Termo de Referência da Parceria Comercial

GovCloud Backup como Serviço (GovCloud BaaS)

Solução para Amplo Mercado

Versão 1.7

Histórico de Revisões

Data	Versão	Descrição	Autor
18/03/2022	1.0	Criação do Documento	Fabrício Paiva – mat. 332.828 Rodrigo Almeida – mat. 334.430
19/04/2022	1.1	Revisão após apontamentos da SUAS	Fabrício Paiva – mat. 332.828 Rodrigo Almeida – mat. 334.430
21/04/2022	1.2	Revisão após atualização do Estudo Técnico	Rodrigo Almeida – mat. 334.430
27/04/2022	1.3	Retirado o cronograma; Alterado texto para informando que o *appliance* de Backup será instalado exclusivamente em Datacenter da Dataprev; Alterado informando que a prospecção de novos clientes pode ser realizada pela Dataprev e pelo Potencial Parceiro; Retirado os requisitos e transferido para um anexo.	Fabrício Paiva – mat. 332.828 Rodrigo Almeida – mat. 334.430
12/05/2022	1.4	Adicionado novos itens na seção 4.1. Condições para Participação na Parceria Comercial	Alan Santos - mat. 342.459 Fabrício Paiva – mat. 332.828 Rodrigo Almeida – mat. 334.430
14/06/2022	1.5	Revisão do Documento para remoção de informações sensíveis e atualização do item 4.4	Rodrigo Almeida – mat. 334.430 Enrica Souza – mat. 345.229 Fabrício Paiva – mat. 332.828
25/07/2022	1.6	Ajustes após consulta pública e revisão do DEAP.	Alan Santos - mat. 342.459 Fabrício Paiva – mat. 332.828 Rodrigo Almeida – mat. 334.430
10/08/2022	1.7	Ajustes após consulta pública.	Alan Santos - mat. 342.459 Fabrício Paiva – mat. 332.828 Rodrigo Almeida – mat. 334.430

Sumário

1. Objetivo do Documento

Esta seção descreve o objetivo desse artefato, sendo de conteúdo fixo e não devendo ser alterada. O propósito desse Documento de Termo de Referência de Parceria Comercial é ser uma referência para evolução dos requisitos técnicos e de negócio para construção do objeto da parceria. O documento consolida e torna público o interesse da Dataprev em avançar com a composição de uma solução através de parceria comercial. Esse artefato **NÃO SUBSTITUI** o estudo técnico preliminar nem o modelo de negócio de uma solução, produto ou serviço.

2. Objeto

O objeto deste documento trata do estabelecimento de possível parceria para oferta de solução de Backup como Serviço - GovCloud BaaS. A solução deve contar com recursos de:

- Backup rápido e com ampla cobertura;
- Recuperação imediata;
- Proteção do Backup de Nuvem com recuperação de desastre;
- Segurança com proteção contra *ransware* e ameaças virtuais;
- Automação de backups;
- Disponibilização de *storage*, com backups rápidos e escalabilidade ilimitada;

Além disso, os itens de trabalhos que estarão protegidos pelo backup são:

- máquinas virtuais (VMs);
- cargas de trabalho baseadas em nuvem;
- endpoints;
- outras cargas de trabalho que podem estar armazenadas em sistemas operacionais hospedados em máquinas físicas, em sistemas cliente servidor tradicionais
- dentre outros.

A viabilização da oferta da solução inclui atividades como:

- instalação de software específico para realização das atividades de *backup/restore* em máquinas físicas;
- configuração de rede para acesso ao ambiente GovCloud;
- preparação de ambiente;
- acesso a um portal de autosserviço onde os usuários clientes podem agendar tarefas de backup;
- definir políticas de retenção;
- Capacitação dos times da Dataprev para operacionalização da solução;
- executar recuperações, entre outros.

A solução GovCloud BaaS deve gerenciar o armazenamento, a segurança, obedecer a requisitos de conformidade legal, e executar todas as ações de operacionalização da infraestrutura necessária para viabilizar a oferta da solução.

3. Glossário

Termo	Significado
BaaS	Backup as a Service. Consiste em oferecer um serviço de backup e restauração da informação que permita garantir a continuidade operacional do negócio do cliente sem se preocupar em investir, administrar, dar suporte e monitorar a ferramenta de backup, respeitando as políticas predefinidas.
Ramsonware	Software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo. Na maioria dos casos ocorre da seguinte forma: primeiro o *ramsonware* ganha acesso ao dispositivo. Dependendo do tipo, todo o sistema operacional ou apenas arquivos individuais são criptografados. Um resgate é, então, exigido das vítimas em questão.

TB	*Terabyte*. 1 TB de armazenamento equivale a 1.000 GB de dados.
Pay as You Go	Pagamento sob consumo
Multi tenant (múltiplos inquilinos)	É um estilo de arquitetura onde você tem uma aplicação centralizada que atende a vários clientes. Neste caso, partindo do Inglês tenant significa locatários ou inquilinos. É um termo utilizado em SaaS onde, na maioria das vezes, os tenants são clientes corporativos.
HDD (Hard Disk Drive)	Disco rígido popularmente chamado também de HD (derivação de HDD do inglês hard disk drive) é a parte do computador onde são armazenados os dados. Utiliza peças mecânicas para ler e gravar dados, já que encontrar e extrair dados por meio físico leva mais tempo do que fazer esse processo por SSD. A vantagem é ser mais barato que o SSD.
SSD (Solid State Drive)	A unidade em estado sólido é um componente de hardware para armazenamento muito mais rápido que o HDD. O SSD não possui discos físicos ou agulhas magnéticas. São mais caros que os HDD, sendo mais rápidos e ocupam menos espaço.
QoS	O QoS (Quality of Service ou Qualidade de Serviço) trata-se de um conjunto de tecnologias funcionando em uma rede para assegurar sua capacidade de executar tráfego de alta prioridade e aplicativos de forma totalmente confiável com capacidade de rede limitada. As tecnologias de QoS são capazes de fazer isso fornecendo uma diferenciada manipulação e alocação de capacidade para os fluxos específicos no tráfego de rede. Assim, isso possibilita que o administrador da rede possa atribuir a ordem em que os pacotes vão ser manipulados e a quantidade de largura de banda disponibilizada a esse fluxo de tráfego ou aplicativo.
LDAP	Lightweight Directory Access Protocol (Protocolo de acesso aos diretórios leves) é um protocolo de rede que roda sobre o TCP/IP que permite organizar os recursos de rede de forma hierárquica, como uma árvore de diretório, onde temos primeiramente o diretório raiz, em seguida a rede da empresa, o departamento e por fim o computador do funcionário e os recursos de rede (arquivos, impressoras, etc.) compartilhados por ele. A árvore de diretório pode ser criada de acordo com a necessidade. Uma das principais vantagens do LDAP é a facilidade em localizar informações e arquivos disponibilizados.

Failover	É o termo utilizado para indicar a tolerância a falhas. Na prática, significa que existem recursos tecnológicos em redundância para evitar a indisponibilidade de um determinado componente. Há sistemas que precisam de alta disponibilidade, isto é, não podem deixar de funcionar ou devem ter o mínimo de parada possível. Nesse cenário, é preciso haver recursos em duplicidade para assumir a posição do componente primário se ocorrer alguma falha ou caso seja preciso realizar a manutenção no ambiente.
On Premise	Um servidor on-premise é aquele em que a própria empresa tem a responsabilidade de processar suas aplicações de hardware e software. Em outras palavras, toda a infraestrutura, customização, configuração e atualização é feita internamente. Por ser um servidor interno, a empresa precisa ter um espaço físico adequado, já que é necessário cuidar da segurança e da operação dos equipamentos.
MFA	Multi-Factor Authentication (Autenticação Multi Fator) é o uso de dois ou mais fatores ou agentes para verificação quanto a autenticidade de algo.

4. Características da Parceria

4.1 Condições para Participação na Parceria Comercial

O potencial parceiro deve obrigatoriamente obedecer às seguintes condições:

4.1.1. Não estar impedido de licitar e contratar com a Administração Pública.

4.1.2. Não estar enquadrado nas vedações previstas no art. 9º da Lei n.º 8.666/93.

4.1.3. Deve possuir estatuto ou contrato social pertinente e compatível com o objeto.

4.1.4. Não estar em processo de dissolução, recuperação judicial, recuperação extrajudicial, falência, concordata, fusão, cisão ou incorporação.

4.1.5. Que não seja sociedade estrangeira não autorizada a funcionar no País.

4.1.6. Que não seja cooperativa de mão de obra conforme o art. 5º da Lei 12.690/2012.

Deve-se observar as condições abaixo:

4.1.7. Possuir cadastro no SICAF (Sistema de Cadastro de Fornecedores, https://www3.comprasnet.gov.br/sicaf-web/index.jsf);

4.1.8. Que não seja cooperativa Não possuir nenhum tipo de sanção vigente nos seguintes sistemas:

4.1.8.1. CEIS (Cadastro de Empresas Inidôneas e Suspensas, mantido pela Controladoria-Geral da União - CGU (https://www.portaltransparencia.gov.br/sancoes/ceis).

4.1.8.2. Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça - CNJ (http://www.cnj.jus.br/improbidade_adm/consultar_requerido.php);

4.1.8.3. Cadastro Nacional de Empresas Punidas - CNEP, mantido pela Controladoria - Geral da União – CGU (https://www.portaltransparencia.gov.br/sancoes/cnep);

4.1.8.4. Lista de Inabilitados e Inidôneos, mantida pelo Tribunal de Contas da União - TCU (https://contas.tcu.gov.br/pls/apex/f?p=2046:5);

4.1.9. Não poderá participar desta parceria todo aquele que se enquadrar art. 38 da Lei nº 13.303/2016 e no art. 21 do Regulamento de Licitações e Contratos da DATAPREV (https://portal3.dataprev.gov.br/sites/default/files/arquivos/regulamento_licitacoes_e_contratos_dataprev_ca_vf_08032018.pdf).

4.1.10. Possuir Declaração de Elaboração Independente de Proposta;

4.1.11. Possuir Declaração da proponente de que não possui, em seu quadro de pessoal, empregados menores de 18 (dezoito) anos em trabalho noturno, perigosos ou insalubres e menores de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz a partir de 14 (quatorze) anos, nos termos do Art. 7º, Inc. XXXIII, da Constituição Federal;

4.1.12. É vedado que familiar de agente público da DATAPREV, ocupante de cargo de direção, chefia ou assessoramento, preste serviço nesta Empresa Pública Federal, observados os ditames e as exceções previstas no Decreto nº 7.203/2010;

4.1.13. Dar conhecimento do Código de Ética da DATAPREV aos empregados da CONTRATADA que exerçam suas atividades nas dependências desta Empresa Pública Federal, a fim de garantir a fiel observância das regras e orientações contidas no referido código.

4.2 Das características da composição da Parceria Comercial

As características da Composição da Parceria Comercial encontram-se no Anexo I.

4.3 Requisitos para Estabelecimento da Parceria

Os requisitos funcionais e não funcionais para estabelecimento desta parceria encontra-se no Anexo I.

4.4 Do processo de revisão dos requisitos de composição do Objeto da Parceria Comercial

Concluída a etapa de consulta pública para refinamento dos requisitos da oferta da solução GovCloud BaaS, o time responsável pela proposição da solução deverá reavaliar os requisitos e atualizá-los de forma consistente com os insumos recebidos pelas empresas participantes da Consulta Pública. Para isso, as seguintes questões devem ser esclarecidas em tempo de consulta pública:

4.4.1. Na visão da empresa participante, o escopo da solução apresentada pela Dataprev é suficiente para a composição do objeto da parceria?

4.4.2. Na visão da empresa participante, os requisitos necessários para composição da parceria comercial são viáveis?

4.4.3. Na visão da empresa participante, quais são os principais riscos negativos para composição do produto objeto da parceria? Há estratégias para minimizar a

probabilidade de ocorrência desses riscos?

4.4.4. Na visão da empresa participante, quais são as principais oportunidades relacionadas à composição do produto objeto da parceria? Há estratégias para maximizar a probabilidade de ocorrência dessas oportunidades?

Caso o participante da consulta pública tenha interesse em realização da composição de parceria comercial atendendo o escopo deste termo de referência, deve responder aos seguintes questionamentos e enviar as informações para a Dataprev:

4.4.5. A empresa cumpre todos os requisitos dos itens 4.1, 4.2 e 4.3 do presente Termo de Referência? Responder Sim ou Não.

4.4.6. A empresa tem interesse na realização da parceria comercial juntamente à Dataprev, nas condições indicadas, ou seja, mediante a prestação de serviço, alocação de infraestrutura e cumprimento dos requisitos funcionais sem remuneração por parte da Dataprev, vinculando o retorno do investimento à receita decorrente de futura prestação do serviço de acordo com o interesse do mercado? Responder Sim ou Não.

4.4.7. A empresa possui um caso de prestação de serviços indicados compatíveis com os requisitos técnicos apresentados no Brasil ou no Exterior? Responder Sim ou Não. Se sim, indicar o caso, com contato para diligência por parte da Dataprev.

4.4.8. A empresa aceita realizar uma Prova de Conceito, que será validada e homologada pelas equipes técnicas da Dataprev, onde apresentará a forma de operacionalização dos requisitos técnicos imediatamente após a resposta do presente questionário e proposta de cronograma com os principais marcos para realização da POC? Responder Sim ou Não.

4.4.9. A empresa concorda em fornecer as informações necessárias para que a Dataprev

possa realizar estimativa de composição de custos e preço final da solução.

4.5 Demais Condições

Não consta.

5. Anexos

ANEXO I – Especificação Técnica

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 a DATAPREV e a PARCEIRA através do atendimento dos requisitos listados nos próximos tópicos e seções do presente documento;

1.2. O equipamento deve ser novo, sem uso anterior e que forme uma solução única, integrando inclusive os sites da Dataprev.

1.3. Os dados de cada cliente da Dataprev deverão ser mantidos de modo que permita ser isolados completamente, ou seja, controladoras, arranjo de discos, performance, não sendo aceitos apenas isolamento lógico.

1.4. A solução deverá permitir a criação de novos *tenants* sob medida para cada cliente da solução Dataprev, tanto no requisito de performance, quanto em espaço utilizado;

1.5. A solução deverá ser gradualmente escalável e é desejável que alcance volumes na ordem de petabytes por inquilino;

1.6. No requisito disponibilidade, o sistema de hardware não deverá possuir nenhum ponto de falha (totalmente redundante) e o dado deve estar armazenado no mínimo em 2 equipamentos com SLA garantido em no mínimo 98%,

1.7. A solução deverá suportar criptografia com chave própria de cada cliente da Dataprev, garantindo o sigilo completo da informação e cumprimento de melhores práticas estabelecidos pela Lei Geral de Proteção de Dados (LGPD),

1.8. A Dataprev e o Cliente poderão estabelecer quaisquer políticas de backup, portanto, o equipamento deverá estar apto a fornecer quaisquer tipos de performance exigidos para curta ou longa retenção de dados de acordo com cada cliente;

1.9. Clientes Dataprev poderão optar por políticas de Backup em diversos locais (regiões de disponibilidade), portanto, a solução entregue deve atender todos os critérios na formação de uma Edge Cloud Backup, não sendo aceitas soluções de cloud públicas ou data centers externos para composição.

1.10. Por se tratar de uma solução que envolve computação, network, armazenamento em formato Edge, fica entendido que a solução deve apresentar todas as características mínimas de serviço cloud embarcada, incluindo disponibilidade, acesso compartimentado, segurança, auditoria, instalações, serviços de mantenimento da infraestrutura.

1.11. Não deverá ocorrer interrupção de serviços em caso de substituição de parte ou peças, obsolescência, atualizações, incluindo atualização de firmware.

1.12. 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;

1.13. Qualquer documentação gerada também estará coberta pela garantia, assim, a DATAPREV poderá solicitar, sem ônus adicional, correção ou refazimento dos documentos que não estiverem de acordo com os padrões definidos ou que não corresponderem, na prática, aos procedimentos adotados;

1.14. 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;

1.15. 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.

1.16. 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.

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

1.18. A DATAPREV deverá indicar quais dos seus Data Centers possuem os requisitos necessários para implantação de equipamento fornecida pela PARCEIRA, que viabilizará a oferta da solução;

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

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

1.21. 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;

1.22. 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;

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

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

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

1.23.3. 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;

1.24. 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;

1.25. É recomendável que os relatórios/dashboards fornecidos pela parceria sejam customizáveis podendo ser adicionados gráficos, tabelas e o período de avaliação de cada relatório.

1.26. 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;

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

1.28. 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;

1.29. 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:

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

1.29.2. 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;

1.29.3. 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;

1.29.4. 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.

1.30. 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;

1.31. 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, do *software e* todas as ações necessárias para garantir que a solução estará de acordo com as características descritas na seção 2 do presente documento (ver seção 2 do presente documento).

1.32. 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);

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

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

1.33.2. Expansão física dos equipamentos quando necessária;

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

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

1.33.5. 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;

1.33.6. Adicionar componentes relacionados à novas tecnologias quando necessário;

1.33.7. Realizar a migração dos equipamentos físicos quando necessário;

1.33.8. Atualização de *firmware* quando necessário;

1.33.9. Manutenção evolutiva e corretiva do *software* da solução, o que pode envolver atualizações deste.

1.34. 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;

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

1.36. 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.

1.37. Sempre que necessário, a DATAPREV poderá solicitar que a PARCEIRA repasse todo o conhecimento sobre qualquer serviço realizado;

1.38. É desejável que a potencial parceira tenha experiência comprovada com o setor público.

1.39. Todos os requisitos da PARCERIA devem ser entregues licenciados e palavras como deve, permite, suporta, efetua, proporciona, possui, etc. significam que a funcionalidade deve ser entregue operacional, sem ônus adicional à Dataprev.

1.40. Fica estabelecido que os casos omissos serão resolvidos entre as partes, respeitados o objeto da presente parceria, a legislação e demais normas reguladoras da matéria.

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 possuir portal de gerenciamento centralizado para todas as instâncias de armazenamento instaladas nos data centers Dataprev e de seus clientes;

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

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

2.5. Deve permitir a execução de rotinas de backup possuindo mecanismos de reserva de banda para as rotinas de backup;

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

2.7. 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 da Dataprev;

2.8. 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*);

2.9. Manter 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*";

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

2.11. Deve possuir um Portal de gestão para os itens que compõe a solução (exemplo: discos, segurança, rede, performance, backup, docker);

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

2.13. Deve possui capacidade de integração com a solução através do consumo via API;

2.14. As APIs devem possuir documentação que permitam, de forma fácil, o correto consumo;

2.15. 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 à PARCEIRA, 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;

3.2. 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, alta disponibilidade, escalabilidade e desempenho. A solução deverá atender os seguintes requisitos:

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

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

3.2.1.1.3. 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;

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

3.2.1.1.5. 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;

3.2.1.2. Permita a replicação de dados localmente e remotamente;

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

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

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

3.2.1.6. Implemente criptografia dos dados salvos;

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

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

3.2.1.9. 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;

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

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

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

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

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

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

3.2.1.16. 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 múltiplos acessos 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, Maria, Mongo, Redis, entre outros, 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 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;

3.2.2.10. 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);

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

3.2.2.12. 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:

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

3.2.2.12.2. Gerenciamento de política de *backup* centralizada;

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

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

3.2.2.12.5. 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;

3.2.2.12.6. Análise de capacidade (com histórico) e carga de utilização do equipamento;

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

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

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

3.2.2.14. 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;

3.2.2.15. 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;

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

3.2.2.17. 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;

3.2.2.18. Fornecer funcionalidade para:

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

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

3.2.2.18.3. 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

A 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:

3.2.3.1. A ferramenta deve prover gerenciamento de custos;

3.2.3.2. 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;*

3.2.3.3. Implemente Políticas de monitoramento de alertas;

3.2.3.4. Possibilitar a previsão de custos e a visualização de recursos consumidos (ex. utilização de volume);

3.2.3.5. Permitir políticas de alertas de utilização de volume;

3.2.3.6. Desejável a disponibilização de relatório de faturamento apresentando 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);

3.2.3.7. Desejável a disponibilização de previsões de custo baseado no perfil atual de consumo;

3.2.3.8. Disponibilizar Log de atividades.

3.2.3.9. Os seguintes requisitos foram sugeridos em tempo de consulta pública e são desejáveis para a oferta da solução:

3.2.3.9.1. A proteção de dados e replicação de máquinas virtuais deverá ser compatível e integrado com ambientes Microsoft, incluindo Hyper-V e System Center versões 2012 e superiores, e ambientes VMware, incluindo vSphere 6.0 e superiores e vCloud Director 10.1 e superiores.

3.2.3.9.2. Deverá permitir a proteção de máquinas virtuais com Windows Server 2012 e superiores, Red Hat Enterprise Linux 6 e superiores e Ubuntu 18.04 e superiores, além de suportar a recuperação granular dos dados

armazenados nos sistemas de arquivo do tipo ext3/4, XFS, btrfs, FAT32, NTFS e ReFS.

3.2.3.9.3. Deverá possuir funcionalidade de recuperação instantânea das máquinas virtuais protegidas, no ambiente de origem (Baas) lado do cliente permitindo reduzir o tempo necessário à recuperação das máquinas, permitindo seu acesso diretamente dos arquivos de backup, provendo recursos que permitam a migração para a produção sem indisponibilidade ou perda de dados.

3.2.3.9.4. Deverá suportar técnicas de backup que permitam otimizar as janelas de backup e o consumo, incluindo suporte à backups sintéticos e incrementais eternos, onde apenas os novos dados sejam trafegados e armazenados, bem como armazenados de forma desduplicada e comprimida.

3.2.3.9.5. Deverá possuir recursos que limitem o impacto das operações de backup nos discos de produção, permitindo definir throttling nas operações de backup quando determinada latência for atingida, garantindo que as aplicações críticas não serão impactadas durante o backup.

3.2.3.9.6. Deverá suportar o backup consistente e a recuperação granular de aplicações críticas, incluindo bases de dados Microsoft SQL Server 2012 e superiores e Oracle 12c e superiores, ambientes de correio eletrônico Microsoft Exchange 2013 e superiores, e controladores de domínio Active Directory, sem a necessidade de agentes.

3.2.3.9.6.1. Deverá suportar recuperar objetos individuais do Exchange, incluindo anexos, compromissos, contatos e mensagens;

3.2.3.9.6.2. Deverá suportar recuperar objetos individuais do Active Directory, incluindo usuários, objetos de política de grupo (GPO), grupos, contas, computadores, registros de DNS;

3.2.3.9.6.3. Deverá suportar recuperar objetos individuais do SQL Server, incluindo bases de dados, tabelas e registros;

3.2.3.9.6.4. Deverá suportar recuperar objetos individuais do Oracle, incluindo bases de dados;

3.2.3.9.7. Deverá suportar a recuperação rápida de um dado armazenado no backup, mesmo com a corrupção do catálogo do backup ou desduplicação, sem necessitar recatalogar todas as imagens, ou correr o risco de não recuperar uma informação se não possuir uma cópia do catálogo.

3.2.3.9.8. Deverá possuir recursos de validação automatizada das máquinas virtuais protegidas, no ambiente de origem (Baas) lado do cliente suportando criar ambiente de validação que simulem a produção, capaz de inicializar simultaneamente múltiplas máquinas protegidas, permitindo executar testes para validar a integridade das aplicações e geração de relatório sobre os testes.

3.2.3.9.9. Deverá possuir recuperação integrada com antivírus, no ambiente de origem (Baas) lado do cliente permitindo que um software de antivírus verifique os dados antes de sua recuperação.

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

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

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

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

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

3.2.4.10. 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.

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

3.2.4.12. Todas as ações presenciais devem atender a Política de Segurança da Dataprev.

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