Banco do Nordeste

ANEXO III
REQUISITOS NÃO FUNCIONAIS

1. FINALIDADE

As informações contidas neste Anexo descrevem os requisitos não funcionais para contratação de plataforma para gerenciamento e monitoração de correspondentes não bancários e sua infraestrutura em nuvem privada a ser instalada no contratante.

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

2. DISPOSIÇÕES GERAIS

2.1. A SOLUÇÃO deverá atender obrigatoriamente aos requisitos não funcionais descritos nos itens deste Anexo. Estes requisitos estão relacionados aos aspectos: Auditoria, Backup e Restore, Banco de dados, Compatibilidade, Consistência de dados, Desempenho, Disponibilidade, Documentação, Identidade Visual, Informações Gerenciais, Integração, Manutenibilidade (Atualização/Evolução), Job Scheduling, Monitoração, Segurança, Usabilidade, Workflow e Proteção de dados pessoais.

2.2. O documento de Especificações dos Requisitos Não Funcionais é composto das seguintes informações:

2.2.1. Requisito;

2.2.2. Descrição;

2.2.3. Atendimento;

2.2.4. Complexidade.

2.3. A coluna “Atendimento” deverá ser preenchida indicando a forma de atendimento do requisito não funcional, conforme abaixo:

2.3.1. **Provido com Standard,** identificada pelo número **1** (um): quando a SOLUÇÃO atender ao requisito suportado pelo código fonte da solução do próprio fabricante, podendo ser requeridas configurações não significativas ou não complexas, e que não afetem futuras atualizações.

1. Grupo de funcionalidades: ADMINISTRAÇÃO DE USUÁRIOS		
Cod. Requisito	**Descrição do requisito**	**PoC (Necessário?)**
1.1.	Permitir suporte a LDAP/SAML/OAuth / SSO	Sim
1.2.	O sistema deve suportar a existência de um usuário com perfil de super administrador responsável pela gestão de senhas e acessos de todos os usuários.	Sim
1.3.	Permitir a criação do usuário com perfil Fiscal de Contrato que possibilite a extração de relatórios gerenciais (PDF, XLS. CSV e TXT) de usuários licenciados na Solução (ativado, em uso, desativado, etc), usuários por módulos, sobre as funcionalidades do Sistema, definição de papéis e hierarquias, dentre outras funcionalidades gerenciais: a) Permitir acesso ao portal do CONTRATADO da SOLUÇÃO para o CONTRATANTE, para a verificação da situação das licenças da solução adquiridas no escopo do contrato	Sim
1.4.	Permitir integração (API, csv, xls e etc) entre plataformas para gestão de usuários (Ativos, Suspensos, Férias, e etc)	Sim
1.5.	Fornecer dashboard gerencial personalizável de gestão de usuários e licenças (Usuários ativos, em uso, desativado, usuários por módulo e etc)	
1.6	A solução deverá suportar, no mínimo, 8.110 (oito mil, cento e dez) usuários simultâneos, segregados nos perfis abaixo e quantidades mantendo os níveis de desempenho, segurança e auditoria exigidos: a) Consultor de Negócios, Corban Master e Subestabelecido: 8.000 (oito) mil licenças de uso; b) Agências Corban: 80 (oitenta) licenças de uso, e; c) Administrador: 30 (trinta) licenças de uso.	

2. Grupo de funcionalidades: USABILIDADE		
Cod. Requisito	**Descrição do requisito**	**PoC (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.	
2.2.	Utilizar e apresentar mensagens e telas no idioma português do Brasil.	Sim
2.3.	Fornecer valores default para campos necessários (obrigatórios).	Sim
2.4.	A interface da Solução deve ser intuitiva, clara, direta e de fácil assimilação por qualquer tipo de usuário.	Sim

2.5.	Oferecer recursos visuais/gráficos que permitam a análise de informações disponibilizadas pela Solução.	
2.6.	Permitir que as informações sejam exibidas em tela antes de sua impressão ou armazenamento.	
2.7.	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.	Sim
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.	Sim
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.	Sim
2.10.	A Solução deve apresentar uma interação flexível, que permite que o usuário controle o fluxo interativo. O usuário deve ser capaz de dispensar ações consideradas desnecessárias, alterar a ordem das ações e tratar os erros, sem necessitar sair do programa.	
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.	
2.12.	A Solução deverá ser acessada de forma responsiva em dispositivos móveis (smartphones, tablets, IOS e Android) e/ou possuir aplicativo específico.	Sim
2.13.	A Solução deverá possuir mecanismos de importação e exportação de dados em massa.	Sim
2.14.	A interface deve ser responsiva, perceptível, operável, compreensível e robusta para todos os usuários conforme as diretrizes WCAG (2.2. ou mais recente)	

3. Grupo de funcionalidades: CONFIABILIDADE		
Cod. Requisito	**Descrição do requisito**	**PoC (Necessário?)**
3.1.	A Solução deverá registrar em log transacional, em tabela específica, toda operação que reflita em 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.	Sim
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 funcionalidades: ACESSIBILIDADE		
Cod. Requisito	**Descrição do requisito**	**PoC (Necessário?)**
4.1.	A Solução deve ter navegabilidade limpa e intuitiva, com a possibilidade de visualizar o processo inteiro em uma única tela.	Sim

5. Grupo de funcionalidades: COMPATIBILIDADE COM AMBIENTE COMPUTACIONAL DO BANCO (On premise) –		
Cod. Requisito	**Descrição do requisito**	**PoC (Necessário?)**
5.1.	Todas as versões de softwares básicos, frameworks, servidores e quaisquer outros recursos utilizados pela Solução deverão ser totalmente providos em infraestrutura *On premise*.	Sim
5.2.	Deve possuir interface Web compatível com os navegadores mais utilizados no mercado, sendo eles: Microsoft Edge, Firefox e Chrome nas suas versões mais recentes.	Sim
5.3.	Todos os módulos que compõem a Solução devem ser compatíveis com os sistemas operacionais Windows 10 e superior e macOS Ventura ou superior, no lado cliente.	Sim
5.4.	Todos os módulos que compõem a Solução devem ser compatíveis com os sistemas operacionais Microsoft Windows Server 2019 e superior ou com a plataforma Linux Red Hat 8 e superior, no lado servidor.	Sim
5.5.	Os componentes da Solução que serão instalados em servidores deverão suportar a execução em ambiente virtualizado com VMWare vSphere 7.X e superior.	Sim
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.	Sim

6. Grupo de funcionalidades: PROTEÇÃO DE DADOS		
Cod. Requisito	**Descrição do requisito**	**PoC (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.	Sim

	Qualquer documento deverá ser apresentado em nome do provedor, sendo facultado ao BANCO promover diligência destinada a esclarecer ou complementar informações.	
6.2.	A Solução deve assegurar que no caso de solução SaaS, toda 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.	Sim
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.	Sim
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).	Sim
6.5.	Todos os dados sensíveis devem ser criptografados em repouso e em trânsito.	Sim
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.	Sim
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.	

7. Grupo de funcionalidades: SEGURANÇA		
Cod. Requisito	**Descrição do requisito**	**PoC (Necessário?)**
7.1.	Permitir assinatura digital que tenham validade jurídica em qualquer etapa do processo.	Sim
7.2.	Permitir reconhecimento facial dos clientes em qualquer parte do processo.	Sim

7.3.	Permitir a utilização da tecnologia de liveness detection (detecção de vida).	Sim
7.4.	Utilizar tecnologia de autenticação multifator (MFA).	Sim
7.5.	Permitir detecção antifraude em todas as etapas do processo.	Sim
7.6.	Detecção de Anomalias em transações em tempo real.	
7.7.	Cruzamento Inteligente de Dados (Com bases de dados internas e externas, listas de fraudes)	
7.8	Bloqueio automatizado de transações classificadas como alto risco e emissão de alerta	Sim

8. Grupo de funcionalidades: AUDITORIA		
Cod. Requisito	**Descrição do requisito**	**PoC (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.	Sim
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 funcionalidades: INFRAESTRUTURA		
Cod. Requisito	**Descrição do requisito**	**PoC (Necessário?)**
9.1	Ambiente Exclusivo e Isolado: a) Instalar nas dependências físicas do contratante. b) Fornecer infraestrutura dedicada ao contratante, com isolamento lógico e físico dos recursos computacionais. c) Permitir a criação de ambientes segregados (ex: produção, homologação, desenvolvimento).	Sim
9.2	Gerenciamento de Recursos:	

	a) Fornecer interface de gerenciamento (portal ou API) para provisionamento, monitoramento e controle de recursos (CPU, memória, armazenamento, rede). b) Suportar orquestração de máquinas virtuais, containers e redes virtuais.	
9.3	Escalabilidade e Elasticidade: a) Fornecer capacidade de escalabilidade vertical e horizontalmente dos recursos computacionais sob demanda, com mínima intervenção manual. 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	Sim
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) Deve suportar no mínimo 2.000 transações por minuto e até 50% da média móvel dos últimos 3 meses do total de transações realizadas, conforme política a ser definida d) Deve suportar até 50% dos usuários ativos na plataforma, conectados de forma simultânea, conforme política a ser definida e) Capacidade de processar picos de carga (ex: Fechamento de mês e semestre) f) Balanceamento de carga entre servidores	Sim, teste de estresse
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.	Sim
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.	Sim
9.7	Segurança e Controle de Acesso: a) Permitir integração com sistemas de identidade (ex: LDAP, AD, SAML). b) Controlar o acesso baseado em papéis (RBAC) e autenticação multifator (MFA). c) Criptografia de dados em repouso e em trânsito. d) Possuir certificados de segurança	Sim
9.8	Interoperabilidade e Portabilidade:	Sim

	a) Suportar padrões abertos (ex: OpenStack, Kubernetes, OVA/OVF). b) Permitir exportar dados e imagens de máquinas virtuais para outros ambientes.	
9.9	Conformidade Legal e Normativa: a) Atender à LGPD, à IN nº 5/2021 (Segurança da Informação) e à IN nº 94/2022 (Contratações de TIC). b) Estar em conformidade com a Resolução CMN nº 4.893/2021 para instituições financeiras	Sim
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.	Sim

10. Grupo de funcionalidades: GERAIS		
Cod. Requisito	**Descrição do requisito**	**PoC (Necessário?)**
10.1.	Conformidade com legislações e regulamentações nacional vigente.	
10.2.	A solução deve ter no mínimo 2 atualizações anuais.	
10.3.	Adequação às normas do Banco Central, CVM, SUSEP etc.	