

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

**ANEXO B – ESPECIFICAÇÕES MÍNIMAS PARA HOMOLOGAÇÃO DE
PROVEDOR DE NUVEM PÚBLICA**

1. Requisitos Gerais

- 1.1.1. Todos os provedores de nuvem ofertados na Solução deverão disponibilizar calculadora pública de preços para os produtos e serviços, acessível através de sítio oficial e público na internet.
- 1.1.2. O provedor de nuvem deverá disponibilizar os recursos de IaaS - Infraestrutura como Serviço, de PaaS – Plataforma como Serviço e SaaS
- 1.1.3. Todos os Provedores de nuvem ofertados deverão possuir política de Acordo de Níveis de Serviço (ANS) publicado em sítio oficial e público na internet.
- 1.1.4. Pelo menos um dos Provedores de Serviço de Nuvem que irão compor a Solução deverá possuir, três Zonas de Alta Disponibilidade no território brasileiro. no mínimo, 2 (duas) zonas de disponibilidade ou data centers instalados e localizados em território nacional.
- 1.1.5. A Contratada deverá possuir autorização formal do Provedor para comercializar e/ou intermediar junto ao governo os serviços de nuvem a serem intermediados.
- 1.1.6. Deverá ser fornecido, no nome da Contratante, suporte de nível empresarial (*Enterprise Support*) para a nuvem pública do Provedor a ser homologado.
- 1.1.7. Os provedores de serviços de nuvem ofertados deverão atender minimamente aos seguintes requisitos:
- 1.1.8. Possuir as certificações:
 - I - ISO 27017;
 - II - ISO 27018;
 - III - ISO 27001;

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

IV - CSA STAR Certification nível dois ou superior;

V - SOC 2 ou superior.

As certificações devem ter validade vigente na data de assinatura do contrato, referentes à infraestrutura de datacenter e/ou zonas de Disponibilidade no Brasil.

- 1.1.9. Os datacenters onde os serviços serão hospedados deverão possuir a certificação TIA 942 TIER III ou, alternativamente, comprovar atender ao conjunto de requisitos dessa certificação.
- 1.1.10. Os provedores devem possuir ambiente do serviço em conformidade com a norma ABNT NBR ISO/IEC 27001:2013, sem prejuízo de outras exigências, objetivando mitigar riscos relativos à segurança da informação;
- 1.1.11. Os provedores de nuvem podem emitir declarações de que utilizam datacenters que atendem aos requisitos da certificação. Na impossibilidade da obtenção da declaração do provedor, o encargo da declaração passará a ser do broker. Será meio de comprovação, referência à publicação no site do provedor, ou portais oficiais, da informação requerida;
- 1.1.12. Devem garantir disponibilidade de serviços de pelo menos 99,9% ao ano, com tempo de inatividade planejado para manutenção programada;
- 1.1.13. Devem garantir a segurança dos dados tanto em repouso quanto em trânsito;
- 1.1.14. Os serviços prestados pelo provedor devem oferecer todas as garantias da legislação brasileira relacionadas a guarda das informações armazenadas em nuvem.
- 1.1.15. Os provedores de nuvens selecionados devem oferecer serviços de escalonamento automático (*autoscaling*), permitindo que soluções tenham acesso automático a maior quantidade de recursos computacionais, em função da demanda ou critério definido.
- 1.1.16. Os provedores de nuvens selecionados devem oferecer funcionalidade de marketplace, com oferta de softwares do mercado e não apenas do próprio provedor.

Anexo B – Especificações Mínimas para Homologação de Provedor de Nuvem Pública

- 1.1.17. Os provedores deverão possuir programa de certificação para arquitetos de solução do próprio provedor. Esse requisito visa permitir que a prestação de serviços seja orientada por padrões técnicos de domínio público e por melhores práticas passíveis de serem avaliados pela equipe técnica do contratante

2. Requisitos Específicos

2.1 Os provedores deverão atender a pelo menos 70% dos requisitos abaixo listados.

2.1.1 As nuvens públicas a serem ofertadas deverão possuir, no mínimo, os seguintes serviços computacionais (rol não exaustivo):

- a) Computação em nuvem - máquinas virtuais
- b) Armazenamento
- c) Backup de Armazenamento
- d) Banco de Dados
- e) Plataforma de Dados e Log Analytics
- f) Análise de Imagens e OCR
- g) Serviços de RAG
- h) Serviços de LLM
- i) Serviços de Machine Learning
- j) Geolocalização
- k) Conectividade e Segurança
- l) Antivirus /DDoS por IP
- m) Transferência de Dados
- n) Conectividade Dedicada

2.1. Computação

- 2.2.1 Permitir o provisionamento de instâncias com vCPU, RAM e disco configuráveis, possibilitando customizar recursos de acordo com as necessidades específicas de processamento;
- 2.2.2 Suportar instâncias nos modos on-demand, reserved e spot, proporcionando flexibilidade e otimização de custos conforme a demanda;

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

- 2.2.3 Possuir recursos para auto escalonamento horizontal e vertical, permitindo ajuste da capacidade automaticamente diante de variações de carga, caso necessário;
- 2.2.4 Permitir a criação e gerenciamento de imagens customizadas, facilitando a padronização e rápida replicação de ambientes;
- 2.2.5 Suportar snapshots e backups programados, garantindo segurança e recuperação de dados em caso de falhas;
- 2.2.6 Possibilitar monitoramento em tempo real dos recursos (CPU, RAM, disco, rede), auxiliando no acompanhamento de desempenho e na tomada de decisões proativas;
- 2.2.7 Suportar compatibilidade com diversos sistemas operacionais disponíveis (Linux, Windows, Ubuntu Server, CentOS, Red Hat Enterprise, Suse, Oracle, etc);
- 2.2.8 Os sistemas operacionais devem estar devidamente licenciados e aptos para o uso de todos os recursos da VM, salvo quando o BNB optar por usar seu próprio licenciamento.
- 2.2.9 Permitir integração com ferramentas de infraestrutura como código, promovendo automação e repetibilidade das operações de TI;
- 2.2.10 Possuir mecanismos de clusterização de VMs para alta disponibilidade, assegurando continuidade de serviço mesmo diante de falhas em componentes individuais;
- 2.2.11 Suportar instâncias equipadas com GPU, otimizando o processamento para aplicações intensivas como IA e renderização gráfica;
- 2.2.12 Permitir provisionamento em múltiplas zonas de disponibilidade, elevando a resiliência contra indisponibilidades regionais;
- 2.2.13 Possibilitar uso de firewall individual por VM com regras customizáveis, reforçando a proteção de cada máquina virtual;
- 2.2.14 Permitir gerenciamento via API RESTful, integrando facilmente com sistemas e fluxos automatizados externos;

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

- 2.2.15 Possuir recursos para migração online de instâncias entre zonas, promovendo flexibilidade operacional sem impacto significativo;

2.2. Armazenamento

- 2.2.1. Disponibilizar volumes SSD para aplicações que demandam alta performance;
- 2.2.2. Oferecer volumes HDD para cargas de trabalho frias e de menor demanda.
- 2.3.2.1 Suportar storage de objetos
- 2.3.2.2 Suportar storage de objetos compatível, no mínimo, com Azure Blob Storage; Google Cloud Storage (GCS) e IBM Cloud Object Storage, promovendo interoperabilidade;
- 2.3.2.3 Deve ser durável, escalável e seguro;
- 2.3.2.4 Deverá possuir recurso de versionamento ou de snapshot;
- 2.3.2.5 Deve possuir API para upload de arquivos via aplicações desenvolvidas, a critério do Banco;
- 2.2.3. Permitir Implementar versionamento automático de objetos e arquivos.
- 2.2.4. Suportar replicação de dados entre regiões (cross-region replication);
- 2.2.5. Garantir criptografia AES-256, mínima, dos dados em repouso;
 - 2.2.5.1. Permitir função de criptografia do volume com mudança da chave gerenciada pelo BANCO;
- 2.2.6. Permitir controlar acessos por políticas IAM ou equivalentes.
- 2.2.7. Disponibilizar acesso por CLI, SDK e API REST.
- 2.2.8. Registrar todos os acessos e modificações em logs detalhados.

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

- 2.2.9. Permitir automatizar o ciclo de vida dos objetos (ILM).
- 2.2.10. Permitir configuração de buckets públicos ou privados conforme necessidade.
- 2.2.11. Suportar upload multipart para objetos grandes;
- 2.2.12. Possibilitar que o volume criado seja anexado às máquinas virtuais e reconhecidos pelos SO's;

2.3. Backup de Armazenamento

- 2.3.1. Permitir automatizar backups com agendamento flexível;
- 2.3.2. Permitir retenção configurável de backups por tipo de dado ou unidade;
- 2.3.3. Assegurar criptografia dos backups em trânsito e em repouso;
- 2.3.4. Suportar snapshots incrementais para economia de espaço;
- 2.3.5. Permitir definir políticas de backup específicas por serviço ou aplicação.
- 2.3.6. Oferecer restauração granular até o nível de versão de arquivo;
- 2.3.7. Isolar ambientes de backup para maior segurança.
- 2.3.8. Monitorar e alertar sobre falhas de backup em tempo real.
- 2.3.9. Validar automaticamente a integridade dos backups realizados.
- 2.3.10. Permitir backup entre diferentes regiões geográficas.
- 2.3.11. Suportar backup de bancos de dados, VMs e volumes.
- 2.3.12. Implementar backups imutáveis (WORM).
- 2.3.13. Exportar backups para fita ou storage de objetos quando necessário.
- 2.3.14. Integrar com soluções de Disaster Recovery (DR).
- 2.3.15. Disponibilizar logs de execução dos backups para auditoria.

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

2.4. Banco de Dados

- 2.5.1 Os serviços de banco de dados devem fornecer plataformas de banco de dados escaláveis, com dimensionamento dinâmico, automação, provisionamento, configuração, atualização e backup;
- 2.5.2 Suportar bancos gerenciados como PostgreSQL, MySQL, SQL Server e Oracle, etc. atendendo diferentes demandas de aplicação.
- 2.5.3 Permitir a criação de instancias de banco de dados;
- 2.5.4 Possuir opção de backup automático com retenção configurável, permitindo restaurar o banco em pontos específicos do tempo.
- 2.5.5 Permitir recuperação point-in-time, possibilitando o retorno a estados anteriores em caso de problemas.
- 2.5.6 Suportar criptografia tanto em repouso quanto em trânsito, assegurando confidencialidade dos dados;
- 2.5.7 Possuir escalabilidade vertical e horizontal com read replicas, aumentando performance e disponibilidade.
- 2.5.8 Permitir alta disponibilidade e failover automático, reduzindo o impacto de falhas.
- 2.5.9 Suportar atualizações automatizadas com janelas de manutenção programáveis;
- 2.5.10 Possuir monitoramento detalhado de queries e índices, identificando gargalos e oportunidades de otimização.
- 2.5.11 Permitir gerenciamento via CLI, interface web e API, oferecendo múltiplas formas de administração.
- 2.5.12 Suportar conectividade com o CONTRATANTE e controle de firewall, restringindo acessos e reforçando segurança;
- 2.5.13 Possuir logs de auditoria e consultas habilitáveis, permitindo rastrear ações e identificar acessos suspeitos;
- 2.5.14 Permitir tuning automático de performance;
- 2.5.15 Suportar gerenciamento de usuários e roles, facilitando o controle de permissões e seguranças;

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

- 2.5.16 Permitir integração com CI/CD para migrações, acelerando e modernizando o ciclo de vida do banco de dados.
- 2.5.17 Suportar modelos chave-valor, documento e coluna larga, permitindo armazenar diferentes formatos de dados conforme a aplicação.
- 2.5.18 Possuir opções gerenciadas a exemplo do MongoDB, DynamoDB, Cassandra e Couchbase, abrangendo diversas necessidades de banco de dados NoSQL.
- 2.5.19 Permitir escalabilidade horizontal automática, para acompanhar picos de demanda sem intervenção manual;
- 2.5.20 Suportar backups automáticos e restauração sob demanda, protegendo dados contra perdas.
- 2.5.21 Possuir suporte a índices secundários e primários, possibilitando consultas rápidas e eficientes.
- 2.5.22 Permitir configuração de leituras e gravações consistentes, ajustando a precisão dos dados conforme a necessidade.
- 2.5.23 Suportar criptografia nativa dos dados, aumentando a proteção das informações armazenadas.
- 2.5.24 Possuir integração com redes privadas, reduzindo risco de exposição indevida dos bancos de dados.
- 2.5.25 Permitir monitoramento em tempo real de throughput e latência, monitorando proativamente o desempenho.
- 2.5.26 Suportar interface de consulta com filtros complexos, facilitando buscas avançadas.
- 2.5.27 Possuir alta disponibilidade em múltiplas zonas, garantindo resiliência e continuidade.
- 2.5.28 Permitir failover automático, transferindo operações para réplicas em caso de falha;
- 2.5.29 Suportar APIs REST e SDKs para integração, ampliando as maneiras de interagir com o serviço.
- 2.5.30 Possuir controle de acesso granular (IAM/RBAC), detalhando permissões por usuário ou função.

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

2.5.31 Permitir replicação cross-region, melhorando a disponibilidade global dos dados.

2.5. Plataforma de Dados e Log Analytics

2.6.1 Deve permitir a centralização e classificação automática dos dados, facilitando seu gerenciamento;

2.6.2 Deve implementar conectores diversos, controle de linhagem, versionamento e auditoria para rastreamento eficiente;

2.6.3 Possuir governança e ingestão (tempo real/batch), anonimização e suporte ao modelo data lakehouse;

2.6.4 Deve oferecer busca semântica, APIs de exploração e painéis interativos para análise avançada;

2.6.5 Integrar com ferramentas de BI, fornecer notificações e possibilitar o tagging por domínio/confidencialidade

2.6. Containers

2.7.1 Possuir clusters de containers com escalonamento automático, para ajustar rapidamente a infraestrutura à carga de trabalho;

2.7.2 Permitir rede overlay com DNS interno, facilitando comunicação eficiente entre serviços em diferentes hosts;

2.7.3 Suportar persistência de dados via volumes, garantindo armazenamento confiável para os containers;

2.7.4 Possuir logs centralizados para cada container, permitindo rastreamento e análise eficazes de eventos e erros;

2.7.5 Permitir deploy por pipelines CI/CD integrados, acelerando a entrega de novas versões de aplicações;

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

- 2.7.6 Suportar mecanismos de autoheal para pods e nodes, mantendo o ambiente saudável diante de falhas;
- 2.7.7 Possuir funcionalidade de rolling update, viabilizando atualizações contínuas sem downtime.
- 2.7.8 Permitir integração com registries privados, protegendo e controlando o acesso às imagens de containers;
- 2.7.9 Suportar controle de acesso RBAC, reforçando a governança e a segurança de permissões dentro do cluster;
- 2.7.10 Possuir suporte a namespaces multi-tenant, segregando ambientes de diferentes equipes ou projetos;
- 2.7.11 Permitir balanceamento de carga L7 nativo, distribuindo requisições de forma inteligente entre os serviços;
- 2.7.12 Suportar service mesh integrado de forma opcional, agregando funcionalidades avançadas de rede, como observabilidade e controle de tráfego;
- 2.7.13 Possuir painel web e CLI para gerenciamento, oferecendo interfaces práticas para administração dos clusters;
- 2.7.14 Permitir configuração de quota por namespace, limitando recursos e evitando competição desleal entre workloads.

2.7. Análise de Imagens e OCR (Optical Character Recognition)

- 2.8.1 Extrair texto de imagens por meio de OCR avançado;
- 2.8.2 Reconhecer rostos em imagens conforme padrões de privacidade;
- 2.8.3 Detectar objetos em fotos ou vídeo;
- 2.8.4 Realizar segmentação de imagens para análise detalhada;
- 2.8.5 Classificar imagens por conteúdo automaticamente;
- 2.8.6 Suportar múltiplos formatos de imagem (JPEG, PNG, etc.);
- 2.8.7 Processar imagens em lote ou streaming;
- 2.8.8 Analisar manuscritos e imagens não digitalizadas;

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

- 2.8.9 Identificar e extrair dados de documentos digitalizados;
- 2.8.10 Utilizar modelos pré-treinados e customizáveis conforme demanda;
- 2.8.11 Retornar resultados em formato estruturado (JSON);
- 2.8.12 Integrar com sistemas via API;
- 2.8.13 Assegurar armazenamento temporário seguro das imagens analisadas;
- 2.8.14 Permitir registrar todas as requisições processadas para fins de auditoria;

2.8. Serviço de RAG (Retrieval-Augmented Generation)

- 2.9.1 Realizar indexação eficiente de bases textuais;
- 2.9.2 Recuperar documentos de forma semântica utilizando técnicas modernas de NLP;
- 2.9.3 Utilizar *embeddings* vetoriais para busca contextualizada;
- 2.9.4 Possibilitar configuração do pipeline de processamento (chunking, ingestão);
- 2.9.5 Integrar geração de respostas automáticas com grandes modelos de linguagem (LLM);
- 2.9.6 Rankear contexto por similaridade, priorizando relevância na resposta;
- 2.9.7 Implementar cache de resultados para acelerar consultas frequentes;
- 2.9.8 Referenciar o documento de origem nas respostas fornecidas;
- 2.9.9 Suportar múltiplos formatos de documentos: PDF, HTML, DOCX, etc;
- 2.9.10 Permitir registrar logs de contexto recuperado para todas as requisições;
- 2.9.11 Permitir customização do prompt de consulta;
- 2.9.12 Controlar parâmetros como temperatura e top-k das respostas;
- 2.9.13 Possibilitar deploy em redes privadas;
- 2.9.14 Disponibilizar auditoria completa das respostas geradas;

2.9. Serviço LLM (Large Language Model)

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

- 2.10.1 Deverá disponibilizar modelos LLM e de *embeddings* com cobrança baseada em blocos de 1K a 1M tokens, contemplando modalidades de entrada (*input*), saída (*output*) e *cached input*, conforme aplicável a cada modelo;
- 2.10.2 Os modelos deverão estar disponíveis para execução em escopos regionais e globais, permitindo que o contratante escolha o modo mais adequado para latência, custo e compliance, sem necessidade de reimplementação de código;
- 2.10.3 Os modelos LLM multimodais deverão processar texto, imagem e áudio, garantindo latência máxima de 1,5s e uptime mínimo de 99,9%;
- 2.10.4 O serviço deverá disponibilizar modelos de *embeddings* capazes de gerar vetores de alta dimensionalidade, com tempo máximo de resposta de 300ms por requisição e suporte a execução regional/global;
- 2.10.5 Os modelos deverão suportar janela de contexto mínima de 128.000 tokens;
- 2.10.6 Os modelos deverão ser disponibilizados via API segura (HTTPS/TLS 1.2 ou superior), com autenticação por chave ou OAuth2, e atender, no mínimo, às normas LGPD, ISO/IEC 27001, 27017 e 27018, incluindo registro detalhado de uso por modelo, data e tipo de token;
- 2.10. Serviço Machine Learning
- 2.11.1 Oferecer ambiente gerenciado para notebooks colaborativos;
- 2.11.2 Suporte nativo a frameworks como TensorFlow, PyTorch e Scikit-learn;
- 2.11.3 Permitir treinamento distribuído com uso de GPU;
- 2.11.4 Possibilitar deploy de modelos como API REST;
- 2.11.5 Monitorar modelos em produção (drift, accuracy);
- 2.11.6 Disponibilizar pipeline completo de treinamento e avaliação;
- 2.11.7 Gerenciar datasets com controle de acesso e versionamento;
- 2.11.8 Versionar modelos treinados para rastreabilidade;

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

- 2.11.9 Permitir automatizar tuning de hiperparâmetros;
- 2.11.10 Fornecer ambiente para AutoML, democratizando uso de IA;
- 2.11.11 Integrar pipelines de ML ao CI/CD;
- 2.11.12 Controlar acesso ao ambiente por políticas IAM;
- 2.11.13 Disponibilizar dashboards detalhados de métricas dos modelos;
- 2.11.14 Permitir conexão direta com storage e data lake corporativo;
- 2.11.15 Acionar pipelines e modelos por eventos definidos.

2.11. Geolocalização

- 2.12.1 Possuir recursos de renderização de mapas, geocodificação, roteamento, cálculo de área e distância;
- 2.12.2 Deve suportar overlay temático, múltiplos formatos e consultas espaciais variadas;
- 2.12.3 Implementar camadas dinâmicas, integração via API/SDK, mapas de calor e tiles customizáveis;
- 2.12.4 Permitir armazenamento geoespacial, interoperabilidade, acesso a mapas offline e controle de autenticação;

2.12. Conectividade e Segurança

- 2.13.1 Permitir alocação de IPs públicos estáticos e dinâmicos, conforme a necessidade da aplicação ou serviço;
- 2.13.2 Suportar simultaneamente endereços IPv4 e IPv6, proporcionando compatibilidade ampla;
- 2.13.3 Possibilitar a reatribuição de IPs públicos entre recursos distintos sem interrupção prolongada;
- 2.13.4 Integrar com sistemas de firewall e regras de segurança, garantindo proteção durante o tráfego externo;

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

- 2.13.5 Oferecer configuração de registro PTR (DNS reverso) para IPs alocados;
 - 2.13.6 Permitir tagueamento de IPs por projeto ou unidade organizacional, facilitando o controle e a governança;
 - 2.13.7 Gerar logs detalhados de uso para cada IP público provisionado;
 - 2.13.8 Detectar automaticamente tráfegos anômalos ou comportamentos suspeitos relacionados ao uso de IP;
 - 2.13.9 Suportar políticas de rate limiting por IP para evitar abusos e sobrecarga.
 - 2.13.10 Garantir alta disponibilidade com mecanismos de IP failover, minimizando indisponibilidades.
 - 2.13.11 Prover proteção contra exaustão de IP, prevenindo esgotamento de recursos.
 - 2.13.12 Disponibilizar auditoria abrangente de atribuição e desvinculação de IPs.
 - 2.13.13 Suportar endereços elásticos (Elastic IP), permitindo realocação dinâmica.
 - 2.13.14 Oferecer gerenciamento completo de IPs via API, facilitando automação.
 - 2.13.15 Possibilitar controle de acesso e gerenciamento de permissões por políticas IAM.
- 2.13. Antivírus / DDoS por IP
- 2.14.1 Fornecer proteção contra ataques DDoS nas camadas L3 a L7, cobrindo todo o espectro de ameaças;
 - 2.14.2 Realizar análise heurística e comportamental do tráfego de rede para identificação proativa de ataques;
 - 2.14.3 Emitir alertas em tempo real sobre eventos de segurança e tentativas de ataque;
 - 2.14.4 Executar bloqueio automático de IPs identificados como maliciosos;

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

- 2.14.5 Disponibilizar dashboard centralizado com estatísticas e detalhes dos ataques detectados;
- 2.14.6 Oferecer mitigação automática de ataques como SYN flood e UDP flood;
- 2.14.7 Permitir consulta ao status de mitigação de ameaças por meio de API;
- 2.14.8 Integrar nativamente com WAF e firewall para respostas coordenadas;
- 2.14.9 Suportar escalabilidade horizontal automática dos serviços de proteção;
- 2.14.10 Implementar resposta a ameaças baseada tanto em assinatura quanto em comportamento;
- 2.14.11 Registrar detalhadamente todos os ataques e tentativas por IP;
- 2.14.12 Classificar ameaças por grau de criticidade;
- 2.14.13 Manter lista automatizada e atualizada de IPs bloqueados;
- 2.14.14 Combinar múltiplas camadas de proteção;

2.14. Transferência de Dados

- 2.15.1 Suportar transferência de dados entre regiões e zonas de disponibilidade distintas;
- 2.15.2 Permitir transferência segura via SFTP, HTTPS e SCP;
- 2.15.3 Assegurar criptografia de dados em trânsito utilizando TLS/SSL;
- 2.15.4 Possibilitar configuração de controle de largura de banda para transferência;
- 2.15.5 Permitir agendamento de transferências para horários específicos;
- 2.15.6 Registrar logs de volume, origem e destino de todas as transferências;
- 2.15.7 Implementar mecanismos automáticos de retry em caso de falha;
- 2.15.8 Suportar compressão de arquivos para otimização;
- 2.15.9 Permitir transferência em lote ou por streaming, conforme a demanda;
- 2.15.10 Oferecer upload e download de arquivos tanto via portal web quanto CLI.
- 2.15.11 Permitir realizar re-tentativa de transferências com verificação de integridade por checksum;

**Anexo B – Especificações Mínimas para Homologação de
Provedor de Nuvem Pública**

2.15.12 Enviar notificações automáticas ao término da tarefa de transferência.

2.15.13 Permitir transferência direta para storage, bancos de dados ou VMs.

2.15.14 Suportar conectividade privada e pública, conforme requisitos de segurança.

2.15. Conectividade Dedicada

2.16.1 O serviço de conectividade deve ser fornecido de acordo com o provedor (ExpressRoute da Microsoft Azure; AWS Direct Connect; Cloud Interconnect; IBM Cloud Direct Link; etc), garantindo conexão privada entre o datacenter do Banco e a nuvem pública, sem utilização da Internet;

2.16.2 O serviço deve ser aderente aos requisitos descritos no item 7 - REQUISITOS DO SERVIÇO GERENCIADO DE CONECTIVIDADE – CSP ↔ BNB do **Anexo – Requisitos Técnicos**

--	--