ANEXO I-A

REQUISITOS, QUANTITATIVOS, OBRIGAÇÕES E NÍVEIS DE SERVIÇO

Este Anexo Técnico estabelece, de forma objetiva, clara e auditável, as condições mínimas para contratação de solução corporativa de banco de dados em memória destinada ao suporte de aplicações críticas. O documento foi estruturado para especificar os requisitos técnicos obrigatórios, os serviços associados, os critérios de aceitação, os níveis mínimos de serviço e as obrigações do contratado.

1. Especificações Técnicas Detalhadas

1.1. Os requisitos a seguir são mínimos e obrigatórios. O CONTRATADO deverá comprovar o atendimento por meio de documentação técnica oficial, matriz de aderência, declaração formal do fabricante ou fornecedor, catálogos, manuais e links oficiais.

2. Requisitos Funcionais

2.1. Permitir operação como banco de dados em memória de uso corporativo, com leitura e gravação em baixa latência.

2.2. Suportar estruturas de dados amplamente empregadas em aplicações modernas, incluindo ao menos chave-valor, listas, conjuntos, hashes e filas.

2.3. Suportar persistência configurável, de modo que a Administração possa definir políticas de durabilidade adequadas ao uso de cada ambiente.

2.4. Permitir replicação entre instâncias e mecanismos de sincronização entre nós com monitoramento do estado de replicação.

2.5. Dispor de mecanismos nativos ou integrados de clusterização para distribuição de carga e expansão horizontal.

2.6. Possibilitar failover automatizado e controlado, com promoção de nós de contingência em caso de falha.

2.7. Permitir operação em topologia de alta disponibilidade entre dois sites para o ambiente de produção.

2.8. Oferecer compatibilidade com o padrão de comandos, bibliotecas cliente, protocolos de comunicação e modelo de consumo já adotados pelas aplicações existentes, minimizando refatorações.

2.9. Comprovar compatibilidade prática com o protocolo e a API utilizados pelo ambiente atual, preservando comportamento funcional esperado pelas aplicações consumidoras.

2.10. Suportar publicação e assinatura de mensagens, quando utilizado pelo ambiente contratante em fluxos assíncronos.

2.11. Possibilitar expiração de chaves, políticas de eviction e gerenciamento de memória configurável por ambiente.

2.12. Permitir segregação lógica entre ambientes, bases, clusters, instâncias ou namespaces, conforme arquitetura adotada.

2.13. Disponibilizar interface administrativa, linha de comando, API ou console equivalente para administração segura da solução.

2.14. Oferecer mecanismos de backup e restauração compatíveis com a criticidade dos dados tratados pela solução.

2.15. Permitir exportação de métricas, eventos, logs e indicadores operacionais para ferramentas corporativas de observabilidade.

2.16. Permitir atualização de versão e aplicação de correções sem perda indevida de configuração e com procedimentos formalizados.

2.17. Suportar autenticação, autorização e controle de acesso com granularidade compatível com ambientes corporativos.

2.18. Permitir auditoria de eventos administrativos relevantes, incluindo acessos, alterações de configuração e ações críticas.

2.19. Disponibilizar documentação técnica oficial abrangendo instalação, configuração, operação, troubleshooting e boas práticas.

2.20. Permitir uso on-premises em infraestrutura do contratante, inclusive virtualizada ou conteinerizada, quando tecnicamente aplicável.

2.21. Disponibilizar suporte técnico especializado do fabricante ou canal oficialmente autorizado, com escalonamento para níveis avançados.

3. Requisitos Não Funcionais

3.1. Apresentar desempenho compatível com processamento em memória e cenários de alta concorrência.

3.2. Assegurar previsibilidade de resposta em cargas elevadas, com comportamento estável sob pico transacional.

3.3. Atender a operação contínua em regime 24x7x365, sem dependência de intervenção manual rotineira para funcionamento básico.

3.4. Suportar expansão horizontal e vertical sem descaracterização da arquitetura da solução.

3.5. Permitir capacity planning com indicadores objetivos de uso de memória, CPU, throughput, latência, fragmentação e filas.

3.6. Possibilitar operação segura em ambientes críticos, com criptografia em trânsito e, quando aplicável, em repouso.

3.7. Possuir controles aderentes às diretrizes de segurança da informação, incluindo autenticação forte, segregação de privilégios e hardening.

3.8. Permitir rastreabilidade e governança operacional, com trilhas de auditoria e relatórios de uso e saúde do ambiente.

3.9. Ser compatível com práticas de gestão de incidentes, mudanças, configuração, capacidade, disponibilidade e continuidade.

3.10. Viabilizar RTO e RPO compatíveis com a criticidade do serviço, conforme parametrização e arquitetura implantadas.

3.11. Permitir manutenção, atualização e correção com procedimentos controlados e risco reduzido de indisponibilidade.

3.12. Ser aderente à LGPD e às normas institucionais aplicáveis, no que se refere à proteção de dados, controle de acesso e minimização de exposição.

3.13. Assegurar interoperabilidade com ferramentas corporativas de monitoramento, logging, automação, ITSM e gestão de ativos.

3.14. Permitir documentação e transferência de conhecimento suficientes para a sustentação pela equipe do contratante.

3.15. Apresentar maturidade operacional compatível com uso corporativo, com versões estáveis, ciclo de atualização definido e suporte continuado.

3.16. Oferecer meios de diagnóstico avançado, análise de causa raiz e coleta de evidências para investigação de incidentes.

3.17. Possibilitar isolamento de falhas, contenção de impacto e recuperação controlada em cenários de pane parcial ou total.

3.18. Evitar dependência de soluções artesanais para funções centrais de disponibilidade, segurança ou administração.

3.19. Permitir padronização operacional entre ambientes de desenvolvimento, homologação e produção.

3.20. Ser fornecida em modelo contratual que estabeleça responsabilidades claras quanto a suporte, atualização, correção e atendimento.

4. Requisitos de Arquitetura, Implantação e Integração

4.1. A solução deverá operar em ambiente on-premises do contratante, por se tratar de componente crítico sujeito a requisitos institucionais de segurança, continuidade e governança.

4.2. Deverá ser compatível com arquitetura distribuída, incluindo múltiplos nós, replicação, cluster e mecanismos de continuidade entre dois datacenters.

4.3. Para produção, deverá admitir arquitetura de alta disponibilidade com redundância entre sites e failover automatizado ou fortemente assistido por política configurável.

4.4. Deverá permitir implantação em ambientes de desenvolvimento, homologação e produção, observadas as diferenças de porte e criticidade de cada camada.

4.5. Deverá suportar integração com diretórios corporativos, ferramentas de identidade, cofres de segredos, plataformas de monitoramento, gestão de logs e soluções de ITSM, quando tecnicamente aplicável.

4.6. Deverá possuir mecanismos de parametrização, tuning e observabilidade suficientes para operação por equipe corporativa.

4.7. Deverá manter alta aderência ao padrão atualmente consumido pelas aplicações internas, de modo que a migração ou substituição ocorra com esforço mínimo de alteração de código, bibliotecas e integrações.

4.8. Deverá permitir segregação entre ambientes e cargas de trabalho, evitando que atividades não produtivas afetem o desempenho do ambiente produtivo.

4.9. Deverá possibilitar migração controlada a partir do ambiente atual, com preservação de configurações essenciais, minimização de indisponibilidade e plano formal de reversão.

4.10. Deverá fornecer procedimentos de instalação, atualização, rollback, backup, restauração, failover, retorno ao estado nominal e validação pós-implantação.

4.11. Quando houver uso de bibliotecas, conectores, clientes ou APIs já consolidados nas aplicações do contratante, a solução deverá manter compatibilidade prática e comprovável com tais componentes.

4.12. O CONTRATADO deverá elaborar arquitetura detalhada da implantação, incluindo topologia, fluxos, portas, dependências, pré-requisitos, sizing e estratégia de alta disponibilidade.

4.13. A solução deverá disponibilizar mecanismos para controle de consumo de memória, filas, persistência, replicação, ressincronização, balanceamento e administração de nós.

4.14. A implantação deverá prever homologação técnica antes da entrada em produção, com testes documentados de desempenho, disponibilidade, recuperação e segurança.

4.15. A solução deverá permitir observabilidade fim a fim, com coleta de métricas, logs e alertas compatíveis com os processos internos do contratante.

4.16. Deverá existir separação clara entre responsabilidades do fornecedor e do contratante durante implantação, operação assistida e sustentação continuada.

5. Requisitos de Serviços Associados

5.1. Fornecimento das subscrições necessárias ao atendimento do quantitativo estimado.

5.2. Serviços profissionais de configuração, parametrização, tuning, validação e estabilização inicial.

5.3. Serviços de migração, transição ou integração com o ambiente atual, quando aplicáveis

5.4. Transferência de conhecimento para equipes técnicas e de fiscalização do contratante.

5.5. Entrega de documentação técnica, administrativa e operacional completa.

5.6. Suporte técnico especializado em regime 24x7x365 para toda a solução licenciada.

5.7. Disponibilização de atualizações corretivas, patches de segurança e orientações para evolução da plataforma durante a vigência contratual.

5.8. Apoio a capacity planning, análise de causa raiz, recomendações de arquitetura e estabilização do ambiente.

6. Quantitativos e Unidades de Medida

6.1. Os quantitativos abaixo refletem a estimativa consolidada no Estudo Técnico Preliminar e deverão ser observados como referência mínima para composição da proposta, ressalvada a obrigação da contratada de entregar todos os componentes acessórios necessários ao perfeito funcionamento da solução.

#ID	Descrição Técnica Resumida	Unidade	Quantidade
01	Subscrição Redis enterprise para ambiente não produtivo com capacidade de 1.000 operações por segundo e 1 GB para desenvolvimento.	Subscrição	21
02	Subscrição Redis enterprise para ambiente não produtivo com capacidade de 1.000 operações por segundo e 1 GB para homologação.	Subscrição	6
03	Subscrição Redis enterprise para ambiente produtivo com capacidade de 1.000 operações por segundo e 1 GB, considerando alta disponibilidade entre dois sites.	Subscrição	32
04	Subscrição Redis para ambiente produtivo com capacidade de 5.000 operações por segundo e 5 GB, considerando alta disponibilidade entre dois sites.	Subscrição	2
05	Serviço corporativo de suporte técnico e assistência especializada 24x7x365 para toda a solução Redis.	Serviço	36
06	Capacitação Redis Software (RS) Developer Training para 12 pessoas (opcional). (*)	Pacote	1
07	Capacitação Redis Software Operator Training para 12 pessoas(opcional). (*)	Pacote	1

(*) A utilização dos serviços de IDs 06 e 07 será facultativa, a critério do BNB. Quando solicitados, o CONTRATADO deverá disponibilizá-los em conformidade com o cronograma de disponibilização estabelecido.

7. Cronograma de Disponibilização

A disponibilização dos serviços da Solução obedecerá ao seguinte cronograma:

Evento	Evento	Responsável	Prazo
1	Assinatura do contrato	CONTRATADO	Até 5 (cinco) dias úteis após a convocação pelo BNB.
2	Disponibilização das subscrições	CONTRATADO	Até 5 (cinco) dias úteis após o evento 1.
3	Termo de Aceitação de Licenças	BNB	Até 5 (cinco) dias úteis após o evento 2.

4	Capacitação Redis Software (Developer Training e Operator Training)	CONTRATADO	Até 5 (cinco) dias úteis a partir da solicitação feita pelo BNB.

8. Obrigações da Contratada

8.1. Fornecer solução plenamente aderente aos requisitos mínimos deste Anexo, incluindo todos os componentes indispensáveis ao funcionamento, ainda que não explicitados nominalmente, desde que necessários para atendimento do objeto.

8.2. Executar instalação, configuração, parametrização, tuning, integração, validação técnica e estabilização inicial da solução.

8.3. Disponibilizar suporte técnico especializado com cobertura 24x7x365, canais formais de atendimento e escalonamento para níveis avançados.

8.4. Fornecer atualizações, patches, correções e orientações técnicas durante toda a vigência contratual, conforme modelo de subscrição ofertado.

8.5. Produzir e manter atualizada a documentação técnica da solução implantada, incluindo arquitetura, topologia, configuração, rotinas operacionais, backup, restauração, contingência e troubleshooting.

8.6. Executar, quando aplicável, migração ou transição controlada do ambiente atual para a solução contratada, com preservação da integridade dos dados e mitigação de impacto em produção.

8.7. Realizar transferência de conhecimento para equipe técnica e equipe de fiscalização do contratante.

8.8. Apoiar a Administração em incidentes críticos, análise de causa raiz, capacity planning, boas práticas e recomendações de evolução do ambiente.

8.9. Guardar sigilo sobre informações, configurações, credenciais, dados operacionais e demais elementos a que tiver acesso em razão da execução contratual.

8.10. Observar integralmente as normas institucionais de segurança da informação, continuidade, controle de acesso e proteção de dados aplicáveis ao contratante.

8.11. Apresentar evidências de atendimento dos SLAs pactuados, relatórios mensais de suporte e registros formais dos chamados atendidos.

9. Níveis de Serviço (SLA)

9.1. Os níveis mínimos de serviço abaixo deverão ser cumpridos como um todo sob pena de glosa em caso de não cumprimento.

Severidade	Exemplo de Enquadramento	Resposta Inicial	Início do Atendimento após resposta inicial	Restabelecimento/Solução
Sev. 1	Indisponibilidade total de produção, falha de cluster, falha de	até 30 minutos	até 30 minutos	solução de contorno em até 2 horas e restauração ou plano formal de

	failover, perda de sincronismo crítico ou incidente de segurança com impacto operacional relevante.			estabilização em até 4 horas.
Sev. 2	Degradação severa de desempenho, perda relevante de redundância, esgotamento de memória, falha de replicação sem parada total.	até 2 horas	até 1 hora	solução de contorno em até 4 horas e correção ou estabilização em até 8 horas.
Sev. 3	Falha parcial, erro de configuração, necessidade de ajuste técnico, tuning ou suporte operacional sem interrupção do serviço crítico.	até 4 horas	até 8 horas	até 3 dias úteis.
Sev. 4	Dúvidas técnicas, orientações, requisições administrativas ou demandas de baixa urgência.	até 2 dias úteis	até 2 dias úteis	até 5 dias úteis.

9.2. Adicionalmente, a solução deverá observar disponibilidade mensal mínima de 99,9% para o serviço de suporte e para os componentes sob responsabilidade direta da contratada, ressalvadas as janelas programadas previamente aprovadas pela Administração. O CONTRATADO deverá fornecer relatórios mensais de SLA, tempo médio de resposta, tempo médio de atendimento, tempo médio de restauração, incidentes por severidade, reincidência e análise de causa raiz para ocorrências críticas.

10. Redutores de níveis de serviço

10.1. Os redutores de níveis de serviço têm como finalidade garantir a resolução dos chamados dentro do tempo estabelecido de restabelecimento da solução.

Severidade	Sev. 1	Sev. 2	Sev. 3	Sev. 4
Desconto aplicado	3,00% do valor da parcela do serviço de suporte e assistência por hora ou fração de atraso	2,50% do valor da parcela do serviço de suporte e assistência por hora ou fração de atraso	1,00% do valor da parcela do serviço de suporte e assistência por hora ou fração de atraso	0,5% do valor da parcela do serviço de suporte e assistência por hora ou fração de atraso

10.2. Tais redutores serão aplicados sob o valor mensal do serviço de suporte e assistência.

11. Disposições Complementares

11.1. A solução ofertada deverá ser comercialmente suportada durante toda a vigência contratual.

11.2. Não será aceita solução que dependa de customizações estruturais não suportadas oficialmente para atender funções centrais de disponibilidade, suporte ou segurança.

11.3. A simples compatibilidade parcial com o ambiente atual não será suficiente; exige-se aderência integral aos requisitos mínimos e comprovação objetiva.

11.4. Sempre que houver referência a compatibilidade com o ambiente atual, deve-se entender compatibilidade funcional e operacional, apta a reduzir impactos de migração e retrabalho nas aplicações consumidoras.

11.5. A contratada deverá cooperar com a fiscalização contratual, fornecendo informações, evidências, relatórios e acesso às equipes técnicas necessárias ao acompanhamento da execução.

12. Capacitação Redis Software (Developer Training e Operator Training)

12.1. A requisição do treinamento é um ato discricionário do CONTRATANTE, podendo ser requisitado ou não a qualquer tempo durante a vigência do contrato, sendo o pagamento efetuado somente após ministrado o treinamento;

12.2. Caso seja requisitado o CONTRATADO deve oferecer treinamento oficial do fabricante da solução em idioma português (BR);

12.3. Após o treinamento com a devida aprovação, os participantes devem receber os certificados oficiais do fabricante da solução;

12.4. Cada treinamento deve ser ministrado para um grupo de 12 pessoas;

12.5. O treinamento poderá ser gravado pelo CONTRATANTE sem nem nenhum custo adicional;

12.6. Todo o material produzido durante o treinamento será propriedade do CONTRATANTE.

ANEXO I-B

DECLARAÇÃO DE NÃO OCORRÊNCIA DE REGISTRO DE OPORTUNIDADE

Ao Banco do Nordeste S/A,
Ref. Edital de Pregão Eletrônico nº. ____/2026

Objeto: Contratação de subscrição Redis Enterprise como solução corporativa de banco de dados em memória, com suporte técnico, assistência especializada e capacitação, para sustentação de aplicações críticas do Banco do Nordeste.

Prezados Senhores,

O (LICITANTE), (qualificação), por meio de seu representante legal, **DECLARA**, que para a apresentação de proposta ao referido Edital, **NÃO** houve ocorrência de "**Registro de Oportunidade**", de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública, conforme disposto na Instrução Normativa Nº 1 de 4 de abril de 2019 e n art. 31 da Lei nº 13.303, de 2016.

Local: _____

Data: ___/___/___

Representante Legal:

(ASSINATURA) _____

RG: _____

CPF: _____