.5. Deve ser possível realizar a manutenção do ciclo-de-vida dos equipamentos e de todo licenciamento de *software* sem custos adicionais;

2.6. Deve permitir a execução de rotinas de backup possuindo mecanismos de reserva de banda para as rotinas de backup (*throttling*);

2.7. deverá possuir mecanismos de reserva de banda para as rotinas de backup (throttling)

2.8. Deve permitir técnicas de compressão de dados otimizada obedecendo as janelas de backup;

2.9. As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como unidade e temperatura, e com acesso restrito a pessoas autorizadas conforme política de segurança, conforme Resolução de Conselho CADM/009/2020;

2.10. A solução deve ofertar possibilidade de migração de *backup* para outras plataformas de outros fornecedores, de forma a garantir a continuidade da operação em caso de encerramento de contrato (evitando *lock-in*);

2.11. Mantém o ambiente protegido de forma fácil e segura com criptografias dos dados. Considerar a melhor técnica de criptografia de acordo com o estado do dado (at rest: dados que não estão sendo acessados e são armazenados em um meio físico ou lógico; in transit: informações que estão viajando de um ponto a outro; in use: quando acesso por um usuário ou aplicativo) evitando, entre outros, ataques "*men in the middle*";

2.12. Deve possuir um portal de Provisionamento do cliente e de autosserviço;

2.13. Portal de gestão do *tenant* (incluindo discos, segurança, rede, performance, backup, docker);

2.14. Bilhetagem de todas as ações (volume, performance, put/get/up/down/snapshots/criptografia) que poderão ser tarifadas à semelhança das nuvens públicas tradicionais;

2.15. Capacidade de integração com a solução através do consumo via API;

2.16. Pagamento apenas do alocado (pelo cliente) *win/win*;

2.17. Viabilizar a oferta de backup integrada com nuvens públicas de mercado.

3. RESPONSABILIDADES DA PARCEIRA E DA DATAPREV

3.1. DA DATAPREV

Para composição da oferta de Backup como Serviço em Nuvem Computacional, a **Dataprev** deverá atender aos seguintes requisitos/atividades:

3.1.1. Identificar datacenter com requisitos necessários para implantação de equipamento fornecida pela PARCEIRA para viabilizar a oferta da solução;

3.1.2. Alocar time especializado na operação e manutenção de equipamentos em datacenter em conformidade com os padrões técnicos necessários para operacionalização de serviço mantendo padrão tier III (realizando suporte de 1º nível da solução);

3.1.3. Realizar, juntamente à PARCEIRA, preparação de pessoal para operação, suporte e manutenção de equipamentos e *softwares* relacionado ao objeto da parceria;

3.1.4. Deve estabelecer, juntamente ao PARCEIRO, a composição de modelo de comercialização para oferta da solução BaaS GovCloud, identificando os elementos de composição da solução para atendimento das instruções normativos e demais regulações dos órgãos de controle (IN GSI/PR 01 de 13 de junho de 2008 e IN GSI/PR 05 de 30 de agosto de 2021, Instruções decorrentes da auditoria TC 036.620/2020-3 do Tribunal de Contas da União)

3.1.5. Deve preparar, juntamente a PARCEIRA, equipe especializada no suporte/operacionalização da solução para apoiar a composição, por parte dos clientes, de políticas de *backup* e *restore* em conformidade com a norma ABNT NBR ISO/IEC 27002 de 2013:

3.1.5.1. Apoio técnico à composição de política de *backup* ou instrumento normativo equivalente, com a identificação de procedimentos/roteiros para apoiar atividades de *backup* e *restore* de sistemas específicos identificados pelo cliente como necessários para atendimento das necessidades de negócio e/ou requisitos da organização onde atua;

3.1.5.2. Viabilizar a testagem regular das cópias de segurança através de testes de recuperação/restauração (*restore*) a fim de detectar eventuais falhas;

3.1.5.3. Apoiar as definições relacionadas a requisitos específicos de segurança da informação, tais como controles de acesso lógico, uso de criptografia, armazenamento em local seguro, armazenamento em local remoto seguro diferente do local original e demais requisitos e a forma como são viabilizados na oferta de nuvem;

3.1.5.4. Apoiar a definição da abrangência, escopo, frequência, tipos de cópias e tempo de retenção das cópias de segurança de dados dos sistemas do cliente, identificando

os meios pelos quais o cliente deve realizar a configuração da gestão das cópias em ferramenta ofertada pela solução;

3.1.5.5. Apoio na configuração dos requisitos necessários para a documentação dos eventos por meio de registros (*logs*) relativos a todos os itens restaurados;

3.1.6. Deve realizar as customizações necessárias no ambiente para garantir as principais características da oferta da solução em nuvem:

3.1.6.1. Autosserviço sob demanda;

3.1.6.2. Amplo acesso via rede;

3.1.6.3. Organização e gerenciamento em grupos de recursos: recursos agrupados para suportar a oferta múltiplos inquilinos;

3.1.6.4. Rápida elasticidade;

3.1.6.5. Serviço Mensurado;

3.1.6.6. Serviço Monitorado e Automático

3.1.7. A equipe da Dataprev deve envidar esforços para que as recomendações da Instrução Normativa GSI/PR 5, de 30 de agosto de 2021 do gabinete de segurança institucional da presidência da república esteja atendida.

3.2. DA PARCEIRA

3.2.1. REQUISITOS GERAIS

Para composição da oferta de Backup como Serviço em Nuvem Computacional, o **PARCEIRO** deverá atender aos seguintes requisitos/atividades:

3.2.1.1. Instalação de solução (appliance) para composição de oferta de Backup-as-a-Service na modalidade on premises com suporte para backup de cargas de trabalho, bem como o restore, atendendo as principais características da oferta da computação em nuvem: autosserviço, pagamento sob consumo, escalabilidade. A solução deverá atender os seguintes requisitos:

3.2.1.2. Suporte a múltiplos inquilinos (multitenant) de forma que os acessos, carga de trabalho e dados possam ser isolados logicamente entre os inquilinos, garantindo a segurança dos dados e o desempenho das aplicações

3.2.1.3. Permita a contratação e o consumo do serviço sob medida, podendo ser adicionado ou reduzido conforme demanda;

3.2.1.4. Permita a medição e consulta dos recursos que foram utilizadas pelos clientes, através de mecanismos de fácil utilização para estas operações, e que permita a integração com outras soluções de bilhetagem;

3.2.1.5. Implemente mecanismos de alta disponibilidade e contingência dos dados para garantir o SLA mínimo de 98% do produto;

3.2.1.6. Tenha capacidade de escalar (liberando pode computacional adicional) horizontalmente e verticalmente para suportar o crescimento futuro de demandas dos clientes e que esta operação possa ser realizada sem *downtime* para os clientes;

3.2.1.7. Permita a replicação de dados localmente e remotamente

3.2.1.8. Garanta um tempo de atendimento e de resolução de chamados técnicos compatível com ambientes de produção;

3.2.1.9. Garanta o controle de acesso e possua mecanismos de auditoria;

3.2.1.10. Possua funções de backup com frequência diária, semanal, mensal e anual;

3.2.1.11. Implemente criptografia dos dados salvos;

3.2.1.12. Implemente desduplicação de dados, permitindo maior capacidade lógica de armazenamento;

3.2.1.13. Permitir a realização de backup e *restore*;

3.2.1.14. Seja capaz de criar políticas de backup personalizadas para viabilizar diferentes modelos de ofertas do produto pela Dataprev e para atender as necessidades específicas de cada cliente;

3.2.1.15. Possibilite o reuso dos dados protegidos (data reuse);

3.2.1.16. Possua relatórios das atividades de backup e *restore*;

3.2.1.17. Permita o monitoramento das atividades de backup e *restore* e o disparo automatizado de alertas de status destas operações;

3.2.1.18. Disponibilize REST APIs para integração com outras aplicações e para automações de operações na nuvem

3.2.1.19. Implemente controle granular de acesso (RBAC) e integração com o protocolo LDAP (Microsoft AD e/ou Open LDAP);

3.2.1.20. Implemente mecanismo de cópia e arquivamento de dados salvos (archiving) para outros storages (objeto ou bloco) e fitas de backup.

3.2.1.21. Permita a migração dos dados armazenados em caso de cancelamento de contrato, evitando a ocorrência de *lock-in*.

3.2.2. REQUISITOS FUNCIONAIS E NÃO FUNCIONAIS DA SOLUÇÃO A SER OFERTADA PELA PARCEIRA

Providenciar a instalação, configuração, capacitação e suporte especializado no(s) equipamento(s) (*appliance*) dedicados para composição de *software* e *hardware* especializado na oferta de soluções de *backup* e *restore* em nuvem computacional, na modalidade *on-premises*, em um ou mais dos datacenters da Dataprev, que atendam aos requisitos listados a seguir:

3.2.2.1. A solução deverá ser suportada por máquinas virtuais adequadas para uso de software básico dos principais sistemas operacionais de mercado;

3.2.2.2. Deve possuir volume em armazenamento compartilhado com utilização de discos mecânicos (HDD) ou discos de estado sólido (SSD) ou tecnologias equivalentes;

3.2.2.3. Serviço de gerenciamento de áreas de armazenamento implementando criptografia de volumes e arquitetura em regime de *failover*, para garantir a continuidade dos serviços em caso de falha de operação de forma transparente e sem perda de informações;

3.2.2.4. Licença de Antivírus fornecendo proteção para compartilhamento de arquivos disponibilizados. Deve incluir a atualização automática das vacinas e do mecanismo de verificação de vírus durante toda a vigência do contrato.

3.2.2.5. Deve permitir a execução de tarefas com necessidades de acesso massivo a dados armazenados, tais como indexação, classificação e conversão de dados, scripts ou ferramentas de auditoria de dados (logs), varredura de antivírus, entre outros;

3.2.2.6. Deve possuir funcionalidades relacionadas à oferta de Backup como Serviço (BaaS) em nuvem, com as seguintes características:

3.2.2.6.1. Licença de uso de *software* na modalidade subscrição para proteção de dados em ambientes virtuais;

3.2.2.6.2. Serviço de utilização de funcionalidade de proteção de dados para máquinas virtuais, realizando os *backups* online sem a necessidade de interrupção do serviço em ambiente *on-premises*, fazendo interface direta com a camada de gerência dos sistemas de virtualização sem requerer instalação de software de *backup* em cada máquina virtual:

3.2.2.6.2.1. Capturar uma imagem completa de máquina virtual;

3.2.2.6.2.2. Restauração de arquivo dentro de máquina virtual sem requerer a restauração total do backup da imagem da máquina virtual;

3.2.2.6.2.3. *Backup* de arquivos hospedados nos principais sistemas operacionais de mercado (ex.: Microsoft Windows e Linux) sem requerer instalação de agentes de *backup*, por meio de ferramentas instaladas automaticamente nas máquinas virtuais;

3.2.2.6.3. Compatibilidade com os principais sistemas operacionais de mercado e backup consistente com diversas aplicações (ex.: Microsoft Active Directory, Exchange, *SharePoint*, SQL Server, Banco de Dados Oracle, MySQL, PostgreSQL, realizando *backups* online sem necessidade de interrupção de serviço);

3.2.2.6.4. Caso seja utilizado software de terceiros na solução, o ciclo-de-vida da solução de terceiros deve ser divulgado com antecedência e os prazos de atualização/manutenção devem ser obedecidos para garantir a continuidade do serviço.

3.2.2.6.5. Deve implementar estratégia de tolerância a falhas (ex.: através de balanceamento de carga), suportar algoritmos de compressão e desduplicação de dados, armazenamento de máquinas virtuais em arquivos de backup distintos, criptografia de dados na origem compatível com modernos padrões de criptografia (ex.: *Advanced Encryption Standard - AES*).

3.2.2.6.6. Deve permitir integração com soluções externas de forma a viabilizar a continuidade do serviço em caso de encerramento contratual (evitando ocorrência de *lock-in*);

3.2.2.6.7. Deve suportar paralelamente as operações de *backup* e *restore* (recuperação);

3.2.2.6.8. Deve suportar a realização de backup nas modalidades full e incremental, permitindo a realização de backups com as frequências diária, semanal, mensal e anual;

3.2.2.6.9. Deve permitir a verificação e checagem automática da consistência dos arquivos de *backup* para garantir a integridade dos dados e verificação de *malware* antes da recuperação de dados para ambiente de produção;

3.2.2.6.10. Deve implementar requisito de imutabilidade dos dados;

3.2.2.6.11. Deve suportar integração com as principais nuvens públicas, tais como integração com repositório em nuvem e a realização de *backups* virtuais e de áreas de armazenamento localizadas em nuvens públicas;

3.2.2.6.12. Deve possuir módulo analítico de proteção de dados em ambiente virtual, fornecendo licença de uso de *software* específico de funcionalidades analíticas, geração de relatórios, com capacidade de exportação para diversos

formatos, identificando os recursos que possuem *backup*, rotinas de *backup*, *restore*, e capacidade de avaliar consumo de processamento, armazenamento, memória e bilhetagem com métricas usuais de mercado de forma a viabilizar a administração do ambiente pelo gestor responsável;

3.2.2.7. Deve entregar o gerenciamento de BaaS em nuvem *on-premises* com funcionalidades equivalentes às modernas plataformas de CMP (*Cloud Management Platform*): suporte a múltiplos inquilinos, autosserviço, bilhetagem automática, pagamento sob consumo e capacidade de gerenciar requisitos de escalabilidade, segurança e controle de acesso;

3.2.2.8. Preferencialmente integrável com repositório de *object storage* remoto, com serviços de inclusão, leitura, exclusão e consultas, acessíveis por meio de API específica;

3.2.2.9. Deve possuir nível de serviço compatível com as principais ofertas de solução no mercado, com possibilidade de monitoramento proativo do ambiente para garantir o atingimento de nível de serviço;

3.2.2.10. Deve atender os requisitos de segurança para garantir a proteção de dados, antecipando ameaças à privacidade, à segurança, e à integridade, prevenindo acesso não autorizado às informações;

3.2.2.11. Deve implementar segurança nas requisições, permitindo criptografia de canal para evitar ataques do tipo "*men in the middle*" (Considerar a melhor técnica de criptografia de acordo com o estado do dado);

3.2.2.12. Deve implantar listas de controles de acesso (ACLs) para conceder permissões específicas a usuários específicos para um recurso ou para um objeto.

3.2.2.13. Permitir a configuração dos equipamentos por CLI (*command line interface*) através de conexão SSH (*secure shell*), além de incluir ferramenta com interface gráfica (GUI) ou WEB (https) que permita gerenciamento integrado do ambiente (*hardware* e *software*), possibilitando:

3.2.2.13.1. Visão unificada do sistema (*dashboard*);

3.2.2.13.2. Gerenciamento de política de *backup* centralizada;

3.2.2.13.3. Ponto único e centralizado de administração com controle baseado em regras (*Role-Based Access Control - RBAC*);

3.2.2.13.4. Visão global de todos os elementos de hardware que compõem a solução;

3.2.2.13.5. Realização de operações de *backup*, *restore*, definição de políticas de backup, análise e edição de *jobs*, consulta de logs e configuração de todos os elementos que compõem a solução;

3.2.2.13.6. Análise de planejamento de capacidade (com histórico) e carga de utilização do equipamento.

3.2.2.13.7. Autenticação integrada dos usuários com suporte ao protocolo LDAP (*Lightweight Directory Access Protocol*).

3.2.2.13.8. Relatórios administrativos, tais como: percentual de Jobs com falha por período e utilização dos recursos de armazenamento.

3.2.2.14. A solução deverá implementar estratégias de QoS para melhor consumo de recursos de rede;

3.2.2.15. A solução deverá ser tolerante a falhas, de modo que a ocorrência de uma ou mais falhas, total ou parcial, de qualquer um dos seus componentes sejam imperceptíveis aos dispositivos externos.

3.2.2.16. A solução deverá prover mecanismo de proteção dos dados armazenado, de forma a suportar a falha simultânea de dois discos quaisquer, sem interrupção do serviço.

3.2.2.17. Os equipamentos devem permitir a substituição dos componentes redundantes sem interrupção do serviço (estratégia conhecida como *hot swapping*);

3.2.2.18. Os equipamentos deverão prover total e plena disponibilidade das informações armazenadas mesmo em face de atividades de manutenção técnica, tais como substituição de componentes, *upgrade* de capacidade ou alteração de características funcionais;

3.2.2.19. Fornecer funcionalidade para:

3.2.2.19.1. O sistema deve permitir manter políticas de retenção dos dados diferentes entre a origem e o destino da replicação;

3.2.2.19.2. O restore deve ser realizado de modo que não impacte a continuidade do negócio;

3.2.2.19.3. O sistema deve ser capaz de enxergar e recuperar dados de *backup* mesmo a partir de uma réplica.

3.2.3. OFERTA DE SOFTWARE PARA GERENCIAMENTO DA REALIZAÇÃO DE BACKUP COMO SERVIÇO (BAAS) NO LADO CLIENTE

3.2.3.1. Plataforma de gerenciamento de recursos e oferta da solução com suporte a múltiplos inquilinos compatíveis às modernas soluções de gestão de *Backup* do lado cliente:

3.2.3.2. A ferramenta deve prover gerenciamento de custos;

3.2.3.3. Configuração para definição de política de backup (frequência de realização de backup, definição de cargas de trabalho), realização de procedimento de *restore*, integração com sistemas objeto de *backup*.

3.2.3.4. Implemente Políticas de monitoramento de alertas;

3.2.3.5. Possibilitar a previsão de custos e visualização do orçamento;

3.2.3.6. Permitir políticas de alertas de orçamento;

3.2.3.7. Disponibilizar relatório de faturamento apresentando com consumo mensal de serviços dos provedores na métrica do item do serviço, utilizando, entre outras unidades de medida, a Unidade de Serviço de Nuvem (USN);

3.2.3.8. Disponibilizar previsões de custo baseado no perfil atual de consumo;

3.2.3.9. Disponibilizar Log de atividades;

3.2.4. Requisitos de Segurança

3.2.4.1. A Solução deverá dispor de medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, à segurança e à integridade, prevenindo acesso não autorizado às informações.

3.2.4.2. É vedada a PARCEIRA ou ao provedor acesso aos dados hospedados na infraestrutura de nuvem privada, sem prévia e formal autorização por parte da DATAPREV.

3.2.4.3. A Solução deverá prover mecanismo de acesso protegido aos dados, por meio de chave de criptografia privada e exclusiva, ou seja, de uso restrito da DATAPREV, garantindo que apenas aplicações e usuários autorizados tenham acesso.

3.2.4.4. A Solução deverá permitir a criptografia automática de dados e objetos armazenados usando AES (Advanced Encryption Standard) de, no mínimo, 256 bits ou outro algoritmo com força de chave equivalente ou superior, neste último caso desde que aprovado pela DATAPREV.

3.2.4.5. A solução deverá possibilitar comunicação criptografada e protegida para transferência de dados.

3.2.4.6. Controle de acesso através da implementação de MFA (*Multi-factor Authentication*);

3.2.4.7. A PARCEIRA deverá estar aderente aos requisitos de segurança especificados na IN GSI/PR 05 de 30 de Agosto de 2021.

3.2.4.8. A solução deverá implementar estratégia para mitigar riscos relacionados a ataques de *ransomwares*;

3.2.4.9. A PARCEIRA deverá criar uma política de atualização de versão de *software*, indicando sua criticidade, informando a DATAPREV sobre o planejamento de atualização.

3.2.4.10. A partir do ponto de entrada/saída da internet nos datacenters da DATAPREV, o provedor ofertado deverá observar as seguintes disposições:

3.2.4.10.1. Inviolabilidade e sigilo do fluxo de suas comunicações pela rede, salvo por ordem judicial, na forma da lei.

3.2.4.10.2. Inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.

3.2.4.11. A solução deve permitir criar Listas de Controle de Acesso (ACLs) para conceder permissões específicas (ou seja, READ, WRITE, FULL_CONTROL) a usuários específicos para um recurso ou para um objeto.

3.2.4.12. Segurança de Chaves: A solução deve permitir criptografar e descriptografar dados e objetos sem perda de performance substantiva.

3.3. Requisitos para instalação de equipamentos em Datacenters da Dataprev

Energia	Tensão de Alimentação: 380 V (Trifásico – 3F+N+T) / 220 V (Monofásico – F+N+T) Corrente do Circuito de Distribuição: 32 A Frequência da Rede: 60 Hz Todos os equipamentos de TI devem possuir fontes de alimentação redundantes, visando aderência aos requisitos de alta disponibilidade da infraestrutura física dos data centers.
Climatização	Especificações Mínimas: Faixa de Operação Recomendada (Class A1 to A4): 18º a 27º C / 40% a 60% RH (umidade); Fluxo de Ar: Front-to-Back (admissão de ar frio pela parte frontal e exaustão de ar quente pela traseira);

	Faixa de Operação Ampliada (Class A2): 10º a 35º C / 20% a 80% RH (umidade); Recursos para envio de informações de temperatura e consumo energético do equipamento. Selo Energy Star – Computer Server Specification ou atestado similar de eficiência energética.
Espaço Físico	Tipo de Rack: Padrão 19", 42U Dimensões Máximas do Rack: 60 cm (largura) x 120 cm (comprimento) Dimensões da Placa de Piso Elevado: 60 cm x 60 cm Máxima Carga Pontual: 545 kg Máxima Carga Distribuída: 1.479 kg/m^2