DESCRIÇÃO DOS SERVIÇOS

As informações contidas neste Anexo descrevem os requisitos não funcionais para contratação da solução tecnológica especializada, oferecida na modalidade Software como Serviço (SaaS), que contempla a distribuição de classes e subclasses de fundos de investimento próprias e de terceiros — inclusive por conta e ordem —, a controladoria do passivo de cotas de classes e subclasses de fundos de investimento, e o atendimento às exigências dos órgãos reguladores e autorreguladores

Os requisitos não funcionais especificados neste documento têm caráter obrigatório, devendo ser rigorosamente atendidos pela Contratada. O não atendimento a qualquer das exigências desclassifica a proposta da Contratada.

ANEXO III - REQUISITOS NÃO FUNCIONAIS

1. Grupo de requisitos: GERAIS		
Item	**Descrição do requisito**	**Validação Técnica de Requisitos, Necessário?**
1.1.	A SOLUÇÃO deve disponibilizar APIs que permitam integração do sistema com soluções externas complementares;	X
1.2.	A SOLUÇÃO deve, em caso de término de contrato de uso, possibilitar a portabilidade de todos os dados armazenados ao longo da utilização pela CONTRATANTE;	
1.2.1	a) No encerramento do Contrato, independentemente do fato que motivou sua extinção, a CONTRATADA deverá realizar a transferência dos dados, documentação técnica da solução, da estrutura de dados, do conhecimento, integrações e das customizações através de meios adequados e em consonância com anexos do Edital.	X
1.2.2	b) Suporte à Migração: prestar suporte técnico ativo durante o processo de transição, incluindo reuniões técnicas, exportação assistida e validação de integridade dos dados.	
1.2.3	c) Notificar antecipadamente: o fornecedor deve comunicar com antecedência mínima de 180 dias no caso de qualquer intenção de descontinuidade do serviço permitindo ao BNB tempo para iniciar o plano de migração.	
1.2.4	d) Plano de continuidade do negócio: o fornecedor deve apresentar um plano formal de continuidade, o que inclui possíveis cenários de falha, como efetuar a recuperação e fornecimento de suporte técnico na migração assistida para outro ambiente ou fornecedor.	X
1.2.5	e) Para o caso de encerramento contratual, inclusive falência do fornecedor: todos os dados do Banco serão entregues em formato aberto/conhecido e estruturado, com o dicionário de dados, além da documentação técnica e os referentes às customizações, incluindo ainda suporte técnico para migração por um período mínimo 180 dias ou conforme o planejamento de migração, sem custos adicionais.	X
1.3.	A SOLUÇÃO deve possuir ferramenta para desenvolvimento de customização de produtos, APIs ou funcionalidades sem interferência do fornecedor;	X
1.4.	A SOLUÇÃO deve permitir 5 (cinco) anos de persistência dos dados para temas legais, regulatórios e autorregulatórios;	X
1.5.	A SOLUÇÃO deve possibilitar que sejam configuradas ROLE padrão para novos usuários cadastrados;	X
1.6.	A SOLUÇÃO deve permitir configuração feita através de interface WEB administrativa única;	X
1.7.	A SOLUÇÃO deve dar visibilidade fim a fim de todas as transações, incluindo as malsucedidas;	X
1.8.	A SOLUÇÃO deve possuir controle de vigência dos registros de qualquer tabela de dados para possibilitar as consultas de histórico;	
1.9.	A SOLUÇÃO deve possuir mecanismo de migração dos dados (Importar/Exportar massivamente);	X
1.10.	A SOLUÇÃO deve disponibilizar testes automatizados que garantam o Core da aplicação;	X
1.11.	A SOLUÇÃO deve permitir automação de deploy (CI/CD) continuous deployment;	

1.12.	A SOLUÇÃO deve possuir local centralizado com toda documentação atualizada do sistema para uso pelos usuários finais;	X
1.13.	A SOLUÇÃO deve possuir local centralizado com toda documentação técnica atualizada do sistema para usuários finais, times de desenvolvimento e suporte operacional;	X
1.14.	A SOLUÇÃO deve possuir 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;	X
1.15.	A SOLUÇÃO deve possuir 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;	X
1.16.	A SOLUÇÃO deve possuir banco de dados padronizado quanto à nomenclatura dos objetos (tabelas, colunas, funções, gatilhos, visões etc.);	X
1.17.	Todas as tabelas da SOLUÇÃO devem possuir chave primária ou chave única;	X
1.18.	O banco de dados da SOLUÇÃO deve possuir índices nos objetos que são alvo das principais consultas das rotinas da aplicação e nos campos que fazem referência a outras tabelas;	X
1.19.	O banco de dados da SOLUÇÃO está estruturado de forma a evitar a redundância de tabelas;	
1.20.	O dono (owner) dos objetos do banco de dados da SOLUÇÃO deverá ser o superusuário. O usuário de conexão da SOLUÇÃO (aplicação) somente tem permissões de DML (Data Manipulation Language) nos objetos do banco de dados;	X
1.21.	A SOLUÇÃO deve permitir a configuração e execução de procedimentos para eliminação de dados históricos, sob controle rígido de permissões de acesso e registro em log de auditoria;	X
1.22.	Todas as versões de softwares básicos, frameworks, servidores e quaisquer outros recursos utilizados pela SOLUÇÃO deverão ser compatíveis com o ambiente computacional do Banco do Nordeste;	
1.23.	A SOLUÇÃO deve garantir 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;	X
1.24.	A documentação técnica da SOLUÇÃO deve estar escrita nos idiomas: português do Brasil ou inglês;	X
1.25.	O help on-line e manual do usuário deverão estar escritos no idioma português do Brasil;	X
1.26.	A SOLUÇÃO deve utilizar e apresentar mensagens e telas no idioma português do Brasil;	X
1.27.	A SOLUÇÃO deve permitir que a identidade visual do BANCO possa ser configurada em seus relatórios e documentos de forma nativa ou personalizada;	X
1.28.	A SOLUÇÃO deve permitir integração com as ferramentas de BI (Business Intelligence) do BANCO, tais como: PowerBI e IBM DataStage;	X
1.29.	A SOLUÇÃO deve permitir 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;	X
1.30.	A SOLUÇÃO deve permitir trabalhar a qualidade dos dados: oferecer mecanismos para tratamento de registros rejeitados ou que estejam fora do padrão esperado;	X

1.31.	A SOLUÇÃO deve permitir exportar uma visão de relatório/consulta para diferentes formatos (TXT, HTML, DOC/DOCX, XLS/XLSX, CSV, XML, ODT, ODS, PDF, ENTRE OUTROS);	X
1.32.	A SOLUÇÃO deve permitir acesso aos dados transacionais de forma on-line para a construção de relatórios/consultas;	X
1.33.	A SOLUÇÃO deve permitir compor dados de diversas fontes (módulos da SOLUÇÃO, sistemas legados, fontes externas) para criação de relatórios/consultas;	X
1.34.	Os módulos da SOLUÇÃO devem apresentar integração entre si, de forma única e nativa;	
1.35.	A SOLUÇÃO deve, preferencialmente, prover arquitetura baseada em micros serviços na construção das integrações entre seus módulos, sistemas legados e sistemas externos;	
1.36.	A SOLUÇÃO deve suportar integrações através de APIs/REST;	X
1.37.	A SOLUÇÃO deve suportar integrações através de serviços web/SOAP;	X
1.38.	A SOLUÇÃO deve suportar integrações com Webpshere Message Broker;	X
1.39.	A SOLUÇÃO deve suportar integrações para envio e recebimento de mensagens de filas com MQSeries;	X
1.40.	A SOLUÇÃO deve permitir reiniciar um processo de carga de onde parou, sem a necessidade de codificar essa inteligência;	X
1.41.	A SOLUÇÃO deve prover recursos de paralelização de processos de carga e processamento de grande volume de dados;	
1.42.	A SOLUÇÃO deve possuir capacidade de reaproveitar as parametrizações efetuadas anteriormente, na implantação de novas versões;	X
1.43.	A SOLUÇÃO deve possuir 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);	
1.44.	A SOLUÇÃO deve possibilitar o monitoramento e rastreamento de mensagens técnicas como mensagens de erros, eventos, transações executadas, entre outras (a partir da camada de aplicação);	X
1.45.	A SOLUÇÃO deve prover interface responsiva com suporte às plataformas móveis principais (Android e iOS), em smartphones e tablets para integração com Internet e Mobile Banking;	
1.46.	A interface da SOLUÇÃO deve ser intuitiva, clara, direta e de fácil assimilação por qualquer tipo de usuário;	X
1.47.	A SOLUÇÃO deve permitir que as informações sejam exibidas em tela antes de sua impressão ou armazenamento;	X
1.48.	Para utilização no backoffice, a SOLUÇÃO deve disponibilizar aplicação web ou desktop que pode ser customizada;	X
1.49.	A SOLUÇÃO deve possibilitar customizações (front-end e/ou back-end), via desenvolvimento de extensões para atender necessidades específicas;	X
1.50.	A CONTRATANTE pode realizar customizações do produto com equipe interna, sem obrigatoriedade de contratação de fornecedor ou empresa parceira;	
1.51.	O Fornecedor deve disponibilizar documentação detalhada da SOLUÇÃO e arquitetura de software, dados, infra, rede, segurança, e plano de implantação inicial;	

1.52.	A SOLUÇÃO deve possuir 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;	
1.53.	A SOLUÇÃO deve disponibilizar recurso de controle e rollback de versões;	X
1.54.	A SOLUÇÃO deve possuir processos bem definidos para tratativa de requisições e incidentes, com SLA, modelo de escalonamento e canais de comunicação com a CONTRATANTE;	X
1.55.	A SOLUÇÃO deve possuir relatórios periódicos das requisições e incidentes, abertos e atendidos;	X
1.56.	A SOLUÇÃO deve possuir atendimento e suporte ao produto em horário comercial, ou 24x7 caso a solução tenha processamento batch em outro horário;	X
1.57.	A SOLUÇÃO deve possuir equipes de suporte técnico e funcional. Caso positivo, listar os locais no Brasil onde existem, informando se a equipe é própria ou terceirizada;	X
1.58.	A SOLUÇÃO deve disponibilizar 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;	X
1.59.	A SOLUÇÃO deve disponibilizar mecanismos para o administrador de sistema confirmar que as integrações (independente da técnica: API, ETL. etc.) estão com erro e precisam ser reenviadas (conciliação de integrações);	X
1.60.	Todas as versões de softwares básicos, frameworks, servidores e quaisquer outros recursos utilizados pela Solução deverão ser totalmente providos em infraestrutura SaaS.	X
1.61.	A Solução deve apresentar conformidade com a norma 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 esses serviços ou, alternativamente, demonstrar atender os objetivos e controles da referida norma, mediante apresentação de políticas, procedimentos, e outros documentos. Qualquer documento deverá ser apresentado em nome do provedor, sendo facultado ao CONTRATANTE promover diligência destinada a esclarecer ou complementar	
1.62.	A SOLUÇÃO deve suportar redundância geográfica e alta disponibilidade;	X
1.63.	A CONTRATADA manterá redundância geográfica em regiões distintas dentro do território nacional;	X
1.64.	Os ambientes de produção e contingência deverão estar logicamente segregados e sujeitos a controles de segurança equivalentes.	X
1.65.	A SOLUÇÃO deve possuir tratamento para diferentes fusos horários e horários de verão;	
1.66.	A SOLUÇÃO deve possuir dicionário de falhas / Códigos de erro;	X
1.67.	A SOLUÇÃO deve permitir integração à gestão e à governança de acesso compatíveis com Azure AD, SAML, OATH 2;	X
1.68.	Todos os módulos que compõem a SOLUÇÃO devem ser compatíveis com o ambiente computacional do BANCO;	
1.69.	A SOLUÇÃO deve suportar a utilização de mecanismos de “data sharing”, com balanceamento de carga entre servidores de banco de dados distintos;	
1.70.	A SOLUÇÃO deve possibilitar o uso de infraestrutura de clusters locais ou geograficamente dispersos em todos os seus componentes;	X

1.71.	Em caso de rotinas batch necessárias ao funcionamento, a SOLUÇÃO deve ser compatível com gerenciamento pela ferramenta BMC Control-M de scheduling e gerenciamento de processamentos batch do BNB;	
1.72.	A SOLUÇÃO deve possibilitar monitoramento das informações de consultas e sessões e definição de gatilhos para identificar consultas com baixo desempenho ou consumo excessivo de recursos;	
1.73.	A SOLUÇÃO deve possuir 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;	
1.74.	A SOLUÇÃO deve suportar 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);	X
1.75.	A SOLUÇÃO deve possuir 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;	
1.76.	A SOLUÇÃO deve possibilitar 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);	X
1.77.	O fornecedor deve se responsabilizar pelas manutenções legais, regulatórias e de autorregulação, dentro dos prazos exigidos pelos órgãos reguladores e autorreguladores brasileiros;	
1.78.	A SOLUÇÃO deve disponibilizar mecanismo seguro para alteração (criação/remoção/atualização/leitura) de dados;	
1.79.	A SOLUÇÃO deve disponibilizar interface para que sejam auditados todos os eventos de acessos, consultas e demais operações aos dados disponibilizados pela ferramenta;	X
1.80.	A SOLUÇÃO deve implementar controles de segurança baseados, no mínimo, no NIST e da série ISO27000;	
1.81.	A autenticação dos usuários e clientes deve seguir boas práticas e os padrões mais elevados de Segurança Cibernética (Padrões de senha, expiração, MFA (para administradores e casos específicos);	X
1.82.	A SOLUÇÃO deve assegurar 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;	X
1.83.	A CONTRATADA compromete-se a armazenar e processar os dados da CONTRATANTE em território nacional, em infraestrutura de nuvem ou data center em conformidade com as exigências do Banco Central do Brasil e da Autoridade Nacional de Proteção de Dados (ANPD).	X
1.84.	A SOLUÇÃO deve implementar procedimentos para fortalecimento dos mecanismos de virtualização, que incluam, no mínimo:	
1.84.1	a) Desabilitar ou remover todas as interfaces, portas, dispositivos ou serviços desnecessários executados pelo sistema operacional;	
1.84.2	b) Configurar com segurança todas as interfaces de rede e áreas de armazenamento virtuais;	
1.84.3	c) Manter todos os sistemas operacionais e as aplicações em execução na máquina virtual em suas versões mais atuais;	X
1.84.4	d) Validar a integridade das operações de gerenciamento de chaves criptográficas;	
1.85.	A SOLUÇÃO deve dispor de mecanismo de autenticação que:	
1.85.1	a) Exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso;	X

1.85.2	b) Suporta tecnologia single sign-on, LDAP, SAML, OAuth para autenticação;	X
1.85.3	c) 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; i. Permite ao Banco gerenciar as próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido;	X
1.85.4	d) Guarda conformidade legal em seus processos de autenticação, controle de acesso, contabilidade e de registro (formato, retenção e acesso);	
1.86.	A SOLUÇÃO deve implementar soluções e procedimentos para garantir a segurança de aplicações web disponibilizadas no ambiente de nuvem, incluindo, no mínimo:	
1.86.1	a) 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;	
1.86.2	b) A verificação e validação de dados de entrada garantindo a 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: i. Entrada duplicada; ii. Valores fora de faixa; iii. Caracteres inválidos em campos de dados; iv. Dados incompletos ou faltantes; v. Comprimento de dados não respeitando limites superiores ou inferiores;	x
1.86.3	c) Realizar, no mínimo, anualmente, testes de penetração de redes e de aplicações;	x
1.86.4	d) Implementar programa de correção de vulnerabilidades, indicando claramente, por criticidade, o tempo de resolução e os procedimentos de correção;	
1.86.5	e) Detecção e Tratamento dos erros e exceções ocorridos durante o acesso a qualquer componente externo ao sistema, por exemplo, banco de dados e webservices;	
1.86.6	f) 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;	x
1.87.	A SOLUÇÃO deve possuir, 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;	x
1.87.1	a) Os planos deverão cobrir, no mínimo: i. eventos de indisponibilidade de data center, falhas de grande escala de rede, incidentes de segurança cibernética, desastre natural e indisponibilidade de terceiros críticos; ii. procedimentos de comunicação interna e externa — inclusive com a CONTRATANTE e órgãos reguladores; iii. estratégias de recuperação tecnológica, logística e operacional; iv. papéis e responsabilidades (incluindo substitutos);	x

	v. listas de contatos e instruções de escalonamento.	
1.88.	A SOLUÇÃO deve estabelecer 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;	x
1.89.	A SOLUÇÃO deve 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;	
1.90.	A entrega da solução em modelo SaaS deve garantir que o datacenter possui mecanismos que permitam, no mínimo, quanto à segurança:	
1.90.1	a) 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;	
1.90.2	b) 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;	
1.90.3	c) 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;	x
1.91.	A SOLUÇÃO deve possuir procedimentos mínimos, em relação ao descarte de ativos de informação e de dados, que assegurem:	
1.91.1	a) 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;	
1.91.2	b) 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	
1.92.	A SOLUÇÃO deve possuir procedimentos necessários para a preservação de evidências, com a possibilidade de uso em tribunais e no devido processo legal;	
1.93.	A SOLUÇÃO deve estar 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;	x
1.94.	A SOLUÇÃO deve estar em conformidade com os requisitos estabelecidos na Resolução CMN 4.893/21;	
1.95.	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;	
1.96.	A SOLUÇÃO deve possuir interface Web compatível com os navegadores mais utilizados no mercado, sendo eles: versões mais recentes do Firefox, Chrome e Edge;	x
1.97.	A SOLUÇÃO deve possuir 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.);	x

1.98.	A SOLUÇÃO deve permitir a gravação automática de trilhas de auditoria incluindo:	x
1.98.1	a) 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;	x
1.98.2	b) 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);	
1.98.3	c) 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;	x
1.98.4	d) 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);	
1.99.	A SOLUÇÃO deve permitir o registro, acompanhamento e execução de planos de ação para tratamento de não conformidades, incluindo a identificação da causa raiz, definição de ações corretivas, responsáveis, prazos e verificação de eficácia, conforme boas práticas de gestão da qualidade.	
1.100.	A SOLUÇÃO deve suportar a autenticação por meio de protocolo oAuth com integração de ferramenta de SSO RedhatSSO/Keycloak 7.3 ou superior;	
1.101.	A SOLUÇÃO deve suportar a autenticação em múltiplos domínios federados de Active Directory do Windows Server 2008 e superior;	
1.102.	A SOLUÇÃO deve possuir 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	
1.102.1	a) **Confidencialidade:** garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;	
1.102.2	b) **Integridade:** garantia de que não haja comprometimento da exatidão e completeza da informação, seja acidental ou intencional, inclusive quanto à origem, trânsito e destino;	
1.102.3	c) **Disponibilidade:** garantia de que usuários, equipamentos ou aplicativos autorizados obtenham acesso à informação, aos ativos e recursos correspondentes, sempre que necessário;	
1.102.4	d) **Autenticidade:** garantia da correta identidade do responsável, seja usuário, equipamento ou aplicativo, pelo tratamento da informação;	
1.102.5	e) **Irretratabilidade (não repúdio):** garantia de que um usuário ou entidade não possa negar a autoria da informação fornecida;	
1.102.6	f) **Pertinência:** acesso ser restrito apenas aos usuários que necessitem da informação.	
1.103.	As informações manipuladas, armazenadas ou que transitem entre as funcionalidades da SOLUÇÃO devem ser protegidas de acordo com sua classificação. A informação utilizada no Banco do Nordeste é classificada como:	
1.103.1	**a) Pública (ou ostensiva):** informação sem classificação, cujo acesso pode ser livre, uma vez que não possui conteúdo crítico para a instituição;	

1.103.2	**b) Reservada:** informação de conhecimento permitido apenas a um grupo de pessoas autorizadas, cuja revelação possa comprometer planos, operações ou objetivos neles previstos ou referidos;	
1.103.3	**c) 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;	
1.103.4	d) 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;	
1.104.	A criação/revisão de perfis de acesso por usuário ou por grupo de usuários deve considerar a estrutura organizacional da empresa;	x
1.105.	A SOLUÇÃO deve permitir delegar autorizações (papéis e perfis de acesso) por período configurável;	x
1.106.	A SOLUÇÃO deve permitir 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;	x
1.107.	A SOLUÇÃO deve prover 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;	x
1.108.	A SOLUÇÃO deve possuir 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;	x
1.109.	A SOLUÇÃO deve possuir mecanismos de integração com a infraestrutura de chaves públicas baseada em Microsoft Windows Server 2008 e superior;	
1.110.	A SOLUÇÃO deve possibilitar o armazenamento de dados de forma dedicada (exclusiva, com acesso pessoal devidamente controlado) para a CONTRATANTE;	x
1.111.	A SOLUÇÃO deve permitir a integração com soluções de SIEM (Gerenciamento e Correlação de Eventos de Segurança) compatíveis com o RSA Netwitness.	
1.112.	A SOLUÇÃO deve estar em conformidade com legislações e regulamentações nacional vigente.	
1.113.	A SOLUÇÃO deve ter no mínimo 2 atualizações anuais.	
1.114.	A SOLUÇÃO deve ser adequada às normas do Banco Central, CVM, AMBIMA.	

2. Grupo de requisitos: USABILIDADE

Item	Descrição do requisito	Validação Técnica de Requisitos, Necessário?
2.1.	A Solução deverá disponibilizar manuais para o usuário final, help on line, manual do administrador e manuais técnicos escrito em língua portuguesa do Brasil.	x
2.2.	Fornecer valores default para campos necessários (obrigatórios).	x
2.3.	A interface da Solução deve ser intuitiva, clara, direta e de fácil assimilação por qualquer tipo de usuário.	x
2.4.	Oferecer recursos visuais/gráficos que permitam a análise de informações disponibilizadas pela Solução.	
2.5.	A Solução deve exibir apenas a informação relevante ao contexto corrente, de forma que o usuário não necessite procurar, no meio de muitos dados, o que precisa para executar sua tarefa.	
2.8.	A Solução deve permitir que o usuário selecione, de forma visual e parametrizável, os campos que deverão ser exibidos ou ocultados nas telas que serão acessadas por estes usuários.	x
2.9.	Os formulários extensos, ou seja, maiores do que a parte visível da tela, deverão estar organizados em ficheiros, abas ou seções ocultáveis de forma a reduzir ou eliminar a rolagem vertical das páginas.	x
2.11.	As consultas de informações operacionais e gerenciais, apresentadas em tela, devem possuir a disponibilidade de impressão como relatório PDF e exportação para arquivos pdf, xls, csv ou txt.	x
2.13.	A Solução deverá possuir mecanismos de importação e exportação de dados em massa.	
2.14.	A interface deve ser responsiva, perceptível, operável, compreensível e robusta para todos os usuários.	

3. Grupo de requisitos: CONFIABILIDADE

Item	Descrição do requisito	Validação Técnica de Requisitos, Necessário?
3.1.	A Solução deverá registrar em log transacional, em tabela específica, toda operação que reflita modificação das informações do banco de dados, armazenando as informações antes e depois de alteradas e a identificação do usuário responsável, bem como data e hora.	
3.2.	A Solução deverá registrar em log específico em tabela, com data/hora de envio, destinatário, mensagem e tipo (e-mail, sms, whatsapp etc) de todos as mensagens de alertas enviadas pelo sistema.	

4. Grupo de requisitos: ACESSIBILIDADE		
Item	**Descrição do requisito**	**Validação Técnica de Requisitos, Necessário?**
4.1.	A Solução deve ter navegabilidade limpa e intuitiva, com a possibilidade de visualizar o processo inteiro em uma única tela.	x

5. Grupo de requisitos: COMPATIBILIDADE COM AMBIENTE COMPUTACIONAL DO BANCO		
Item	**Descrição do requisito**	**Validação Técnica de Requisitos, Necessário?**
5.6.	Permitir 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.	x

6. Grupo de requisitos: PROTEÇÃO DE DADOS		
Item	**Descrição do requisito**	**Validação Técnica de Requisitos, Necessário?**
6.1.	A Solução deve apresentar conformidade com a norma 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 esses serviços ou, alternativamente, demonstrar atender os objetivos e controles da referida norma, mediante apresentação de políticas, procedimentos, e outros documentos. Qualquer documento deverá ser apresentado em nome do provedor, sendo facultado ao BANCO promover diligência destinada a esclarecer ou complementar informações.	X
6.3.	A Solução deve prover mecanismo de acesso protegido aos dados, por meio de comunicação criptografada, garantindo que apenas aplicações e usuários autorizados tenham acesso.	

6.4.	A Solução deve atestar informações referentes a medidas adotadas em proteção de dados pessoais, devendo ser capaz de demonstrar: a) diretrizes de tratamento; b) 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; c) medidas protetivas para garantia da confidencialidade dos dados pessoais; 4 medidas protetivas durante as comunicações com o BANCO; d) registro de atividades de tratamento de dados pessoais; e) solicitação de autorização na subcontratação de terceiros para atividades de tratamento de dados pessoais; f) medidas de devolução / descarte dos dados; g) suportar autenticação dos usuários via LDAP com Microsoft Active Directory- 9 desenvolvimento do código web em conformidade com as melhores práticas e normas correlatas de codificação segura, seguindo princípios de Privacy by Design e Privacy by Default, em toda a solução, considerando que dados mínimos devem seguir as definições de tratamento de dados pessoais instituídas pela Lei Geral de Proteção de Dados Pessoais (LGPD).	
6.5.	Todos os dados sensíveis devem ser criptografados em repouso e em trânsito.	
6.6.	A solução deve estar em conformidade com a Lei nº 13.709/2018 (LGPD), garantindo a proteção de dados pessoais dos usuários, incluindo mecanismos de consentimento, controle de acesso, anonimização, rastreabilidade e exclusão de dados conforme previsto na legislação vigente.	
6.7.	O sistema deve implementar mecanismos automatizados, configuráveis e auditáveis para exclusão de dados pessoais, com base em critérios como fim da finalidade, solicitação do titular ou determinação legal.	
6.8.	A CONTRATADA atuará, conforme o caso, como operadora do conjunto dos dados pessoais tratados no âmbito da SOLUÇÃO, cabendo à CONTRATANTE a definição das finalidades e das bases legais para o tratamento. a) Tratar os dados pessoais exclusivamente nos termos e para os fins estabelecidos pela CONTRATANTE; b) Garantir o cumprimento dos princípios da LGPD (art. 6º), incluindo finalidade, necessidade, transparência, segurança e prevenção; c) Manter controles técnicos e organizacionais compatíveis com o risco, incluindo: criptografia, autenticação forte, logging seguro, controle de acesso baseado em perfil, segregação de ambientes e hardening de sistemas; d) Apoiar a CONTRATANTE no cumprimento dos direitos dos titulares previstos nos arts. 18 a 20 da LGPD (acesso, portabilidade, anonimização, exclusão, revogação de consentimento etc.); e) Notificar a CONTRATANTE sobre qualquer incidente de segurança com dados pessoais em até 2 (duas) horas após sua detecção, contendo informações mínimas previstas na LGPD art. 48 §1º.	

7. Grupo de requisitos: SEGURANÇA

Item	Descrição do requisito	Validação Técnica de Requisitos, Necessário?
7.1.	Utilizar tecnologia de autenticação multifator (MFA).	X
7.2.	Permitir detecção antifraude em todas as etapas do processo.	
7.3.	Detecção de Anomalias em transações em tempo real.	
7.4.	Cruzamento Inteligente de Dados (Com bases de dados internas e externas, listas de fraudes)	

8. Grupo de requisitos: AUDITORIA

Item	Descrição do requisito	Validação Técnica de Requisitos, Necessário?
8.1.	A solução deve permitir o registro e a rastreabilidade de todos os eventos e ações realizadas pelos usuários no sistema, incluindo data, hora, identificação do usuário, tipo de ação executada e contexto da operação, com o objetivo de garantir auditoria, segurança e conformidade com normas regulatórias.	X
8.2.	A solução deve permitir o registro, acompanhamento e execução de planos de ação para tratamento de não conformidades, incluindo a identificação da causa raiz, definição de ações corretivas, responsáveis, prazos e verificação de eficácia, conforme boas práticas de gestão da qualidade.	

9. Grupo de requisitos: INFRAESTRUTURA

Item	Descrição do requisito	Validação Técnica de Requisitos, Necessário?
9.1	Ambiente Exclusivo e Isolado: a) Fornecer infraestrutura dedicada ao contratante, com isolamento lógico dos recursos computacionais. b) Permitir a criação de ambientes segregados (ex: produção e homologação).	X
9.3	Escalabilidade e Elasticidade: a) Fornecer capacidade de escalabilidade vertical e horizontal dos recursos computacionais sob demanda, com mínima intervenção manual.	X

	b) Suportar políticas de auto escalonamento de recursos com base em métricas de uso. c) Suportar expansão modular da infraestrutura física (scale-out) d) Suporte a um crescimento de usuários e volume de dados sem degradação de desempenho	
9.4	Alta Disponibilidade e Continuidade: a) Garantir infraestrutura com tolerância a falhas e SLA mínimo de 99,74%. b) Disponibilizar mecanismos de failover automático e replicação de dados entre zonas de disponibilidade. c) Capacidade de processar picos de carga (ex: Fechamento de mês e semestre) d) Balanceamento de carga entre servidores	
9.5	Backup e Recuperação: a) Disponibilizar solução integrada de backup periódico automático, com retenção configurável. b) Disponibilizar funcionalidade para restauração granular de arquivos, volumes ou instâncias completas. c) O sistema deve implementar um mecanismo de expurgo automático de dados, permitindo a configuração do período de retenção das informações, com valor padrão parametrizável. Após esse período, os dados deverão ser permanentemente removidos do sistema, incluindo backups e arquivos de log, conforme as políticas de retenção definidas. d) O sistema deve permitir a parametrização dos tipos de dados a serem expurgados, possibilitando que diferentes categorias de informação (como dados pessoais, transacionais, logs de auditoria, entre outros) sejam incluídas ou excluídas do processo de expurgo, de acordo com as necessidades do negócio e requisitos legais.	x
9.6	Monitoramento e Auditoria: a) Prover ferramentas de monitoramento em tempo real de desempenho, disponibilidade e segurança. b) Gerar logs de auditoria com trilha completa de ações administrativas e operacionais. c) Proporcionar a criação e configuração de alertas automatizados em caso de falhas. (ex: SMS, Whatsapp etc.) d) Fornecer painéis de visualização (dashboards) personalizáveis. e) A solução deverá possuir mecanismo de monitoração com geração de logs, evento para armazenamento de dados históricos de desempenho, falhas e disponibilidade da solução como um todo e de suas principais funcionalidades e componentes, contemplando integração com a Solução de monitoração a ser definida pelo Contratante.	
9.10	Suporte a Ambientes Híbridos: a) Permitir integração com ambientes locais (on-premises) e outras nuvens públicas ou privadas. b) Suportar VPNs, redes privadas virtuais e conexões dedicadas.	X

10. Grupo de requisitos: PLANO DE CONTIGÊNCIA E TRANSIÇÃO DE SERVIÇOS		
Item	**Descrição do requisito**	**Validação Técnica de Requisitos, Necessário?**

10.1.	O plano de contingência deverá apresentar a estratégia e o método de trabalho da CONTRATADA para continuidade dos serviços, onde deverá constar, no mínimo, os seguintes tópicos: a) Identificação dos profissionais da CONTRATADA envolvidos na contingência, seus papéis e responsabilidades; b) Cronograma identificando as tarefas, recursos e marcos de referência; e c) Estruturas e atividades de gerenciamento da contingência e as regras propostas de relacionamento/atendimento da CONTRATADA.	X
10.2.	A CONTRATADA deverá assumir total responsabilidade pela continuidade dos serviços, garantindo que a CONTRATANTE não será prejudicada com qualquer esforço adicional requerido.	