

ANEXO I – DESCRIÇÃO DOS SERVIÇOS

1. Objeto

Contratação de solução de software existente no mercado, doravante chamada SOLUÇÃO, para substituir sistema proprietário, de modo a atender às necessidades do Banco do Nordeste (“BNB”) quando da realização das atividades inerentes à prestação de serviços de distribuição e de controladoria de passivo de cotas de classes e subclasses de fundos de investimento financeiros e Fundos Mútuos de Privatização – FMP doravante tratados como FUNDO ou FUNDOS inclusive para atendimento às normas dos órgãos reguladores e autorreguladores inerentes a esses produtos.

2. Requisitos Técnicos

Os requisitos a seguir descritos são necessários para que o BNB possa desenvolver as atividades de distribuição de FUNDOS próprios e de terceiros (distribuição por conta e ordem) e de controladoria do passivo de FUNDOS próprios e de terceiros, podendo um FUNDO possuir o BNB como prestador de um ou dos dois tipos de serviços. Os FUNDOS podem ter administradores fiduciários distintos e serem distribuídos através do internet/mobile banking do BNB e/ou das suas agências bancárias e/ou através de ferramentas de tecnologia de terceiros, como as plataformas digitais de investimento. Os FUNDOS podem ser de varejo, restrito, exclusivos, fundos de fundos etc.

2.1 Requisitos Funcionais

- 2.1.1 Possuir funções de controle de usuários por perfil de acesso e departamentos (agências bancárias, unidade gestora da controladoria do passivo, unidade gestora de distribuição, auditoria etc.), permitindo delimitar quais funcionalidades permitidas para cada perfil de acesso e/ou departamento.
- 2.1.2 Permitir opção de camadas de validação de aplicação/resgates, com usuários editores e usuários aprovadores;
- 2.1.3 Permitir que usuário interno do BNB lotado em agência bancária ou em outra unidade de negócio sua (doravante tratado como USUÁRIO) registre/exclua comandos de Aplicação e Resgate em FUNDOS inclusive agendamentos em nome de clientes de sua unidade de negócio;
- 2.1.4 Permitir que usuário interno lotado no setor gestor do sistema (doravante tratado como GESTOR) registre/exclua comandos de Aplicação e Resgate em FUNDOS inclusive agendamentos em nome de clientes de todas as unidades de negócios;
- 2.1.5 Permitir realizar mais de um comando (aplicação/resgate) para o mesmo cliente, em uma mesma conta corrente, no mesmo FUNDO em um mesmo dia;
- 2.1.6 Possuir funcionalidades para Fundos Mútuos de Privatização – FMP, tais como aplicação, resgate, bloqueios, desbloqueios, transferências etc.;
- 2.1.7 Possuir funcionalidade que permita restringir a disponibilidade de um FUNDO para um determinado grupo de clientes considerando critérios determinado pelo BNB (utilizado para fundos com restrições em seu público-alvo);

- 2.1.8 Permitir funcionalidades que permitam controle e consulta dos clientes isentos de tributos;
- 2.1.9 Permitir realizar operações de bloqueios e desbloqueios administrativos e judiciais;
- 2.1.10 Possuir funcionalidades para FUNDOS com atributos de Aplicação e/ou Resgate Automáticos com respectivos débitos ou créditos na conta corrente no BNB vinculada ao investimento;
- 2.1.11 Possuir função de envio de notificações a usuários internos de acordo com regras parametrizáveis através de ferramentas como: e-mail, SMS, mensagens instantâneas etc., para alertas, lembretes ou notificações;
- 2.1.12 Realizar cálculo de tributos dos cotistas dos FUNDOS;
- 2.1.13 Permitir Efetuar, Consultar e Excluir o estorno de tributos;
- 2.1.14 Permitir as seguintes consultas:
- Saldo médio;
 - Operações que geraram Termo de Adesão e Ciência de Risco;
 - Agendamento de aplicações e resgates;
 - Comandos de aplicações e resgates excluídos;
 - Aplicações e resgates realizados;
 - Cálculos de rentabilidade;
 - Clientes isentos de tributos;
 - Limites operacionais dos FUNDOS (aplicação inicial, movimentações mínimas etc.);
 - Maiores clientes;
 - movimentação com saldo dos cotistas nos FUNDOS;
 - Movimentação de Fundos Mútuos de Privatização – FMP;
 - movimentação de rendimentos negativos;
 - Movimento diário de aplicações e resgates;
 - informações de clientes com aplicações ou resgates automáticos;
 - Operações agendadas rejeitadas;
 - Bloqueios/desbloqueios administrativos, judiciais e transferências;
 - Aplicações rejeitadas por insuficiência de saldo em conta corrente;
 - Posição diária dos saldos por FUNDO e por agência;
 - Posição de cotista por FUNDO e por agência;
 - Perfil mensal de Cotistas, Quantidade de Cotistas, entre outras (dados requeridos pela Comissão de Valores Mobiliários - CVM);
 - Informações por Segmento de Investidor - Patrimônio Líquido e número de cotistas;
 - Previsão de aplicação e resgates a serem convertidos em cotas;
 - Ranking Global - ANBIMA;
 - Relação de cotista isentos de imposto de renda (Entidades imunes);
 - Rentabilidade mensal;
 - Resgates ocorridos;
 - Resumo analítico e sintético das aplicações e resgates;
 - Informações relacionadas a receitas com taxas de administração, gestão, distribuição conforme legislações tributárias federais, estaduais ou municipais e para uso gerencial;
 - Valores das cotas;
 - Código da Conta Preferencial do CLIENTE;
 - Critérios de Tributação;
 - Isenção de Tributação;
 - Lançamento de Tributos Incidentes;

- 2.1.15 Permitir Incluir, Consultar e Excluir documentos exigidos pela regulação tais como: regulamentos, termo de adesão e risco, entre outros;
- 2.1.16 Permitir gerar informações da estatística global dos FUNDOS requeridas pela ANBIMA;
- 2.1.17 Permitir gerar relatório mensal de evolução de ingressos e retiradas de informações tais como quantidade de cotas aplicadas e resgatadas, valor financeiro aplicado e resgatado, entre outros;
- 2.1.18 Permitir consultar informe de rendimentos das aplicações e tributação recolhida para Secretaria da Receita Federal do cliente;
- 2.1.19 Permitir Alterar, Consultar, Incluir e Excluir dados do Passivo;
- 2.1.20 Permitir Alterar, Consultar, Incluir e Excluir dados do Ativo;
- 2.1.21 Permitir o Detalhamento de informações de FUNDOS - Internet e Mobile Banking;
- 2.1.22 Permitir consultar saldo consolidado, detalhado e com rendimento negativo (quando houver) dos fundos de investimento de um dado cliente;
- 2.1.23 Permitir encerrar o sistema para atualização de cotas, Imposto de Renda, IOF envio de créditos e débitos à conta corrente e outros;
- 2.1.24 Permitir gerar Declaração do Imposto sobre a Renda Retido na Fonte - DIRF;
- 2.1.25 Permitir Gerar Informe de rendimentos – Pessoa Física e Pessoa Jurídica;
- 2.1.26 Permitir Exibir Saldo de Conta Corrente em operações de aplicação e resgate;
- 2.1.27 Permitir enviar bloqueio/débito de saldo para conta corrente em operações de aplicação em fundo de investimento;
- 2.1.28 Permitir crédito do valor do resgate em conta corrente de acordo com prazo de cotização dos FUNDOS;
- 2.1.29 Permitir retenção de tributos semestrais para recolhimento à Receita Federal pelo BNB à título de "come-cotas";
- 2.1.30 Permitir Manutenção do Perfil do cotista para fins de prestação de informações tais como emitir extrato mensal, tributação, imunidade e outras;
- 2.1.31 Permitir efetuar o Processamento Movimentos de bloqueios administrativos, bloqueios judiciais, desbloqueios e transferências;
- 2.1.32 Permitir efetuar o processamento dos movimentos manuais de aplicações e resgates realizados durante o horário permitido conforme regulamentos dos FUNDOS;
- 2.1.33 Permitir efetuar o Processamento Rentabilidade;
- 2.1.34 Permitir comandar, manualmente, o reprocessamento de geração de informações para sistemas integrados por meio de processos "batch", quando aplicável;
- 2.1.35 Permitir comandar, manualmente, o reprocessamento do Passivo de Fundos de Investimentos;
- 2.1.36 Permitir Emitir Relatório de relação de cotista com Aplicação e Resgate Por Período e na data base (data específica escolhida pelo usuário);
- 2.1.37 Permitir Emitir Relatório com informações quando houver resgate de Fundo Mútuo de Privatização - FMP para devolução de recursos FGTS à Caixa Econômica Federal;
- 2.1.38 Permitir Emitir Relatório Resumo Efetivo de Movimentação de aplicações e resgates manuais ou automáticas, aplicações e resgates rejeitados e resgate come-cotas, no dia ou em outras periodicidades;
- 2.1.39 Permitir gerar informações de receitas com taxa de administração e gestão de acordo com o domicílio do cliente - tomador do serviço - (Lei Complementar nº 175 de 23/12/2020);
- 2.1.40 Permitir gerar informações de Receitas com Taxa de Gestão/Distribuição consolidadas por Agência;
- 2.1.41 Permitir dispor de função de escrituração no registro complementar de cotistas com atribuição de código para cada cotista conforme Art. 34 da Resolução CVM 175, de

- 23/12/2022 (“RCVM 175”), ou seja, codificação de cotistas na Distribuição por Conta e Ordem;
- 2.1.42 Permitir dispor de função para exportação da movimentação de cotistas FUNDO e Administrador Fiduciário;
 - 2.1.43 Permitir calcular taxas de performance, entrada e saída, conforme aplicável;
 - 2.1.44 Permitir calcular, apurar e reter os tributos pertinentes a cada cotista, no caso de cotas de FUNDOS abertos;
 - 2.1.45 Permitir dispor de função para conciliar as movimentações financeiras dos cotistas no Passivo de Fundos de Investimento com a movimentação da conta corrente de cada Fundo de investimento;
 - 2.1.46 Permitir processar e liquidar a amortização e distribuição de rendimentos em nome de cada cotista mediante as informações recebidas do Administrador Fiduciário, considerando tributos aplicáveis a cada cotista;
 - 2.1.47 Permitir processar e liquidar eventos, tais como: cisão, incorporação, encerramento de fundos e outros eventualmente disponíveis;
 - 2.1.48 Possibilitar a convocação digital de cotistas (por e-mail ou por outro método);
 - 2.1.49 Permitir consulta de clientes que assinaram os termos de aplicação automática;
 - 2.1.50 Permitir consulta de clientes que assinaram os termos de adesão e ciência de risco;

2.2 Integrações Mapeadas

- 2.2.1 Obter as informações dos usuários internos, com base em suas unidades de trabalho e autorização de acesso;
- 2.2.2 Consultar e listar históricos das contas correntes dos cotistas;
- 2.2.3 Gerar arquivo com as informações de Saldo Médio de FUNDO ou grupo de FUNDOS especificados com ou sem segmentação de clientes;
- 2.2.4 Enviar comandos de débito e crédito para as contas corrente dos cotistas;
- 2.2.5 Enviar movimentação contábil;
- 2.2.6 Gerar informações para a e-Financeira - Instrução Normativa Receita Federal do Brasil nº 1571, de 02 de julho de 2015;
- 2.2.7 Gerar informações para Escrituração Fiscal Digital de Retenções e Outras Informações Fiscais EFD-Reinf (Instrução Normativa nº 2043, de 12 de agosto de 2021 da Receita Federal do Brasil);
- 2.2.8 Gerar informações para o Banco Central do Brasil - BACEN (Arquivos 5401 e 5402);
- 2.2.9 Gerar informações para que seja possível avaliar o desempenho das agências, bem como as suas remunerações;
- 2.2.10 Acessar informação de e-mail para geração de lista de clientes cotistas para envio de mala diretas;
- 2.2.11 Automatizar o processo de assinatura eletrônica do termo de adesão e ciência de risco, termo de autorização de aplicação automática e análise do perfil do investidor - API (assinatura eletrônica);
- 2.2.12 Possibilitar o envio de documentos (por exemplo: Termo de Adesão e Ciência de Risco) para sistemas de gerenciamento de documentos (arquivo digital);
- 2.2.13 Gerar consulta, aplicações e resgates em FUNDOS através do Internet e Mobile Banking;
- 2.2.14 Gerar informações para envio ao Administrador Fiduciário cadastrado;
- 2.2.15 Gerar extrato mensal dos movimentos dos cotistas;

- 2.2.16 Preencher questionário de perfil de investidor, conforme dispõe a regulação vigente (Obs: esta integração somente será necessária, caso a SOLUÇÃO não disponibilize tal funcionalidade);
- 2.2.17 Gerar consulta saldos de fundos de investimentos em canais de comunicação;
- 2.2.18 Gerar consulta saldos de fundos de investimentos para sistema interno de Automação Bancária;
- 2.2.19 Gerar informações de fundos de investimentos para o sistema interno de gerenciamento de clientes;
- 2.2.20 Gerar informações de fundos de investimentos para o sistema interno de rentabilidade de clientes;
- 2.2.21 Gerar informações de fundos de investimentos para o sistema interno de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento ao Terrorismo;
- 2.2.22 Gerar informação de perfil mensal de Cotistas, Quantidade de Cotistas, entre outras, para Comissão de Valores Mobiliários - CVM;
- 2.2.23 Gerar Informações por Segmento de Investidor - Patrimônio Líquido e número de cotistas - ANBIMA;
- 2.2.24 Gerar Informações do Ranking Global para ANBIMA;
- 2.2.25 Enviar Tarifas de extratos de fundos para sistema interno de Tarifas;
- 2.2.26 Consultar bloqueios judiciais com base em sistema interno de Ordens Judiciais;
- 2.2.27 Enviar ordens automatizadas de aplicações e resgate para sistema interno;
- 2.2.28 Gerar informações para o Open Banking;
- 2.2.29 Efetuar importação dos valores de cotas, taxa de gestão, taxa de administração e taxa de custódia informadas pelo Administrador Fiduciário;
- 2.2.30 Consulta dados de funcionários de terceirizados cadastrados;

2.3 Requisitos não funcionais

- 2.3.1. Disponibiliza APIs que permitam integração do sistema com soluções externas complementares;
- 2.3.2. Em caso de término de contrato de uso, a solução deve possibilitar a portabilidade de todos os dados armazenados ao longo da utilização pela CONTRATANTE;
- 2.3.3. Possui ferramenta para desenvolvimento de customização de produtos, APIs ou funcionalidades sem interferência do fornecedor;
- 2.3.4. A solução possibilita expurgo automático de dados;
- 2.3.5. A solução permite 5 (cinco) anos de persistência dos dados para temas legais e regulatórios;
- 2.3.6. A solução possibilita que sejam configuradas ROLE padrão para novos usuários cadastrados;
- 2.3.7. Permitir configuração feita através de interface WEB administrativa única;
- 2.3.8. Dar visibilidade fim a fim de todas as transações, incluindo as malsucedidas;
- 2.3.9. A solução possui controle de vigência dos registros de qualquer tabela de dados para possibilitar as consultas de histórico;
- 2.3.10. A ferramenta possui mecanismo de migração dos dados (Importar/Exportar massivamente);
- 2.3.11. Disponibiliza testes automatizados que garantam o Core da aplicação;
- 2.3.12. Permitir automação de deploy (CI/CD) continuous deployment;
- 2.3.13. Possui local centralizado com toda documentação atualizada do sistema para uso pelos usuários finais;

- 2.3.14. Possui local centralizado com toda documentação atualizada do sistema para usuários finais, times de desenvolvimento e suporte operacional;
- 2.3.15. Possui programa de treinamento de usuários (administradores e usuários normais da aplicação). Caso positivo, informar escopo, objetivo, idiomas, quantidade máxima de alunos por turma e carga mínima. Informar também caso exista um treinamento hands-on capaz;
- 2.3.16. Possui programa de treinamento técnico para manutenção / operacionalização (desenvolvimento sem interferência do fornecedor e operação da solução). Caso positivo, informar escopo, objetivo, idiomas, quantidade máxima de alunos por turma e carga mínima. Informar também caso exista um treinamento hand-son capaz de capacitar mais rapidamente os usuários;
- 2.3.17. O banco de dados da SOLUÇÃO possui padronização quanto à nomenclatura dos objetos (tabelas, colunas, funções, gatilhos, visões etc.);
- 2.3.18. Todas as tabelas da SOLUÇÃO possuem chave primária ou chave única;
- 2.3.19. O banco de dados da SOLUÇÃO possui índices nos objetos que são alvo das principais consultas das rotinas da aplicação e nos campos que fazem referência a outras tabelas;
- 2.3.20. O banco de dados da SOLUÇÃO está estruturado de forma a evitar a redundância de tabelas;
- 2.3.21. O dono (owner) dos objetos do banco de dados da SOLUÇÃO será o superusuário. O usuário de conexão da SOLUÇÃO (aplicação) somente tem permissões de DML (Data Manipulation Language) nos objetos do banco de dados;
- 2.3.22. A SOLUÇÃO permite a configuração e execução de procedimentos para eliminação de dados históricos, sob controle rígido de permissões de acesso e registro em log de auditoria;
- 2.3.23. Todas as versões de softwares básicos, frameworks, servidores e quaisquer outros recursos utilizados pela SOLUÇÃO são compatíveis com o ambiente computacional do Banco do Nordeste;
- 2.3.24. A SOLUÇÃO garante que a sessão do usuário não seja perdida por conta de falha em um nó do cluster (lógico / físico) de execução. A sessão pode ser migrada para outro nó quando houver falha, sendo esta uma operação transparente para o usuário;
- 2.3.25. A documentação técnica do sistema está escrita nos idiomas: português do Brasil ou Inglês;
- 2.3.26. O help on-line e manual do usuário estão escritos no idioma português do Brasil;
- 2.3.27. A SOLUÇÃO utiliza e apresenta mensagens e telas no idioma português do Brasil;
- 2.3.28. A SOLUÇÃO permite que a identidade visual do BANCO possa ser configurada em seus relatórios e documentos;
- 2.3.29. A SOLUÇÃO permite integração com as ferramentas de BI (Business Intelligence) do BANCO;
- 2.3.30. A SOLUÇÃO permite conexões com múltiplas fontes de dados de forma transparente, possibilitando a conexão com bases de dados relacionais através de conectores ODBC, JDBC, XML e arquivos texto;
- 2.3.31. A SOLUÇÃO permite trabalhar a qualidade dos dados: oferecer mecanismos para tratamento de registros rejeitados ou que estejam fora do padrão esperado;
- 2.3.32. A SOLUÇÃO permite exportar uma visão de relatório/consulta para diferentes formatos (TXT, HTML, DOC/DOCX, XLS/XLSX, CSV, XML, ODT, ODS e PDF);
- 2.3.33. A SOLUÇÃO permite acesso aos dados transacionais de forma on-line para a construção de relatórios/consultas;
- 2.3.34. A SOLUÇÃO permite compor dados de diversas fontes (módulos da SOLUÇÃO, sistemas legados, fontes externas) para criação de relatórios/consultas;

- 2.3.35. Os módulos da SOLUÇÃO apresentam-se integrados entre si, de forma única e nativa;
- 2.3.36. A SOLUÇÃO provê arquitetura baseada em micros serviços na construção das integrações entre seus módulos, sistemas legados e sistemas externos;
- 2.3.37. A SOLUÇÃO suporta integrações através de APIs/REST;
- 2.3.38. A SOLUÇÃO suporta integrações através de serviços web/SOAP;
- 2.3.39. A SOLUÇÃO suporta integrações com Webpsphere Message Broker;
- 2.3.40. A SOLUÇÃO suporta integrações para envio e recebimento de mensagens de filas com MQSeries;
- 2.3.41. A SOLUÇÃO permite reiniciar um processo de carga de onde parou, sem a necessidade de codificar essa inteligência;
- 2.3.42. A SOLUÇÃO provê recursos de paralelização de processos de carga e processamento de grande volume de dados;
- 2.3.43. A SOLUÇÃO possui capacidade de reaproveitar as parametrizações efetuadas anteriormente, na implantação de novas versões;
- 2.3.44. A SOLUÇÃO possui ferramenta para aplicação de correções no sistema, de forma automatizada, que facilite e minimize o impacto de atualizações de versões, possibilitando a análise dos objetos afetados (parametrizações, alterações de código e novos desenvolvimentos);
- 2.3.45. A SOLUÇÃO possibilita o monitoramento e rastreamento de mensagens técnicas como mensagens de erros, eventos, transações executadas, entre outras (a partir da camada de aplicação);
- 2.3.46. A SOLUÇÃO provê interface responsiva com suporte às plataformas móveis principais (Android e iOS) para integração com Internet e Mobile Banking;
- 2.3.47. A interface da SOLUÇÃO é intuitiva, clara, direta e de fácil assimilação por qualquer tipo de usuário;
- 2.3.48. A SOLUÇÃO permite que as informações sejam exibidas em tela antes de sua impressão ou armazenamento;
- 2.3.49. Para utilização no back office, a solução disponibiliza aplicação web ou desktop que pode ser customizada;
- 2.3.50. A SOLUÇÃO possibilita customizações (front-end e/ou back-end), via desenvolvimento de extensões para atender necessidades específicas;
- 2.3.51. A Contratante pode realizar customizações do produto com equipe interna, sem obrigatoriedade de contratação de fornecedor ou empresa parceira;
- 2.3.52. O Fornecedor disponibiliza documentação detalhada da solução e arquitetura de software, dados, infra, rede, segurança, e plano de implantação inicial;
- 2.3.53. A SOLUÇÃO possui mecanismos de integração dos serviços de nuvem com as aplicações existentes nos datacenters do BNB de forma bidirecional (ser possível a uma aplicação invocar operações disponíveis na outra parte), a integração utilizando protocolos de comunicação que sejam padrão de mercado;
- 2.3.54. A SOLUÇÃO disponibiliza recurso de controle e rollback de versões;
- 2.3.55. A SOLUÇÃO possui processos bem definidos para tratativa de requisições e incidentes, com SLA, modelo de escalonamento e canais de comunicação com a CONTRATANTE;
- 2.3.56. A SOLUÇÃO possui relatórios periódicos das requisições e incidentes, abertos e atendidos;
- 2.3.57. A SOLUÇÃO possui atendimento e suporte ao produto em horário comercial, ou 24x7 caso a solução tenha processamento batch em outro horário;
- 2.3.58. A SOLUÇÃO possui equipes de suporte técnico e funcional da solução. Caso positivo, listar os locais no Brasil onde existem, informando se a equipe é própria ou terceirizada;

- 2.3.59. A SOLUÇÃO disponibiliza interfaces para que administradores de sistemas possam monitorar 100% do ambiente de produção no qual a solução está sendo executada. Se atende, informar se são ferramentas próprias do proponente ou se são soluções terceirizadas, como também se são módulos adquiridos e instalados a parte ou se são módulos padrão da solução;
- 2.3.60. A SOLUÇÃO disponibiliza mecanismos para administrador de sistema confirmar que integrações (independente da técnica: API, ETL. etc.) estão com erro e precisam ser reenviadas (conciliação de integrações);
- 2.3.61. Caso a SOLUÇÃO seja disponibilizada apenas como on-premises permite deployment em ambiente virtualizado com VMWARE vSphere 7 ou superior.;
- 2.3.62. Caso seja na modalidade Cloud, funciona nos provedores Google, Oracle, Amazon (AWS) ou Microsoft (Azure);
- 2.3.63. A SOLUÇÃO suporta redundância geográfica e alta disponibilidade;
- 2.3.64. A SOLUÇÃO possui tratamento para diferentes fusos horários e horários de verão;
- 2.3.65. A SOLUÇÃO possui dicionário de falhas / Códigos de erro;
- 2.3.66. A solução permite integração a gestão e governança de acesso compatíveis com Azure AD, SAML, OATH 2;
- 2.3.67. Todos os módulos que compõem a SOLUÇÃO são compatíveis com o ambiente computacional do BANCO;
- 2.3.68. A SOLUÇÃO permite a integração com ferramentas de escritório (MS Office e Open Office) e serviços de Agenda e Correio Eletrônico compatível com interfaces MAPI e IMAP e integração com agentes de correio eletrônico em padrão SMTP e POP3;
- 2.3.69. A SOLUÇÃO suporta a utilização de mecanismos de “data sharing”, com balanceamento de carga entre servidores de banco de dados distintos;
- 2.3.70. A SOLUÇÃO possibilita o uso de infraestrutura de clusters locais ou geograficamente dispersos em todos os seus componentes;
- 2.3.71. Em caso de rotinas batch necessárias ao funcionamento da SOLUÇÃO são compatíveis com gerenciamento pela ferramenta BMC Control-M de scheduling e gerenciamento de processamentos batch do BNB;
- 2.3.72. A SOLUÇÃO possibilita monitoramento das informações de consultas e sessões e definição de gatilhos para identificar consultas com baixo desempenho ou consumo excessivo de recursos;
- 2.3.73. A SOLUÇÃO possui inteligência na geração dos alertas, por meio de mecanismo de correlação e propagação de eventos, com o objetivo de evitar a emissão de alertas sem significado;
- 2.3.74. A SOLUÇÃO permite mecanismos que permitam o Backup e o Restore dos tipos completo (full) e incremental para todos os dados e metadados contidos na SOLUÇÃO, independentemente se estão em SGBD ou Filesystem;
- 2.3.75. A SOLUÇÃO possibilita a integração à ferramenta de geração de backup e "disaster recovery" em uso no BANCO (IBM Spectrum Project versão 8 e superior para plataforma distribuída e Removable Media Management (RMM) e Hardware Security Modules (HSM) para a plataforma mainframe);
- 2.3.76. A SOLUÇÃO suporta a conversão de valores, labels, moeda, formatos padrões de data e hora, mensagens do sistema (erros, alertas, notificações) de acordo com o idioma configurado (Pt/Br);
- 2.3.77. A SOLUÇÃO possui procedimentos de controle de acesso que abordem a transição entre as funções e unidades organizacionais do BANCO, os limites e controles dos privilégios dos usuários e os controles de utilização das contas de usuários;

- 2.3.78. A SOLUÇÃO possibilita estabelecer os perfis de acesso para que os usuários tenham acessos apenas as informações que pertençam ao seu respectivo perfil (se atende, citar como são estabelecidos os perfis);
- 2.3.79. O fornecedor se responsabiliza pelas manutenções regulatórias/legais, de acordo com a legislação brasileira, dentro dos prazos exigidos pelos órgãos reguladores brasileiros;
- 2.3.80. A SOLUÇÃO disponibiliza mecanismo seguro para alteração (criação/remoção/atualização/leitura) de dados;
- 2.3.81. A SOLUÇÃO disponibiliza interface para que sejam auditados todos os eventos de acessos, consultas e demais operações aos dados disponibilizados pela ferramenta;
- 2.3.82. A SOLUÇÃO implementa controles de segurança baseados, no mínimo, no NIST e da série ISO27000;
- 2.3.83. A autenticação dos usuários e clientes segue boas práticas e os padrões mais elevados de Segurança Cibernética (Padrões de senha, expiração, MFA (para administradores e casos específicos);
- 2.3.84. A SOLUÇÃO apresenta conformidade com a normas ABNT NBR ISO/IEC 27017 (serviços em nuvem) e ABNT NBR ISO/IEC 27701 (privacy), além da ABNT NBR ISO/IEC 27001:2013 referente aos serviços de computação em nuvem e aos data centers que hospedem os serviços;
- 2.3.85. A SOLUÇÃO assegura que a infraestrutura de nuvem que suportará o serviço, bem como todo o ciclo de vida da informação, seja processamento ou armazenamento, esteja localizado no Brasil, conforme Norma Complementar 14 IN01/DSIC/SCS/GSIPR de 14/03/18;
- 2.3.86. A SOLUÇÃO disponibiliza informações referentes a medidas adotadas em proteção de dados pessoais, sendo capaz de demonstrar:
- Diretrizes de tratamento;
 - Capacidade de atender adequadamente, e em tempo hábil, uma solicitação do Banco, Autoridade Legalmente Constituída ou Titular, utilizando meios como: portal de privacidade, portal de segurança da informação, e-mail de contato do encarregado de privacidade (DPO), etc, relativos ao tratamento dos dados pessoais realizados;
 - Medidas protetivas para garantia da confidencialidade dos dados pessoais;
 - Medidas protetivas durante as comunicações com o BANCO;
 - Registro de atividades de tratamento de dados pessoais;
 - Solicitação de autorização na subcontratação de terceiros para atividades de tratamento de dados pessoais;
 - Medidas de devolução / descarte dos dados;
- 2.3.87. A SOLUÇÃO implementa procedimentos para fortalecimento dos mecanismos de virtualização, que incluam, no mínimo:
- Desabilitar ou remover todas as interfaces, portas, dispositivos ou serviços desnecessários executados pelo sistema operacional;
 - Configurar com segurança todas as interfaces de rede e áreas de armazenamento virtuais;
 - Estabelecer limites para a utilização dos recursos de máquina virtual (Virtual Machine - VM);

- Manter todos os sistemas operacionais e as aplicações em execução na máquina virtual em suas versões mais atuais;
- Validar a integridade das operações de gerenciamento de chaves criptográficas;
- Possuir controles que permitam aos usuários autorizados do órgão ou da entidade acessarem os registros de acesso administrativo do monitor de máquina virtual - Hypervisor;
- Habilitar o registro completo do Hypervisor;
- Suportar o uso de máquinas virtuais confiáveis (Trusted VM) do Banco que estejam em conformidade com as políticas e práticas de fortalecimento de redes exigidas ao provedor de serviço de nuvem;

2.3.88. A SOLUÇÃO dispõe de mecanismo de autenticação que:

- Exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso;
- Suporta tecnologia single sign-on para autenticação;
- Suporta mecanismos de autenticação multifator ou alternativa que aumente o grau de segurança no processo de autenticação de usuários, de acordo com nível de criticidade da informação manipulada;
- Permite ao Banco gerenciar as próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido;
- Guarda conformidade legal em seus processos de autenticação, controle de acesso, contabilidade e de registro (formato, retenção e acesso);

2.3.89. A SOLUÇÃO implementa soluções e procedimentos para garantir a segurança de aplicações web disponibilizadas no ambiente de nuvem, incluindo, no mínimo:

- Desenvolver código web em conformidade com as melhores práticas de codificação segura OWASP v. 1.3 ou superior, bem como os princípios do Security by Design e normativos vigentes;
- A verificação e validação de dados de entrada garante correção e consistência dos dados, redução do risco de erros e prevenção de ataques conhecidos como injeção de código, para detectar e tratar, no mínimo, os seguintes erros:
 - Entrada duplicada;
 - Valores fora de faixa;
 - Caracteres inválidos em campos de dados;
 - Dados incompletos ou faltantes;
 - Comprimento de dados não respeitando limites superiores ou inferiores;
- Realizar, no mínimo, anualmente, testes de penetração de redes e de aplicações;
- Implementar programa de correção de vulnerabilidades, indicando claramente, por criticidade, o tempo de resolução e os procedimentos de correção;
- Detecção e Tratamento dos erros e exceções ocorridos durante o acesso a qualquer componente externo ao sistema, por exemplo, banco de dados e webservices;
- Permitir pesquisas por quaisquer das informações armazenadas nos registros (logs), apresentando, no mínimo, usuário, data, hora, estação de trabalho (IP e agente do navegador), alterações e consultas efetuadas;

- 2.3.90. A SOLUÇÃO possui, de forma documentada, processos de gestão de continuidade de negócios, em conformidade com a ISO 22301/2019, incluindo os planos de continuidade de negócios, plano de comunicação, e o plano de recuperação em caso de desastre, além de estabelecer procedimentos de recuperação e de restauração da plataforma, infraestrutura, aplicações e dados após incidente de perda de dados ou falha na disponibilidade dos serviços contratados;
- 2.3.91. A SOLUÇÃO estabelece um canal de comunicação seguro utilizando, no mínimo, os protocolos de segurança do tipo IPsec/IKE e Transport Layer Security TLS versão 1.2 ou superior;
- 2.3.92. A SOLUÇÃO utilizar padrão de encriptação seguro, que possa ser implementado com chaves de encriptação geradas e armazenadas pelo órgão ou pela entidade, no mínimo, AES (criptografia simétrica), SHA-2 (hash) e ECC (criptografia de curva elíptica). Os módulos de criptografia usados pela aplicação devem ser compatíveis com o padrão FIPS 140-2 ou padrão equivalente;
- 2.3.93. No caso de Cloud ou SaaS, o datacenter possui mecanismos que permitam, no mínimo, quanto à segurança:
- Possuir sistema de Firewalls operando em cluster no modo “ativo/ativo” com distribuição de carga entre links de comunicação e atuando como contingência entre eles, com chaveamento automático de conexões ativas em casos de falhas críticas em um dos equipamentos. O Firewall deve ainda possuir capacidade de filtragem de pacotes, recurso para uso de banda com criptografia, suporte para túneis VPN, suporte para implementação de vLans;
 - Possuir sistema de prevenção de ataques (IPS – Intrusion Prevention System) no nível de borda da rede, com gerenciamento ativo e características de interações automatizadas com sistemas de firewall;
 - Possuir equipe de monitoramento e resposta a incidentes de segurança da informação e cibernética, 24 horas, 7 dias por semana, 365 dias por ano, com procedimentos formalizados, incluindo tempos de resposta, e passíveis de compartilhamento e alinhamento com o grupo de resposta a incidentes de segurança do Banco;
- 2.3.94. Possui procedimentos mínimos, em relação ao descarte de ativos de informação e de dados, que assegurem:
- Sanitizar ou destruir, de modo seguro, os dados pertencentes ao Banco existentes nos dispositivos descartados por meio da utilização de métodos que estejam em conformidade com os padrões estabelecidos para a conduta e as melhores práticas;
 - Destruir, de modo seguro, ativo de informação que contenham dados pertencentes ao Banco, no fim do ciclo de vida ou considerado inservível, com o fornecimento de um Certificado de Destruição de Equipamento Eletrônico (Certificate of Electronic Equipment Destruction - CEED) e discriminar os ativos que foram reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição;
 - Armazenar, de modo seguro, ativos de informação que contenham dados do Banco a serem descartados, em ambiente com acesso físico controlado, com registro de toda movimentação de entrada e de saída de dispositivos.

- 2.3.95. Possui procedimentos necessários para a preservação de evidências, com a possibilidade de uso em tribunais e no devido processo legal;
- 2.3.96. A SOLUÇÃO está em conformidade com os padrões de segurança de nuvem, por meio de auditoria anual Service and Organization Controls 2 (SOC 2), conduzida por um auditor independente, com a apresentação dos relatórios de tipo I e tipo II;
- 2.3.97. A SOLUÇÃO está em conformidade com os requisitos estabelecidos na Resolução CMN 4.893/21;
- 2.3.98. Os dados armazenados (ou em trânsito) no provedor devem estar criptografados e o esquema criptográfico adequado à classificação das informações e considerado como aceitável e seguro pelo mercado. As chaves criptográficas utilizadas devem estar de posse exclusiva do Banco;
- 2.3.99. A SOLUÇÃO possui interface Web compatível com os navegadores mais utilizados no mercado, sendo eles: versões mais recentes do Firefox, Chrome e Edge;
- 2.3.100. A SOLUÇÃO possui regras implementadas relacionadas à validação de dados, tais como: Caracteres inválidos; Informações incompletas, Informações excedendo limites pré-estabelecidos e Informações de controle inconsistentes (por exemplo: datas, cpf, dias da semana, dias do mês, ano, dígito verificador etc.);
- 2.3.101. A SOLUÇÃO permite gravação automática de trilhas de auditoria incluindo:
- Concessões de acesso, tentativas de acesso não autorizado, operações realizadas, autorizações concedidas, modificações e alterações nos dados, inclusive para eventos que modifiquem as permissões de acesso do usuário;
 - Registros configurados, a critério da área de negócio, que devem conter, no mínimo, as seguintes informações: - data e hora de início e fim do evento; - tipo do evento (consulta, inclusão, alteração, exclusão, logon, logout); - identificação do responsável; - identificação do aplicativo, tela ou função utilizados; - origem do evento (IP e/ou nome da máquina); - resultado final (sucesso ou falha); - detalhes do evento (informações adicionais sobre o evento significativos para análise das ocorrências);
 - Registros protegidos contra violação de confidencialidade e integridade, ou seja, somente ser possível sua consulta a usuários autorizados e não ser possível operações de alteração e exclusão;
 - Implementação de recursos de auditoria e tracking que permitam rastrear a origem do registro, que transformações sofreu e como foi carregado. A ferramenta provê log de execução dos processos com informações de data e hora de início e fim do evento, tipo do evento, resultado (sucesso ou falha) e detalhes do evento (informações adicionais sobre o evento, significativas para análise das ocorrências);
- 2.3.102. A SOLUÇÃO provê meios de garantir o sigilo no tráfego e no armazenamento da informação, pelo uso de criptografia, hash, e protocolos de transporte seguro, como: TLS 1.2 ou superior, https, ssl etc.;
- 2.3.103. A SOLUÇÃO suporta SSL 256 bits e superior para criptografia do canal de transmissão de dados e de informações trocadas entre servidores internos e externos;
- 2.3.104. Suporta autenticação por meio de protocolo OAuth com integração de ferramenta de SSO RedhatSSO/Keycloak 7.3 ou superior;
- 2.3.105. A SOLUÇÃO suporta a autenticação em múltiplos domínios federados de Active Directory do Windows Server 2008 e superior;

2.3.106. A SOLUÇÃO possui mecanismos que permitam a adoção da abordagem Security by Design (SbD), com vistas a garantir a segurança ao longo de todo o ciclo de vida da aplicação, incluindo a observância dos seguintes princípios:

- **Confidencialidade:** garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
- **Integridade:** garantia de que não haja comprometimento da exatidão e completeza da informação, seja acidental ou intencional, inclusive quanto à origem, trânsito e destino;
- **Disponibilidade:** garantia de que usuários, equipamentos ou aplicativos autorizados obtenham acesso à informação, aos ativos e recursos correspondentes, sempre que necessário;
- **Autenticidade:** garantia da correta identidade do responsável, seja usuário, equipamento ou aplicativo, pelo tratamento da informação;
- **Irretratabilidade (não repúdio):** garantia de que um usuário ou entidade não possa negar a autoria da informação fornecida;
- **Pertinência:** acesso ser restrito apenas aos usuários que necessitem da informação.

2.3.107. As informações manipuladas, armazenadas ou que transitem entre as funcionalidades da SOLUÇÃO são protegidas de acordo com sua classificação. A informação utilizada no Banco do Nordeste é classificada como:

- **Pública (ou ostensiva):** informação sem classificação, cujo acesso pode ser livre, uma vez que não possui conteúdo crítico para a instituição;
- **Reservada:** informação de conhecimento permitido apenas a um grupo de pessoas autorizadas, cuja revelação possa comprometer planos, operações ou objetivos neles previstos ou referidos;
- **Secreta:** informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da instituição, a assuntos de inteligência e a planos ou detalhes, programas ou instalações estratégicas, cujo conhecimento não autorizado possa acarretar dano grave à segurança do Banco do Nordeste, seus colaboradores, parceiros e clientes;
- As Informações reservadas, secretas, ou pessoais são consideradas sigilosas. As Informações previstas em legislação municipal, estadual ou federal, sobretudo aquelas relacionadas com regras de sigilo fiscal, bancário, de operações e serviços no mercado de capitais, comercial, profissional, industrial e segredo de justiça são também consideradas sigilosas;

2.3.108. A criação/revisão de perfis de acesso por usuário ou por grupo de usuários permite levar em consideração a estrutura organizacional da empresa;

2.3.109. A SOLUÇÃO permite delegar permissões (papéis e perfis de acesso) por período configurável;

2.3.110. A SOLUÇÃO permite a habilitação e a desabilitação automática de recursos e funcionalidades da aplicação (no mínimo, opções de menu, abas, campos, botões, ações como aprovação, exclusão e correlatos) de acordo com as permissões de acesso dos usuários;

2.3.111. A SOLUÇÃO provê mecanismo, de forma automática, para garantia de identidade, autenticidade e autorização de acesso de forma que cada usuário, ou grupo de usuários, possa acessar apenas a módulos, funcionalidades, transações, campos e

telas permitidas para o seu perfil de acesso, permitindo definição de perfis de utilização individuais e de grupos, com a possibilidade de diferenciar o controle de acesso dos usuários através de perfil, regras de negócio, alçadas e eventos funcionais;

- 2.3.112. A SOLUÇÃO possui controle de sessão que obrigue nova autenticação quando houver, pelo menos, perda de integridade de informações de controle de acesso, falha na comunicação com algum servidor ou aplicativo, e tempo limite sem atividade expirado;
- 2.3.113. A SOLUÇÃO possui mecanismos de integração com a infraestrutura de chaves públicas baseada em Microsoft Windows Server 2008 e superior;
- 2.3.114. A SOLUÇÃO possibilita o armazenamento de dados de forma dedicada (exclusiva, com acesso pessoal devidamente controlado) para a CONTRATANTE;
- 2.3.115. A SOLUÇÃO de integração com soluções de SIEM (Gerenciamento e Correlação de Eventos de Segurança) compatíveis com o RSA Netwitness;

3 Suporte e Treinamento

- 3.1 Possuir local centralizado com toda documentação atualizada do sistema para usuários finais, times de desenvolvimento e suporte operacional;
- 3.2 A documentação da API de integração com demais ferramentas do BNB deve ser clara, ampla e plena, de forma a listar e exemplificar todas as funcionalidades disponíveis na API;
- 3.3 Possuir programa de treinamento de usuários (usuários normais, administradores, mantenedores e desenvolvedores de aplicações integrantes). Caso positivo, informar escopo, objetivo, idiomas, quantidade máxima de alunos por turma e carga mínima;
- 3.4 A documentação técnica do sistema deve estar escrita nos idiomas: português do Brasil ou inglês;
- 3.5 O *help on-line* e manual do usuário estão escritos no idioma português do Brasil;
- 3.6 possuir processos bem definidos para tratativa de requisições e incidentes, com SLA, modelo de escalonamento e canais de comunicação com a CONTRATANTE;
- 3.7 possuir relatórios periódicos das requisições e incidentes, abertos e atendidos;
- 3.8 possuir atendimento e suporte 24x7 ao produto;
- 3.9 possuir equipes de suporte técnico e funcional da SOLUÇÃO. Caso positivo, listar os locais no Brasil onde existem, informando se a equipe é própria ou terceirizada;

4 Cronograma

Fase	Atividades	Atividades Macro	Tempo Estimado
1	Criação/Migração da Base de Dados		
2	Início do Projeto		
3	Implementação		

SILVIA KELLY SOARES BEZERRA

Gerente de Ambiente em exercício

Ambiente de Distribuição e Suporte de Fundos de Investimento