Banco do Nordeste

ANEXO II – REQUISITOS NÃO FUNCIONAIS

1. FINALIDADE

1.1. Este documento descreve os requisitos relacionados ao uso de Solução para Automação e Inteligência de Pagamentos a Fornecedores, doravante denominado SOLUÇÃO, em termos de desempenho, usabilidade, confiabilidade, segurança, disponibilidade, manutenibilidade e tecnologias envolvidas.

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.

2.3.2. **Provido com Customização**, identificada pelo número 2 (dois): quando a SOLUÇÃO exigir a codificação e/ou configurações significativas ou complexas, e que não afetem futuras atualizações.

2.3.3. **Não provido**, identificada pelo número **3** (três): quando a SOLUÇÃO **não fornecer** o requisito não funcional.

2.4. A coluna “Complexidade” deverá ser preenchida somente se o requisito for atendido através de customização, e se refere ao nível de complexidade para atender o requisito não funcional. Deverá ser preenchido conforme orientação a seguir:

2.4.1. **Simples**: quando o esforço de implementação for igual ou inferior a 8 (oito) horas.

2.4.2. **Moderada**: quando o esforço de implementação for entre 8 (oito) e 40 (quarenta) horas.

2.4.3. **Complexa**: quando o esforço de implementação for superior a 40 (quarenta) horas.

3. USABILIDADE

Item	Descrição	Situação de Atendimento do Requisito (1, 2 ou 3)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
3.1.	A SOLUÇÃO deverá disponibilizar manuais para o usuário final, *help on-line*, manual do administrador e manuais técnicos escrito em língua portuguesa do Brasil.		
3.2.	Utilizar e apresentar mensagens e telas no idioma português do Brasil.		
3.3.	Fornecer valores default para campos necessários (obrigatórios).		
3.4.	A interface da SOLUÇÃO deve ser intuitiva, clara, direta e de fácil assimilação por qualquer tipo de usuário.		
3.5.	Oferecer recursos visuais/gráficos que permitam a análise de informações disponibilizadas pela SOLUÇÃO.		
3.6.	Permitir que as informações sejam exibidas em tela antes de sua impressão ou armazenamento.		
3.7.	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, bem como 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.		
3.8.	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.		
3.9.	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.		
3.10.	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.		

3.11.	A SOLUÇÃO deverá ser acessada de forma responsiva em dispositivos móveis (smartphones, tablets, IOS e Android) e/ou possuir aplicativo específico.		

4. PROTEÇÃO DE DADOS

Item	Descrição	Situação de Atendimento do Requisito (1, 2 ou 3)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
4.1	A SOLUÇÃO deve apresentar 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 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.		
4.2	A SOLUÇÃO deve assegurar que 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.		
4.3	A SOLUÇÃO deve prover mecanismo de acesso protegido aos dados, por meio de comunicação criptografada, garantindo que apenas aplicações e usuários autorizados tenham acesso.		
4.4	A solução deve atestar informações referentes às medidas adotadas em proteção de dados pessoais, devendo ser 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. • Suportar autenticação dos usuários via LDAP com Microsoft Active Directory. • 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).		

5. SEGURANÇA

Item	Descrição	Situação de Atendimento do Requisito (1, 2 ou 3)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
5.1.	Possuir metodologia de gestão de riscos, elaborada em conformidade com as melhores práticas de mercado e com a legislação vigente, bem como adotar e aplicar metodologia para o gerenciamento dos riscos, em especial de segurança cibernética, da informação e de dados pessoais		

5.2.	Implementar 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. • Habilitar o registro completo do Hypervisor. • Possuir controles que permitam aos usuários autorizados do órgão ou da entidade acessarem os registros de acesso administrativo do monitor de máquina virtual -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.		
5.3.	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.		

5.4.	Deve impor mecanismo de autenticação que exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso.		
5.5.	Deve suportar tecnologia **single sign-on** para autenticação.		
5.6.	Deve suportar mecanismos de autenticação multifator ou outra alternativa que aumente o grau de segurança no processo de autenticação de usuários, de acordo com nível de criticidade da informação manipulada.		
5.7.	Deve permitir ao Banco gerenciar as próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido.		

5.8.	Deve guardar conformidade legal em seus processos de autenticação, controle de acesso, contabilidade e de registro (formato, retenção e acesso).		
5.9.	Implementar soluções e procedimentos para garantir a segurança de aplicações web disponibilizadas no ambiente de nuvem, incluindo, no mínimo: - Firewalls especializados na proteção de sistemas e aplicações; - Desenvolver código web em conformidade com as melhores práticas de codificação segura OWASP v. 1.3 ou superior, bem como os princípios do S*ecurity by Design* e normativos vigentes; A verificação e validação de dados de entrada deverão ser consideradas, onde aplicáveis, para garantir correção e consistência dos dados, reduzir o risco de erros e prevenir 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;		

	- A solução deve detectar e tratar todos os erros e exceções ocorridos durante o acesso a qualquer componente externo ao sistema, por exemplo, banco de dados e webservices. Deve 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.		
5.10.	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 que deve 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.		
5.11.	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.		
5.12.	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.		
5.13.	Deve possuir mecanismos que permitam, no mínimo, quanto à segregação de dados: - Isolar, utilizando separação lógica, todos os dados e serviços do Banco de outros clientes de serviço em nuvem; - Segregar o tráfego de gerenciamento do tráfego de dados do Banco; - Implementar dispositivos de segurança entre zonas; - Possuir capacidade de criar ACLs para as redes virtuais do Banco, garantindo assim camadas opcionais de segurança para cada rede, controlando o tráfego entre elas atrás de firewalls e ainda a segmentação destas redes virtuais com várias sub-redes; - Deve permitir a criação de regras de inbound e outbond em protocolo IPv4 e, quando necessário, IPv6 para controles de tráfego; - Deve ter a capacidade de criar sub-redes e associá-las a uma ACL para a devida segmentação do tráfego; - Por padrão todo o tráfego entre redes virtuais deve ser negado, até que uma ACL de permissão seja criada, devendo esta apresentar explicitamente os protocolos, portas, origem e destino do tráfego permitido.		
5.14.	O datacenter deverá possuir 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; • Deverá 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.		
5.15.	Possuir 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.		
5.16.	Deverá possuir procedimentos de notificação de incidente cibernético contra os serviços ou dados do Banco sob sua custódia. Em caso de ocorrência do incidente cibernético, a comunicação deve ser realizada de forma imediata.		
5.17.	Deverá possuir procedimentos necessários para a preservação de evidências, com a possibilidade de uso em tribunais e no devido processo legal.		
5.18.	Demonstrar 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.		

5.19.	Em caso de encerramento contratual, assegurar ao Banco capacidade de cumprimento do art. 17, inciso IV, da Resolução CMN 4.893/21.		
5.20.	A SOLUÇÃO deverá estar em conformidade com os requisitos estabelecidos na Resolução CMN 4.893/21.		
5.21.	A SOLUÇÃO deverá prover meios de garantir o sigilo no tráfego e no armazenamento da informação, pelo uso de criptografia, *hash*, protocolos de transporte seguro, como por exemplo: https, ssl.		
5.22	Os dados armazenados (ou em trânsito) no provedor devem estar criptografados, sendo que o esquema criptográfico deve ser adequado à classificação das informações e considerado como aceitável e seguro pelo mercado. As chaves criptográficas utilizadas devem estar de posse exclusiva do Banco. O acesso indevido a dados pelo provedor, bem como as alterações posteriores, inclusive deleção, devem ser registrados e não devem ser alterados sob nenhuma hipótese, deve ser de acesso exclusivo do Banco, e deve ser alertado de forma		

	imediata. Solução de DLP/CASB deve compor ferramentas que permitam ao Banco o controle da informação classificada e rotulada, seja armazenada ou em trânsito.		

6. INFRAESTRUTURA DE TI

Os requisitos deste bloco devem ser considerados apenas para a modalidade ***Software as a Service (On Cloud)***

Item	Descrição	Situação de Atendimento do Requisito (1, 2 ou 3)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
6.1.	Possuir, de forma documentada, processos de gestão de mudanças, seguindo as práticas do ITIL v3 (*Information Technology Infrastructure Library*) ou superior.		
6.2.	Todo o processo de tratamento de dados, inclusive pessoais, deverá ocorrer apenas dentro do território nacional, disponibilizado em infraestrutura de datacenter, acessível através de link de dados dedicado, ambos de responsabilidade do CONTRATADO, e também pela internet.		
6.3.	O *datacenter* deverá possuir mecanismos que permitam, no mínimo, quanto à disponibilidade: - Garantir disponibilidade de, no mínimo, 99,741%, cuja comprovação será dada pela certificação TIA 942 TIER II, ou superior; - Ser um AS (*Autonomous System*) participante de grupo de Redes IP gerenciados por mais de uma operadora de redes utilizando o protocolo BGP; - Possuir equipe de monitoramento técnico para acompanhamento da disponibilidade dos serviços, atendimento ao cliente e acionamento das equipes de suporte técnico de 2o e 3o		

	níveis e engenharia de redes e segurança, em regime 24hs, 07 dias por semana e 365 dias no ano; - O CONTRATADO deverá manter backup diário por 30 dias, semanal por 60 dias e mensal por 1 ano e sua recuperação não deve envolver custos adicionais ao Banco do Nordeste; - Os backups devem ser mantidos *offline* e o testes de recuperação periódicos dos dados armazenados devem ser comprovados formalmente, garantindo a disponibilidade e a integridade; - Os *backups* deverão abranger todos os módulos do sistema fornecido; - Disponibilizar, quando solicitado pelo Banco do Nordeste, no prazo máximo de 24 horas, cópia do backup em local alinhado com o CONTRATADO; - Permitir configuração de regras de *firewall* e IPS específicas para o Banco do Nordeste, através de solicitação por chamado técnico seguindo as boas práticas de gestão de solicitações e incidentes do ITIL v3 ou superior.		
6.4	O ambiente remoto do CONTRATADO deverá se conectar ao datacenter do BANCO através de pelo menos 2 (dois) *links* de comunicação de dados, providos e mantidos pelo CONTRATADO.		
6.5	A conexão deverá ser provida por operadoras de telecomunicações diferentes, sendo conectadas à rede do BANCO em pontos distintos, dentro do mesmo *datacenter*		

6.6	A tecnologia dos links de comunicação deverá ser do tipo MPLS (*Multiprotocol Label Switch*) ou fibra GPON (até 100Mbps) ou uma fibra dedicada em conjunto com um *switch EDD*.		
6.7	A velocidade de cada um dos circuitos deverá ser de, no mínimo, 50 (cinquenta) Mbps		
6.8	O CONTRATADO deverá fornecer, quando solicitado pelo BANCO, a média de utilização dos circuitos, perdas, latência e jitter.		
6.9	A velocidade deve ser garantida fim-a-fim e deverá possuir mecanismos de qualidade de serviço (QoS). Os acessos deverão ser de fibra ótica ou par metálico e é vedado qualquer trecho com a tecnologia a rádio		

6.10	Em qualquer momento do contrato, caberá ao BANCO auditar o fornecimento de redes descrita nos anexos desta RFP.		
6.11	Os circuitos e acessos deverão possuir estrutura (acesso e ponto de presença – POP) totalmente separadas, incluindo os acessos físicos, roteadores concentradores e operadoras distintas		
6.12	O *Backbone* de uma operadora deverá ter interligação com, no mínimo, 2 rotas distintas, onde uma rota pode assumir integralmente o tráfego da outra em caso de interrupção		
6.13	Para o atendimento através de fibra GPON (até 100Mbps) ou uma fibra dedicada em conjunto com um switch EDD, o tamanho do frame permitido deverá ser de até 1526 bytes		

6.14	O balanceamento entre os links deverá ocorrer de forma automática, permitindo a utilização simultânea de ambos os circuitos e no caso da indisponibilidade de um circuito o outro deverá assumir os serviços em sua totalidade.		
6.15	Fica a cargo do CONTRATADO o fornecimento de todos os equipamentos para prover comunicação fim-a-fim, como roteadores, firewall, balanceadores, etc. Todos os equipamentos deverão estar acompanhados de cabos, placas, conectores e licenças de software para atender os requisitos de conexão de rede.		
6.16	Em caso de falha de um dos circuitos, o chaveamento deve ser automático e de forma transparente, não indisponibilizando os serviços.		
6.17	A comunicação de dados entre o CONTRATADO e o BANCO será conectada no segmento de parceiros e estará sob regras de segurança deste perímetro.		

6.18	O CONTRATADO deverá garantir que seus equipamentos de borda fechem conexão segura através de túneis criptografados com o equipamento de *Firewall* do CONTRATANTE, garantindo que toda a comunicação seja realizada utilizando criptografia. Os equipamentos de borda devem suportar VPN IPsec Site-to-Site com, no mínimo, os seguintes padrões de segurança: Diffie-Hellman Group 5, Group 14, Group 19 e Group 20; Algoritmo Internet Key Exchange (IKEv1 e v2); AES 128 e 256 (Advanced Encryption Standard); Autenticação SHA-1 e SHA-256; Autenticação via certificado IKE PKI.		
6.19	O CONTRATADO deverá garantir funcionalidades de Firewall nos seus equipamentos de borda e, a critério do BANCO, estas regras poderão ser definidas e auditadas pelo CONTRATADO. É vedado o acesso à Internet na infraestrutura de conectividade que engloba a comunicação de dados entre o CONTRATADO e o BANCO. Eventuais conexões com a Internet, necessárias ao ambiente computacional do CONTRATADO, deverão ser segregadas fisicamente da infraestrutura computacional que possuir meios de comunicação com o datacenter do BANCO.		

7. COMPATIBILIDADE COM AMBIENTE COMPUTACIONAL DO BANCO

Os requisitos deste bloco devem ser considerados apenas para a modalidade **On Premise**

Item	Descrição	Situação de Atendimento do Requisito (1, 2 ou 3)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
7.1.	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.		
7.2.	Deve possuir interface *Web* compatível com os navegadores mais utilizados no mercado, sendo eles: Internet Explorer 9.0 e superior; versões mais recentes do Firefox e Chrome.		
7.3.	Todos os módulos que compõem a SOLUÇÃO devem ser compatíveis com os sistemas operacionais e superior, no lado cliente, além disso devem ser compatíveis com o ambiente computacional do BANCO.		
7.4.	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, além disso devem ser compatíveis com o ambiente computacional do Banco do Nordeste.		
7.5.	Os componentes da SOLUÇÃO que serão instalados em servidores deverão suportar a execução em ambiente virtualizado com VMWare vSphere e superior.		
7.6.	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.		
7.7.	A SOLUÇÃO deve permitir a captura de dados por meio de coletores que suportem os seguintes tipos de código de barra: Numéricos (EAN-8, EAn-13, Codabar) ou AlfaNuméricos (Code128, Code39).		

8. CONFIABILIDADE

Item	Descrição	Situação de Atendimento do Requisito (1, 2 ou 3)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
8.1	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.		
8.2	A SOLUÇÃO deverá registrar em log específico com data/hora de envio e mensagem todos os e-mails de alertas enviado pelo sistema.		

9. ACESSIBILIDADE

Item	Descrição	Situação de Atendimento do Requisito (1, 2 ou 3)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
9.1	A SOLUÇÃO deverá fornecer recursos de acessibilidade que ofereça condições de usuários com necessidades especiais poderem utilizar o sistema. Estes recursos visam promover a inclusão desses usuários e ampliar a utilização de suas funcionalidades dentro do BANCO. Devem ser seguidos os padrões recomendados pelo W3C no *Web Accessibility Initiative*.		
9.2	A SOLUÇÃO deve ter navegabilidade limpa e intuitiva, com a possibilidade de visualizar o processo inteiro em uma única tela.		