A SOLUÇÃO deverá atender obrigatoriamente aos requisitos não funcionais e às características técnicas descritos itens 1 e 2 deste anexo. Os requisitos não funcionais e técnicos descritos a seguir atendem aos aspectos relacionados com segurança, desempenho, integração e infraestrutura.

1. REQUISITOS NÃO FUNCIONAIS

	Descrição do Requisito
	DOCUMENTAÇÃO GERAL
1.1	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).
1.2	Documentação descrevendo os componentes da arquitetura da SOLUÇÃO (versão de componentes e produtos de terceiros de que necessite a SOLUÇÃO).
1.3	Documentação descrevendo os procedimentos de instalação e atualização da SOLUÇÃO e seus componentes (manual técnico de instalação e configuração).
1.4	Tabela de códigos de erro e exceções da SOLUÇÃO.
1.5	Acesso a base de conhecimento dos principais procedimentos de resolução de problemas.
1.6	Documentação descrevendo os procedimentos de administração da SOLUÇÃO (manual do módulo de administração).
1.7	Documentação descrevendo a política de expurgo de dados.
1.8	Manual de utilização da SOLUÇÃO (Manual do Usuário).
1.9	Documentação descrevendo os mecanismos que garantam o sigilo no tráfego e armazenamento de informações com o nível de criticidade que detenham, p.ex., criptografia de senha de usuário de banco de dados e credenciais de usuários administradores.
1.10	Documentação descrevendo as configurações necessárias para garantir alta disponibilidade e desempenho baseado em cenários de quantidade máxima

Descrição do Requisito
de sessões concorrentes.
1.11 Documentação descrevendo os procedimentos de implantação da SOLUÇÃO (Diagrama de Implantação)
1.12 Documentação descrevendo os procedimentos de monitoração da SOLUÇÃO.
1.13 Documentação descrevendo os procedimentos de manutenção da base de dados da SOLUÇÃO.
CONSTRUÇÃO E INFRAESTRUTURA
1.14 SOLUÇÃO baseada em interface gráfica Web.
1.15 Possuir interface Web compatível com Internet Explorer 8.0 e superior, Firefox 20.0 e superior e Chrome mais recente.
1.16 Ser compatível com o SGBD DB2 para z/OS versão 8.1.0 e superior.
1.17 Ser compatível com o SQL Server 2008 e superior.
1.18 Os Componentes instalados para a solução devem ser compatíveis com a plataforma Windows Server 2008 e superior ou com a plataforma Linux RedHat 6 e superior
1.19 SOLUÇÃO deve suportar ser executada em ambiente virtualizado.
1.20 A SOLUÇÃO ser compatível com o servidor de aplicação Websphere 8.5.5 e superior ou IIS 7.5 e superior.
USABILIDADE, CUSTOMIZAÇÃO E PERSONALIZAÇÃO
1.21 Interface responsiva com suporte às plataformas móveis principais (Android e iOS).

Descrição do Requisito
1.22 Possibilitar a customização da interface gráfica de usuário através de parametrizações e customizações.
1.23 Utilizar e apresentar mensagens, telas e help online no idioma português do Brasil.
1.24 Ter baixo tempo de resposta às requisições feitas através da interface (menor que 2 segundos).
1.25 Interface intuitiva e de fácil utilização, sugerindo valores padrões para campos de preenchimento obrigatório.
1.26 Possuir recursos para visualização das informações em vídeo (na tela da estação de trabalho) antes de sua impressão ou armazenamento em arquivos.
1.27 Permitir a importação e exportação de dados preferencialmente em formatos de padrões abertos, podendo ser TXT, HTML, DOC, XLS, ODT, ODS.
1.28 Permitir vinculação/anexação de dados cadastrados com documentos do tipo: TIF, JPEG, BMP, TXT, DOC, PPT, XLS, HTML, ODT, ODP.
1.29 Possibilitar a customização da interface para o padrão visual da Intranet do Banco do Nordeste.
1.30 Permitir a customização de funcionalidades da SOLUÇÃO, inclusive aspectos funcionais e de regras de negócio.
1.31 Permitir mensurar as customizações demandas utilizando Análise de Ponto de Função para cálculo de esforço.

Descrição do Requisito
1.32 Permitir fácil intercâmbio de customizações entre os ambientes de desenvolvimento de software a citar: desenvolvimento, teste, homologação e produção, com a adequada e devida separação entre esses perímetros.
1.33 Garantir que novas versões do produto ou correções de problemas na versão implantada suportem as customizações aplicadas à SOLUÇÃO conforme necessidade do negócio.
SEGURANÇA
1.34 Possibilitar a autenticação dos usuários via LDAP utilizando repositório de usuários AD (Active Directory) do Windows Server 2003 e superior.
1.35 Suportar a autenticação em múltiplos domínios federados de *Active Directory* do *Windows Server 2003* e superior.
1.36 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.
1.37 Permitir criação e manutenção de perfis de acesso diferenciados com níveis de autorização por módulos, funcionalidades, transações e interface de telas de acordo com a natureza da atividade do usuário e sua área de atuação.
1.38 Possibilitar a integração aos aplicativos de gestão de recursos humanos e de segurança de acesso para permitir o cadastramento e associação de usuários aos perfis pré-definidos automaticamente, de acordo com unidade de lotação e função.
1.39 Permitir criação de regras automáticas para manutenção de usuários e perfis, como alterar ou excluir o acesso de usuários em caso de transferência de unidade ou alteração de função.
1.40 Possibilitar cadastramento de usuários e associação a perfis em lote ou individualmente.
1.41 Permitir a associação manual de usuários aos perfis pré-definidos de maneira simples e amigável.
1.42 Controlar a seção do usuário através de timeout configurável por inatividade e por tempo de seção.
1.43 Permitir que os logs gerados pela SOLUÇÃO possam vir a ser auditados por ferramentas externas ao sistema.

1.44	Possuir mecanismos de integração com a infraestrutura de chaves públicas baseada em Microsoft Windows Server 2008 e superior.
1.45	Suportar autenticação utilizando tecnologia de Single Sign-On (SSO) para aplicações WEB.
1.46	Suportar a utilização 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.
1.47	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.
1.48	Deve prover mecanismos de criptografia na comunicação entre todos os seus componentes (clientes, servidores de aplicação, servidores de banco de dados, etc.).
1.49	O armazenamento de credenciais de acesso à solução (usuário/senha) deve ser criptografado.
1.50	Garantir a continuidade da sessão do usuário em caso de falha em um dos nós do cluster de servidores, de forma transparente para o usuário.
1.51	Atender a prática de “Segregação de função” quando da atribuição de responsabilidades e direitos de acesso. “Segregação de função” consiste na divisão de tarefas gerenciais ou operacionais, ou de áreas de responsabilidade de forma a prevenir e reduzir oportunidades de modificações não autorizadas ou mau uso de dados ou serviços.
1.52	Atender a prática de "menor privilégio" quando da atribuição de responsabilidades e direitos de acesso. “Menor privilégio” determina que cada agente de um sistema (como processo, usuário, programas, entre outros) receba um conjunto mais restritivo de privilégios para acessar apenas informações e recursos necessários para seu propósito legitimo. Esse princípio limita o dano que pode resultar de acidentes, erros, ou uso não autorizado.
1.53	Atender a prática de "need to know" quando da atribuição de responsabilidades e direitos de acesso. “Need to know” estabelece permitir acesso a informações e recursos necessários apenas para realizar as responsabilidades / atribuições. Esse princípio dificulta o acesso não autorizado a recursos sem comprometer o acesso legítimo.
1.54	Quando da integração assíncrona com sistemas externos, em caso da perda de conexão com esses sistemas, a solução deverá ser capaz de sincronizar as operações efetuadas quando a comunicação for restabelecida. Para comunicação obrigatoriamente síncrona, a perda da conexão implica na interrupção isolada desse serviço.

1.55 Em transações internas da solução, que não envolvam integrações com outros sistemas, dados que tenham sido manipulados durante um processo que ocorreu falha deverão ter seus valores retornados aos valores anteriores ao início do processamento, garantindo a integridade dos mesmos.
RECUPERAÇÃO DE INFORMAÇÕES
1.56 Disponibilizar uma interface amigável para criação de relatórios/gráficos, dinamicamente, com parametrização de campos, filtros, definição de ordenação, totalizadores e formatação de saída dos dados.
1.57 Permitir que as informações sejam exibidas em vídeo antes de sua impressão ou armazenamento em arquivo.
1.58 Permitir que os relatórios gerados dinamicamente possam ser exportados nos formatos TXT, HTML, DOC/DOCX, XLS/XLSX, CSV, XML, ODT, ODS e PDF.
1.59 Prover mecanismo para agendamento da execução dos relatórios criados dinamicamente, de forma eventual e periódica.
AUDITORIA
1.60 Realizar gravação automática de trilhas de auditoria para controle de modificações e alterações nos dados, inclusive para eventos que modifiquem as permissões de acesso do usuário.
1.61 Cada registro da trilha de auditoria deve 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); • Nome da máquina origem do evento; • Domínio da máquina de origem do evento; • Resultado final (sucesso ou falha); • Detalhes do evento (informações adicionais sobre o evento, significativos para análise das ocorrências).
1.62 Permitir que os logs gerados pela solução possam vir a ser auditados por ferramentas externas ao sistema.

1.63 Permitir registro das ações dos administradores.
1.64 Os registros em trilha de auditoria deverão ter proteção contra violação de confidencialidade e integridade, ou seja, somente deve ser possível sua consulta a usuários autorizados e não deve ser possível operações de alteração e exclusão.

2. CARACTERÍSTICAS TÉCNICAS

Descrição do Requisito
2.1. Prover administração centralizada da instância implantada de modo a permitir a configuração de parâmetros gerais, cadastros e perfis de usuários e manutenções da plataforma.
2.2. 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 VI - Ambiente Computacional do Banco do Nordeste.
2.3. Caso existam rotinas *batch* necessárias ao funcionamento da SOLUÇÃO, elas deverão ser passíveis de gerenciamento pela ferramenta BMC Control-M de *scheduling* e gerenciamento de processamentos *batch*, respeitando-se o conteúdo do Anexo VI - Ambiente Computacional do Banco do Nordeste.
2.4. Possuir funcionalidades para monitoramento e gerenciamento de eventos para situações de contenção dos recursos de infraestrutura utilizados pela SOLUÇÃO e para perda de desempenho da SOLUÇÃO, no conceito fim a fim, considerando níveis de serviço a serem previamente acordados para cada funcionalidade e a critério do BANCO
2.5. Possibilitar o uso de infraestrutura de clusters locais ou geograficamente dispersos em todos os seus componentes.
2.6. Suportar a utilização de mecanismos de “data sharing”, com balanceamento de carga entre servidores de banco de dados distintos.
2.7. Integrar-se à ferramenta de geração de backup e “disaster recovery” em uso no Banco (IBM TIVOLI STORAGE MANAGER Versão 6 e superior para plataforma distribuída e GFS STACK RMM e HSM para plataforma mainframe).
2.8. Suportar, de forma nativa, o protocolo de transferência de arquivos FTP e as linguagens de marcação XML e XSLT.
2.9. Suportar SSL 128 bits para criptografia do canal de transmissão de dados.

Descrição do Requisito
2.10. Suportar SSL 128 bits para a criptografia de informações trocadas entre servidores
2.11. Permitir a implantação seguindo o ciclo de desenvolvimento de software em ambientes de Desenvolvimento, Teste, Homologação e Produção.
2.12. Fornecer um cliente para os sistemas operacionais Android e iOS utilizados nos principais smartphones e tablets do mercado ou deve ser compatível com os navegadores (browsers) utilizados nos dispositivos para renderização de conteúdo.
2.13. Todos os módulos que compõem a SOLUÇÃO devem ser compatíveis com os sistemas operacionais Windows XP e Windows 7 (32 e 64 bits), ou superior, no lado cliente. A versão de componentes e produtos de terceiros de que necessite a SOLUÇÃO deverá ser compatível com o ambiente computacional do BNB descrito no Anexo VI - Ambiente Computacional do Banco do Nordeste e sistemas operacionais supracitados.
2.14. A SOLUÇÃO, no lado servidor, deve ser suportada para executar em ambiente virtualizado com *VMWare vSphereEnterprise Plus* 5.0 e superior.
2.15. Permitir integração com a Suíte IBM Cognos 10.1.1 e superior para extração de informações e produção de data marts, através de conectores do fabricante ou JDBC/ODBC;
2.16. Suportar integrações através de serviços web publicados com protocolo SOAP ou REST implementando autorização de acesso aos serviços para a comunicação com Portais Corporativos compatíveis com a especificação padrão de Portlets;