1. Anexo III - Requisitos Técnicos e de Segurança

A SOLUÇÃO deverá atender obrigatoriamente aos requisitos não funcionais e às características técnicas descritos nos itens deste anexo. Os requisitos não funcionais e técnicos descritos a seguir atendem aos aspectos relacionados com segurança, desempenho, integração e infraestrutura.

1.1. REQUISITOS NÃO FUNCIONAIS & CARACTERÍSTICAS TÉCNICAS

Descrição do Requisito
GERAL
1.1.1. Todas as versões de softwares básicos, frameworks, servidores e quaisquer outros recursos utilizados pela solução deverão ser totalmente compatíveis com o ambiente computacional do Banco do Nordeste, conforme Anexo IV Ambiente Computacional do Banco do Nordeste.
1.1.2. Os componentes da SOLUÇÃO que serão instalados em servidores deverão suportar a execução em ambiente virtualizado com VMWare vSphere 5.5 e superior.
1.1.3. Os componentes da SOLUÇÃO de uso no ambiente Internet do Banco do Nordeste, que são acessados via navegador (browser) devem ser compatíveis com Internet Explorer 11.0 e superior, e com o Firefox 25 e superior.
1.1.4. A SOLUÇÃO deverá prover mecanismo de verificação, controle e atualização de versões nos aplicativos correspondentes aos módulos CAIXA, RETAGUARDA e ATM.
1.1.5. A SOLUÇÃO deve possuir integração entre todos os softwares ofertados;
1.1.6. A SOLUÇÃO deve possuir alta disponibilidade e escalabilidade, permitindo a implementação de clusters ativos com balanceamento de carga na própria solução;
DOCUMENTAÇÃO GERAL
1.1.7. Documentação descrevendo a Arquitetura da solução (diagrama de representação arquitetural; decomposição em subsistemas, pacotes ou camadas; configuração de hardware/software onde a aplicação será instalada).
1.1.8. Documentação descrevendo os procedimentos de instalação e atualização da solução (manual técnico de instalação e configuração).
1.1.9. Documentação descrevendo os procedimentos de administração da solução (manual do módulo de administração).
1.1.10. Manual de Utilização da Solução (Manual do Usuário) em Português.
1.1.11. Documentação descrevendo as configurações necessárias para garantir alta disponibilidade e performance baseado em cenários de quantidade máxima de sessões concorrentes.
USABILIDADE

1.1.12. O e manual do usuário deverão estar escritos no idioma Português do Brasil.
1.1.13. A documentação técnica do sistema deverá estar escrita nos idiomas Português do Brasil ou Inglês.
BANCO DE DADOS
1.1.14. A SOLUÇÃO deverá utilizar SGBD IBM DB2 for z/OS versão 10.1 como repositório de dados conforme disposto no Anexo IV – Ambiente Computacional do Banco do Nordeste.
SERVIDOR DE APLICAÇÃO
1.1.15. A solução deve ser compatível com o ambiente de execução de aplicação IBM WebSphere Application Server (WAS) for z/OS versão 7.x ou Microsoft Internet Information Services 7.x quando compatível com o ambiente computacional do Banco de acordo com o disposto no Anexo IV – Ambiente Computacional do Banco do Nordeste.
SEGURANÇA
1.1.16. A SOLUÇÃO deve possibilitar a autenticação dos usuários via LDAP utilizando repositório de usuários AD (Active Directory) do Windows Server 2008 e superior.
1.1.17. A SOLUÇÃO deve suportar a autenticação em múltiplos domínios federados de Active Directory do Windows Server 2008 e superior.
1.1.18. A SOLUÇÃO deve prover mecanismo para garantia de identidade, autenticidade e autorização de acesso de forma que cada usuário, ou grupo de usuários, possa acessar apenas as funcionalidades permitidas para o seu perfil de acesso.
AUDITORIA
1.1.19. A SOLUÇÃO deve gravar automaticamente trilhas de auditoria para controle de modificações e alterações nos dados, inclusive para eventos que modifiquem as permissões de acesso do usuário.
INTEGRAÇÃO
1.1.20. Caso a SOLUÇÃO possua a necessidade de integração por meio de arquivo com os sistemas do Banco do Nordeste, deverá fazê-lo por meio do sistema de mensageria IBM WebSphere MQ(MQSeries), respeitando o conteúdo do Anexo IV – Ambiente Computacional do Banco do Nordeste.
1.1.21. Caso a SOLUÇÃO possua rotina batch a mesma deverá ser compatível com o sistema de processamento e scheduling BMC Control-M, respeitando o conteúdo do Anexo IV – Ambiente Computacional do Banco do Nordeste.
1.1.22. Caso a SOLUÇÃO possua a necessidade de usar rotinas ETL, deverá fazê-lo por meio dos produtos da ferramenta IBM Cognos, respeitando o conteúdo do Anexo IV – Ambiente Computacional do Banco do Nordeste.
1.1.23. A SOLUÇÃO deverá possuir a capacidade para integrar-se ao IBM WebSphere Message Broker, respeitando o conteúdo do Anexo IV – Ambiente Computacional do Banco do Nordeste.

APLICATIVO DE INTERNET BANKING
1.1.24. A SOLUÇÃO deverá prover aplicativo para INTERNET BANKING.
1.1.25. O aplicativo de INTERNET BANKING deverá estar no idioma Português do Brasil.
1.1.26. O aplicativo de INTERNET BANKING deverá ser compatível com os principais navegadores do mercado, sendo eles Microsoft Internet Explorer 11 e superior, e Mozilla Firefox 25 e superior e Google Chrome 35 e superior de forma independente do sistema operacional utilizado pelo cliente.
1.1.27. O aplicativo de INTERNET BANKING deverá ser acessível pelos navegadores (browser) para smartphones e tablets Android 2.2 e superior e iOS 5 e superior e Windows Phone 8 e superior em
1.1.28. O aplicativo de INTERNET BANKING deverá possuir integração com o sistema de segurança G-Buster 3.14 e superior.
1.1.29. O aplicativo de INTERNET BANKING poderá fazer uso de mensagens SMS para notificações diretas aos clientes.
APLICATIVO DE MOBILE BANKING
1.1.30. A SOLUÇÃO deverá prover aplicativo para MOBILE BANKING.
1.1.31. O aplicativo de MOBILE BANKING deverá estar no idioma Português do Brasil.
1.1.32. O aplicativo de MOBILE BANKING deverá possuir cliente para tablets e smartphones com Android 2.2 e superior.
1.1.33. O aplicativo de MOBILE BANKING deverá possuir cliente para tablets e smartphones com iOS5 e superior.
1.1.34. O aplicativo de MOBILE BANKING deverá possuir integração com o sistema de segurança G-Buster 3.14 e superior.
1.1.35. O aplicativo de MOBILE BANKING deverá possuir recurso utilizar a câmera do dispositivo como leitor de código de barra.
1.1.36. O aplicativo de MOBILE BANKING deverá possuir recurso para exibição de mapas.
1.1.37. O aplicativo de MOBILE BANKING deverá possuir recurso para localização geográfica baseada no GPS do dispositivo.
APLICATIVO PARA TERMINAL DE AUTOATENDIMENTO (ATM)
1.1.38. A SOLUÇÃO deverá prover aplicativo para os terminais de AUTOATENDIMENTO.
1.1.39. O aplicativo de AUTOATENDIMENTO deverá estar no idioma Português do Brasil.
1.1.40. O aplicativo de AUTOATENDIMENTO deve ser suportada pelo fabricante para ser executada na plataforma operacional Microsoft Windows 7 e superior.
1.1.41. O aplicativo de AUTOATENDIMENTO deve ser suportada pelo fabricante para ser executada na plataforma operacional Red Hat Enterprise Linux 6 e superior.
1.1.42. O aplicativo de AUTOATENDIMENTO deve suportar o protocolo de acesso a dispositivos J/XFS ou XFS.
1.1.43. O aplicativo de AUTOATENDIMENTO deve acessar os dispositivos periféricos por meio do J/XFS ou XFS.
1.1.44. O aplicativo de AUTOATENDIMENTO deverá ser compatível com os equipamentos Perto TMF-4100 (em operação) e Dielbold ATM-4534C (em aquisição).
APLICATIVO PARA TERMINAL DE CAIXA (CAIXA)

1.1.45. A SOLUÇÃO deverá prover aplicativo para os terminais de CAIXA.
1.1.46. O aplicativo de CAIXA deverá estar no idioma Português do Brasil.
1.1.47. O aplicativo de CAIXA deve suportar o protocolo de acesso a dispositivos J/XFS ou XFS.
1.1.48. O aplicativo de CAIXA deve acessar os dispositivos periféricos por meio do J/XFS ou XFS.
1.1.49. O aplicativo de CAIXA deverá utilizar o Microsoft Active Directory como repositório de usuários.
1.1.50. Se o aplicativo de CAIXA for WEB deverá ser compatível com os principais navegadores de mercado, sendo eles Microsoft Internet Explorer 11 e superior, Mozilla Firefox 25 e superior e Google Chrome 35 e superior. Se o aplicativo de CAIXA for DESKTOP deverá ser compatível ou possuir versão especifica para as seguintes plataformas: a) Plataforma Operacional Microsoft Windows 7 e superior. b) Plataforma Operacional Red Hat Enterprise Linux 6 e superior.
1.1.51. O aplicativo de CAIXA deverá ser compatível com os equipamentos Diebold DT-9850 E Dielbold LS-5550.
APLICATIVO PARA TERMINAL DE RETAGUARDA (RETAGUARDA)
1.1.52. A SOLUÇÃO deverá prover aplicativo para os terminais de RETAGUARDA de agência.
1.1.53. O aplicativo de RETAGUARDA deverá estar no idioma Português do Brasil.
1.1.54. O aplicativo de RETAGUARDA deverá utilizar o Microsoft Active Directory como repositório de usuários.
1.1.55. Se o aplicativo de RETAGUARDA for WEB deverá ser compatível com os principais navegadores de mercado, sendo eles Microsoft Internet Explorer 11 e superior, Mozilla Firefox 25 e superior e Google Chrome 35 e superior. Se o aplicativo de RETAGUARDA for DESKTOP deverá ser compatível ou possuir versão especifica para as seguintes plataformas: a) Plataforma Operacional Microsoft Windows 7 e superior. b) Plataforma Operacional Red Hat Enterprise Linux 6 e superior.
BARRAMENTO DE INTEGRAÇÃO DE SERVIÇOS BANCÁRIOS (BARRAMENTO)
1.1.56. A SOLUÇÃO deverá prover um módulo para o BARRAMENTO de serviços bancários para centralização dos serviços bancários.
1.1.57. O BARRAMENTO deve ser compatível para instalação com o ambiente de execução de aplicação IBM WebSphere Application Server (WAS) for z/OS versão 7.x ou com o IBM Integration Bus (IIB) versão 9.x ou superior conforme o disposto no Anexo – Ambiente Computacional do BNB.
1.1.58. O BARRAMENTO deverá centralizar toda a comunicação entre os módulos da SOLUÇÃO.
1.1.59. O BARRAMENTO deverá possuir a capacidade para consumir dados contidos em SGBD IBM DB2 for z/OS versão 10.x.
1.1.60. O BARRAMENTO deverá possuir a capacidade para consumir dados contidos em SGBD Microsoft SQL Server 2008 / 2005 / 2000.
1.1.61. O BARRAMENTO deverá possuir a capacidade para consumir dados contidos em VSAM.

1.1.62. O BARRAMENTO deverá possuir a capacidade para consumir dados contidos em arquivos de texto (ASCII).
1.1.63. O BARRAMENTO deverá possuir procedimentos ou rotinas para importar e exportar as informações geradas para integração com outros sistemas.
1.1.64. O BARRAMENTO deverá possuir a capacidade para exportar informações em arquivo texto (ASCII).
1.1.65. O BARRAMENTO deverá possuir a capacidade para consumir dados contidos em arquivos de texto (ASCII).
1.1.66. O BARRAMENTO deverá permitir o consumo de mensagens no formato ISO8583.
1.1.67. O BARRAMENTO deverá permitir o provimento de mensagens no formato ISO8583.
1.1.68. O BARRAMENTO deverá possibilitar o consumo de mensagens provido pelo IBM WebSphere MQ(MQSerie), respeitando o conteúdo do Anexo IV – Ambiente Computacional do Banco do Nordeste.
1.1.69. O BARRAMENTO deverá permitir o provimento de dados por meio de WebServices Seguros com o WS-Security (Profile Username Token).
1.1.70. O BARRAMENTO deverá disponibilizar interface de WebServices compatíveis com SOAP 1.1 e 1.2 para que outras aplicações possam interagir com a solução.
1.1.71. O BARRAMENTO deverá possuir a capacidade para consumir dados contidos em Web Services com SOAP 1.1 e 1.2.
1.1.72. O BARRAMENTO deverá disponibilizar interface de WebServices Seguros com o WS-Security (Profile Username Token).
1.1.73. O BARRAMENTO deverá permitir o consumo de WebServices (SOAP).
1.1.74. O BARRAMENTO deverá permitir o consumo de WebServices Seguros com o WS-Security (Profile Username Token).
1.1.75. O BARRAMENTO deverá ser o centralizador e integrador da comunicação entre os módulos de canais da SOLUÇÃO.
1.1.76. Caso a solução possua a necessidade de integração por meio de arquivo com os sistemas do Banco do Nordeste, poderá fazer por meio do sistema de mensageria IBM WebSphere MQ(MQSeries), respeitando o conteúdo do Anexo IV – Ambiente Computacional do Banco do Nordeste.
1.1.77. Caso a solução possua rotina batch a mesma deverá ser compatível com o sistema de processamento e scheduling BMC Control-M, respeitando o conteúdo do Anexo IV – Ambiente Computacional do Banco do Nordeste.
MONITORAMENTO DA SOLUÇÃO (MONITOR)
1.1.78. A SOLUÇÃO deverá prover aplicativo para o monitoramento da solução.
1.1.79. A SOLUÇÃO de monitoramento deverá ser composta pelos módulos: a) Warehouse para centralização das informações b) Agentes para coleta das informações c) Console para visualização e manipulação das informações
1.1.80. O módulo de agentes de monitoramento deve ser compatível com o ambiente utilizado para os aplicativos da SOLUÇÃO, tais como o aplicativo de terminal de autoatendimento, o aplicativo de terminal de caixa, o aplicativo de retaguarda.

1.1.81. O módulo de warehouse deve ser compatível ou possuir versões específicas para a Plataforma Operacional Microsoft Windows 7 e superior, e Plataforma Operacional Red Hat Enterprise Linux 6 e superior
1.1.82. Se o módulo de console de monitoramento for WEB deverá ser compatível com os principais navegadores de mercado, sendo eles Microsoft Internet Explorer 11 e superior, Mozilla Firefox 25 e superior e Google Chrome 35 e superior. Se o módulo de console de monitoramento for DESKTOP deverá ser compatível ou possuir versão especifica para as seguintes plataformas: c) Plataforma Operacional Microsoft Windows 7 e superior. d) Plataforma Operacional Red Hat Enterprise Linux 6 e superior.
1.1.83. O módulo de console de monitoramento deverá estar no idioma Português do Brasil ou Inglês.
1.1.84. O módulo de console de monitoramente deve usar o repositório de usuários do Microsoft Active Directory.
1.1.85. O aplicativo de monitoramento deve ser capaz de monitorar o funcionamento dos equipamentos de AUTOATENDIMENTO (ATM).
SEGURANÇA
1.1.86. A SOLUÇÃO deve suportar a autenticação LDAP
1.1.87. A SOLUÇÃO deve suportar a autenticação em múltiplos domínios federados de Microsoft Active Directory e possibilitar que as permissões de acesso e uso de seus módulos sejam concedidas a usuários e grupos do domínio
1.1.88. A SOLUÇÃO deve permitir o controle de níveis de acesso com base em perfil de usuário e grupos de usuários, aplicável a todas suas funcionalidades.
1.1.89. A SOLUÇÃO deve implementar timeout em cada módulo e possuir mecanismo de timeout para logoff de usuários após determinado tempo de inatividade, a ser controlado por parâmetro.
1.1.90. A SOLUÇÃO deve permitir que os logs gerados possam vir a ser auditados por outras ferramentas.
1.1.91. A SOLUÇÃO deve permitir a adoção de mecanismos que asseguram a implementação de leitura de dispositivos do tipo token e smartcard, de forma que o logon e logoff de uma sessão sejam feito automaticamente com a inserção e remoção do dispositivo.
1.1.92. A SOLUÇÃO deve suportar criptografia entre o browser e o servidor Web, utilizando HTTPS/SSL.
1.1.93. A SOLUÇÃO deve disponibilizar recursos de criptografia para armazenamento de informações sigilosas na base de dados.
1.1.94. A SOLUÇÃO deve considerar a segurança nas integrações (interfaces) com outros sistemas a fim de evitar comprometimento das informações.
1.1.95. A SOLUÇÃO deve segregar seus módulos e funções, de modo a garantir proteção de acesso a dados e execução de funções baseado em perfis de usuários, e permitir a integração com política de permissão baseado em grupos do AD.
CONTROLE DE SESSÃO
1.1.96. A SOLUÇÃO, no caso de aplicação web, deve apresentar uma mensagem de erro e retornar à página inicial no caso de ocorrer perda da sessão.

1.1.97. Na ocorrência das situações abaixo, a SOLUÇÃO deve fechar a interface com o usuário ou outro sistema, obrigando nova autorização: a. Perda de integridade de informações de controle de acesso; b. Falha na comunicação com o servidor; c. Tempo limite sem atividade expirado.
TOLERÂNCIA A FALHAS
1.1.98. Quando ocorrer falha de comunicação envolvendo a SOLUÇÃO, ela deve permanecer em funcionamento, registrar essas falhas em log e exibir uma mensagem explicativa da falha ocorrida ao usuário e orientá-lo a fechar o aplicativo.
1.1.99. Quando ocorrer falha de comunicação com outros sistemas integrados, a SOLUÇÃO deve continuar em funcionamento, propiciando acesso às suas outras funções não relacionadas com a integração.
1.1.100. Na iminência de uma falha, a SOLUÇÃO deve entrar em estado de falha segura (estado alternativo e seguro) de forma a manter os dados consistentes e íntegros, bem como a garantir o atendimento aos requisitos de segurança.
CAPACIDADE DE RECUPERAÇÃO
1.1.101. Quando da integração assíncrona com outros sistemas, em caso da perda de conexão com esses sistemas, a SOLUÇÃO deve ser capaz de sincronizar as operações efetuadas quando a comunicação for restabelecida. Para comunicação obrigatoriamente síncrona, a perda da conexão deve implicar na interrupção isolada desse serviço.
1.1.102. Quando ocorrer uma falha em suas transações internas, que não envolvam outros sistemas, a SOLUÇÃO deve permitir que os dados manipulados retornem aos valores anteriores ao início do processamento, garantindo a sua integridade.
1.1.103. A SOLUÇÃO deve poder ser recuperada sem comprometer a proteção das informações, mesmo após a descontinuidade das operações.
1.1.104. A SOLUÇÃO deve dispor de controles de recuperação que a reconstruam para um estado de funcionamento alternativo e seguro ou previnam a entrada de estados inseguros como uma resposta direta de ocorrência de falhas, descontinuidade de operações ou reinício do sistema. Em geral, outras partes da SOLUÇÃO devem permanecer operacionais pela redundância de componentes críticos, por exemplo, pelo uso de espelhamento de disco ou rotas alternativas. Falhas que devem ser antecipadas incluem: a. Ações anormais que ensejam em falha e que sempre resultam na corrupção da SOLUÇÃO (por exemplo: inconsistência de tabelas críticas ou quaisquer corrupções na execução do código causadas por falhas transientes de hardware, firmware, processador, energia ou comunicação). b. Falhas em mídias que deixam todo ou parte da SOLUÇÃO inacessível ou que causam sua corrupção (por exemplo: erros de paridade ou de disco rígido). c. Descontinuidade de operação causada por intervenções administrativas equivocadas ou ausência pontual desta intervenção (por exemplo: desligamento não planejado do servidor, ignorar a exaustão de recursos críticos, configuração inadequada).

1.1.105. A SOLUÇÃO deve permitir as seguintes estratégias de recuperação: a. Automática – ocorre a partir da tolerância a falhas ou de algum controle que realiza uma autoverificação, colocando a SOLUÇÃO no estado de funcionamento alternativo e seguro para, posterior e automaticamente, recuperá-lo ao seu estado normal. b. Manual – ocorre a partir da intervenção do administrador que coloca a SOLUÇÃO no estado de funcionamento alternativo e seguro para, posterior e manualmente, recuperá-lo ao seu estado normal.
INTEGRIDADE DE DADOS
1.1.106. A SOLUÇÃO deve garantia a integridade dos dados em todas as transações. Para isto, devem ser observadas as seguintes regras: a. Há exclusão física e lógica junto às bases de dados envolvidas com a transação. b. Os controles de entrada de dados por usuários e ou interface utilizam validações para os tipos de dados, ou expressões regulares, entre outras técnicas para evitar a entrada de dados inconsistentes ou scripts com comandos invasores. c. Há controle de *rollback* para retorno a um estado anterior à alteração de dado em caso de ocorrência de erros e ou falhas. d. Há controle de concorrência nas transações onde sempre a informação mais atual é preservada. e. O acesso às bases de dados ocorre por meio de visões.
1.1.107. A SOLUÇÃO deve controlar as integrações com outros sistemas de forma a evitar o comprometimento das informações ou que um problema em um sistema comprometa o funcionamento de outro.
1.1.108. A SOLUÇÃO deve controlar as interfaces de usuário e de sistemas a partir de validações na entrada de dados.
1.1.109. A SOLUÇÃO deve garantir a acurácia dos cálculos por ela realizados, verificando, por exemplo, problemas de arredondamento e tipos de variáveis.
GERENCIAMENTO DE EXCEÇÃO
1.1.110. Para o gerenciamento correto das exceções, as seguintes ações devem ser executadas: a. Nenhuma página de erro interno da SOLUÇÃO deve aparecer para o usuário final. Deve existir uma página de erro padrão, configurável com mensagens ou informações relacionadas, que seja lançada no caso de exceções não previstas; b. Caso ocorra algum tipo de erro (inerente ao negócio) na montagem de qualquer interface, uma mensagem de erro deve ser apresentada informando o erro ocorrido e retornar automaticamente à página que a acionou;