banco da amazônia

ANEXO IV - ESPECIFICAÇÕES DE REQUISITOS NÃO FUNCIONAIS

1. FINALIDADE

1.1. Este documento descreve os requisitos relacionados ao uso da SOLUÇÃO de CX, doravante denominado SOLUÇÃO, em termos de desempenho, usabilidade, confiabilidade, segurança, disponibilidade, manutenibilidade e tecnologias envolvidas.

1.2. Os requisitos não funcionais estabelecem níveis mínimos de desempenho, disponibilidade, segurança, usabilidade e manutenibilidade, sendo vedada qualquer inferência sobre tecnologia específica, fornecedor, linguagem de programação, banco de dados ou arquitetura proprietária.

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. Este 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.

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

2.5. A proposta será desclassificada caso este documento não seja entregue ou seja entregue sem preenchimento ou com informações diferentes da solicitada.

3. A pontuação do preenchimento quanto ao atendimento e complexidade de atendimento dos requisitos seguirá o seguinte quadro:

ATENDIMENTO	PONTUAÇÃO	COMPLEXIDADE	PONTUAÇÃO
CUSTOMIZADO(2)	2 pontos	COMPLEXA	1 ponto
		MODERADA	2 pontos
STANDARD (1)	5 pontos	SIMPLES	3 pontos

3.1. Serão considerados aptos para participar da POC os licitantes que somarem 90% ou mais da pontuação máxima da coluna “atendimento” (>= pontos).

4. REQUISITOS NÃO FUNCIONAIS

4.1. USABILIDADE

Item	Descrição	Situação de Atendimento do Requisito (1 ou 2)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
3.1.1.	A SOLUÇÃO deverá disponibilizar manuais para o usuário final, *help on line*, manual do administrador e manuais técnicos escrito em língua portuguesa do Brasil.		
3.1.2	Utilizar e apresentar mensagens e telas no idioma português do Brasil.		
3.1.3	Fornecer valores default para campos necessários (obrigatórios).		
3.1.4	A interface da SOLUÇÃO deve ser intuitiva, clara, direta e de fácil assimilação por qualquer tipo de usuário.		
3.1.5	Oferecer recursos visuais/gráficos que permitam a análise de informações disponibilizadas pela SOLUÇÃO.		
3.1.6	Permitir que as informações sejam exibidas em tela antes de sua impressão ou armazenamento.		
3.1.7	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. 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.		
3.1.8	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.		
3.1.9	No que couber, a SOLUÇÃO deve apresentar uma interação flexível, que permite que o usuário controle o fluxo interativo, sendo capaz de dispensar ações consideradas desnecessárias sem necessitar sair do programa.		
3.1.10	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.		
3.1.11	A SOLUÇÃO deverá ser acessada de forma responsiva em dispositivos móveis (smartphones, tablets, IOS e Android) e/ou possuir aplicativo específico.		

3.1.12	A solução deve prover console para gerenciamento		

4.2. ACESSIBILIDADE

Item	Descrição	Situação de Atendimento do Requisito (1 ou 2)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
3.2.1	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.		
3.2.2	A SOLUÇÃO deve ter navegabilidade limpa e intuitiva, com a possibilidade de visualizar a consulta 360º do cliente em uma única tela.		

4.3. MANUTENIBILIDADE

Item	Descrição	Situação de Atendimento do Requisito (1 ou 2)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
3.3.1	A plataforma deverá fornecer ambientes para homologação funcional do usuário antes de publicação de atualizações em ambiente de produção. Referidos ambientes deverão ser segregados do ambiente de desenvolvimento.		

4.4. PROTEÇÃO DE DADOS (LGPD)

Item	Descrição	Situação de Atendimento do	Nível de Complexidade da Customização

		Requisito (1 ou 2)	(Simples, Moderada ou Complexa)
3.4.1	Apresentar certificação válida do provedor que hospeda a solução referente à norma ISO/IEC 27701:2019 - Técnicas de segurança — Extensão da ISO/IEC 27001 e ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.		
3.4.2	Em caso de hospedagem em nuvem pública apresentar certificação válida do provedor que hospeda a solução referente à norma ISO/IEC 27018:2021 - Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de Dados Pessoais.		
3.4.3	Caso seja necessária a utilização de consentimento como hipótese de tratamento de dados pessoais conforme descrito na LGPD, a solução deve possuir: • meios para se integrar com ferramentas de gestão de consentimento a ser definida pelo Banco. • procedimento para o expurgo/anonimização dos dados pessoais, caso ocorra a revogação do consentimento.		
3.4.4	Permitir a customização de termos de aceite/disclaimer/consentimento para início do tratamento dos dados, incluindo link para política de privacidade ou outras páginas pertinentes.		
3.4.5	Prover mecanismos que possibilitem implementar além do controle de acesso a funcionalidades da solução de acordo com o perfil, regras de negócio para restringir o acesso a informações (telas, relatórios, exportações etc.) de acordo com o perfil/lotação do usuário quando do interesse do Banco. Exemplo: Um Gerente de Relacionamento da só tem acesso a visualizar informações de seus clientes; Um Gerente Geral de Agência só tem acesso a clientes de sua Agência. A solução também deve permitir, pela não apresentação ou mascaramento de dados pessoais, dados pessoais sensíveis e informações protegidas por sigilo bancário, restringir a lista de atributos a serem visualizados de um determinado cliente de acordo com o perfil de acesso do usuário.		
3.4.6	Possuir registro/log de acesso das consultas/relatórios/exportações que envolvam dados pessoais, dados pessoais sensíveis e informações protegidas por sigilo bancário dos clientes, incluindo os parâmetros/filtros utilizados.		
3.4.7	Apresentar a declaração de Atendimento de Boas Práticas de Privacidade da Solução		

4.5. SEGURANÇA

Item	Descrição	Situação de Atendimento do Requisito (1 ou 2)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
3.5.1	A SOLUÇÃO deverá permitir integração de autenticação na plataforma com o Microsoft Entra ID (Antigo Azure AD).		
3.5.2	A SOLUÇÃO deverá suportar autenticação por meio de protocolos adotados pelo Banco, bem como integração com ferramentas de SSO (Single Sign-On).		
3.5.3	A SOLUÇÃO deverá 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, campos e telas permitidas para o seu perfil de acesso, permitindo definição de perfis de utilização individuais e de grupos. Deve haver possibilidade de diferenciar o controle de acesso dos usuários através de perfil, regras de negócio, alçadas e eventos funcionais.		
3.5.4	A SOLUÇÃO deverá 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.		
3.5.5	A SOLUÇÃO deverá possuir interface Web compatível com os navegadores mais utilizados no mercado, com versões mais recentes do Firefox, Edge e Chrome.		
3.5.6	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 (ex.: https, ssl)		
3.5.7	A SOLUÇÃO deverá estabelecer um canal de comunicação seguro utilizando, no mínimo, TLS (Transport Layer Security) versão 1.2 ou superior.		
3.5.8	A SOLUÇÃO deverá suportar SSL 256 bits ou superior para a criptografia de informações trocadas entre servidores internos e externos.		
3.5.9	Os dados armazenados (ou em trânsito) na SOLUÇÃO deverão estar criptografados e o esquema criptográfico adequado à classificação das informações e considerado como aceitável e seguro pelo mercado. 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.		
3.5.10	A SOLUÇÃO deverá permitir gravação automática de trilhas de auditoria incluindo 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.		

3.5.11	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.		
3.5.12	Cada registro da trilha de auditoria a ser configurada, deve conter, no mínimo, as seguintes informações: a) data e hora de início e fim do evento; b) tipo do evento (consulta, inclusão, alteração, exclusão, logon, logout); c) identidade do usuário (se aplicável); d) identificação do aplicativo, tela ou função utilizados; e) origem do evento (IP e/ou nome da máquina); f) resultado final (sucesso ou falha); g) detalhes do evento (informações adicionais sobre o evento significativos para análise das ocorrências).		
3.5.13	A SOLUÇÃO deverá 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.		
3.5.14	A SOLUÇÃO deverá ter capacidade de manter a rastreabilidade de operações para auditoria, garantindo a estruturação de um histórico de alterações.		
3.5.15	A SOLUÇÃO deverá possuir mecanismos de auditoria com integração com a solução de correlacionamento de eventos (Security Information and Event Management - SIEM).		
3.5.16	A SOLUÇÃO deverá permitir upgrade e aplicação de patches sem parada ou comprometimento de disponibilidade dos sistemas envolvidos.		
3.5.17	Durante todo o período do contrato, o CONTRATADO obriga-se a substituir, recuperar e/ou modificar os softwares e/ou firmwares instalados, sem ônus de qualquer natureza ao Banco, nos casos comprovados de mau funcionamento, falhas de segurança e de outras falhas, de modo a ajustá-los aos resultados que atendam às especificações técnicas. O CONTRATADO deverá comunicar ao Banco a descoberta de quaisquer problemas, bugs ou limitações presentes na SOLUÇÃO imediatamente após a descoberta do problema.		
3.5.18	O CONTRATADO deverá garantir a independência entre a correção de defeitos (patches) e a geração de novas versões do software, sem ônus adicional ao Banco, em função da necessidade de atualização de componente para suportar nova versão do software, dentro do prazo de validade do contrato.		
3.5.19	A SOLUÇÃO deverá possibilitar o armazenamento de dados de forma dedicada (exclusiva, com acesso pessoal devidamente controlado) para o Banco.		
3.5.20	Em caso de término de contrato de uso, a SOLUÇÃO deverá possibilitar a portabilidade de todos os dados armazenados ao longo da utilização pelo Banco.		
3.5.21	A SOLUÇÃO deverá disponibilizar mecanismo seguro para alteração (criação/remoção/atualização/leitura) e migração (importar/exportar) de dados.		

3.5.22	A CONTRATADA deverá possuir procedimentos mínimos, em relação ao descarte de ativos de informação e de dados, que assegurem: 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; b) 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; c) 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.		
3.5.23	O CONTRATADO deverá garantir tempo mínimo de armazenamento de informações e históricos de 12 (doze) meses, e com respectivo procedimento de cópia de segurança (backup) das informações.		
3.5.24	A infraestrutura que será utilizada para a instalação da SOLUÇÃO, deverá ser ofertada pela CONTRATADA e deverá ter comprovação documental de certificação que valide: a) Estar hospedada em datacenter ou por meio de "Cloud Computing" baseados na norma ANSI/TIA 942; b) Disponibilidade mínima de 99,9%; c) A oferta do serviço por meio de "Cloud Computing" implicará o compromisso de que a infraestrutura que suportará a SOLUÇÃO, 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.		
3.5.25	A SOLUÇÃO deverá suportar redundância geográfica e alta disponibilidade.		
3.5.26	A CONTRATADA deve implementar soluções e procedimentos para garantir a segurança de aplicações web disponibilizadas no ambiente computacional, incluindo, no mínimo: a) Firewalls especializados na proteção de sistemas e aplicações; b) 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; c) A verificação e validação de dados de entrada garante 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: d) Entrada duplicada; e) Valores fora de faixa; f) Caracteres inválidos em campos de dados;		

	g) Dados incompletos ou faltantes; h) Comprimento de dados não respeitando limites superiores ou inferiores; i) Realizar, no mínimo, anualmente, testes de penetração de redes e de aplicações; j) Implementar programa de correção de vulnerabilidades, indicando claramente, por criticidade, o tempo de resolução e os procedimentos de correção; k) Detecção e Tratamento dos erros e exceções ocorridos durante o acesso a qualquer componente externo ao sistema, por exemplo, banco de dados e webservices; l) 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.		
3.5.27	A CONTRATADA deverá garantir, através dos recursos de segurança disponibilizados para o atendimento ao cenário proposto, a inviolabilidade dos dados e dos serviços prestados. Para isso, deverão ser utilizados, além dos recursos físicos, mecanismos de controle de perímetro (Firewall, IDS, IPS e afins) que garantem a disponibilidade dos serviços e servidores.		
3.5.28	A SOLUÇÃO deverá garantir a inviolabilidade no armazenamento, tráfego, e eventual manuseio dos dados, ou seja, durante qualquer intervenção técnica a ser realizada.		
3.5.29	A CONTRATADA deverá permitir a realização de teste de segurança, de exercícios de ataque (Red Team) ou de análise de vulnerabilidade, em qualquer ativo de informação de responsabilidade do Banco, nos serviços contratados de processamento e armazenamento de dados e de computação em nuvem, em função da obrigatoriedade de reportar, seja para colegiados estatutários, órgãos de controle e ou auditorias, o resultado de qualquer uma dessas ações de segurança contra os ativos da informação corporativos.		
3.5.30	A CONTRATADA deverá permitir que o(s) sistema(s) adquiridos pelo Banco, que compartilhem dados ou informações cujo conteúdo seja protegido pelo sigilo fiscal, bancário ou comercial ou envolvam dados ou informações pessoais ou sensíveis ou protegidas por lei ou regulamentação vigente, sejam submetidos ao Banco para análise prévia e para realização de testes de segurança, com prazo mínimo de cinco (05) dias úteis antes da disponibilização em produção.		
3.5.31	A CONTRATADA deverá permitir que o Banco realize testes de segurança em plataformas de aplicativos web/cliente-servidor e infraestrutura de TI, porém sem se limitar a estas. Poderão ser realizados os testes do tipo Black Box, Gray Box e White Box. As vulnerabilidades identificadas são categorizadas baseando-se na lista de CWE (Common Weakness Enumeration) do Mitre e a classificação é baseada no padrão CVSS (Common Vulnerability Scoring System), implementado pela NVD (National Vulnerability Database), de acordo com a complexidade de exploração, nível de remediação ou nível de criticidade da aplicação para o negócio. Ao final dos testes, será formalizado por relatório técnico à CONTRATADA uma descrição detalhada para cada vulnerabilidade que contém orientações de como esta pode ser explorada e mitigada.		

3.5.32	Caso o relatório técnico identifique vulnerabilidade(s) associada(s) com o ativo analisado, a CONTRATADA deverá apresentar um plano de ação para correção da vulnerabilidade. Após a realização dos procedimentos de correção pela CONTRATADA, o Banco deverá ser informado para que seja realizado um novo processo de análise de vulnerabilidade para validar as ações de mitigação implementadas. O resultado dessa análise será divulgado pelo Banco, indicando se as ações de mitigação implementadas foram aceitas ou rejeitadas.		
3.5.33	A CONTRATADA deverá disponibilizar operação 24 horas, 7 dias por semana, 365 dias por ano, de monitoramento e resposta a incidentes cibernéticos, com procedimentos formalizados, com capacidade de atuação, recuperação e de coleta de evidências passíveis de compartilhamento e alinhamento com o grupo de resposta a incidentes de segurança do Banco.		
3.5.34	A CONTRATADA 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.		
3.5.35	A CONTRATADA deverá possuir procedimentos necessários para a preservação de evidências, com a possibilidade de uso em tribunais e no devido processo legal.		
3.5.36	A CONTRATADA deverá possuir processos bem definidos para tratativa de requisições e incidentes. Caso positivo, apresentar matriz com: tipo de prioridade suportada, SLA, modelo de escalonamento e canais de comunicação com o Banco.		
3.5.37	A CONTRATADA deverá possuir relatórios periódicos das requisições e incidentes (abertos e atendidos). Para tal, a CONTRATADA deverá descrever o conteúdo existente no relatório e periodicidade de envio.		
3.5.38	A CONTRATADA deverá possuire apresentar, 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 e 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.		
3.5.39	Está em conformidade com os requisitos estabelecidos na Resolução CMN 4.893/21		
3.5.40	A CONTRATADA deverá implementar controles de segurança baseados no mínimo no NIST e ISO27001.		

4.6. ARMAZENAMENTO E DADOS

Item	Descrição	Situação de Atendimento do Requisito (1 ou 2)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
3.6.1	Capacidade inicial de 1 TB (um terabyte) de armazenamento com possibilidade de expansão.		
3.6.2	A solução deve fazer uso de serviços de armazenamento em nuvem		
3.6.3	A solução deve permitir a importação de qualquer formato de arquivo ou informação		
3.6.4	Deve existir documentação explicando e exemplificando as possíveis integrações de dados para a solução		
3.6.5	Deve existir catálogo de consulta a API´s disponíveis para integração		

4.7. COMPATIBILIDADE

Item	Descrição	Situação de Atendimento do Requisito (1 ou 2)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
3.8.1	Todas as versões de softwares básicos, frameworks, servidores e quaisquer outros recursos utilizados pela SOLUÇÃO deverão ser totalmente providos pelo CONTRATADO em infraestrutura *On Cloud*.		
3.8.2	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.		
3.8.3	Todos os módulos / sistemas da plataforma ofertada deverão funcionar de forma transparente, sendo plenamente integrados entre si.		

4.8. AUDITORIA

3.9.1	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.		

3.9.2	A SOLUÇÃO deverá registrar em log específico com data/hora de envio e mensagem todos os e-mails de alertas enviado pelo sistema.		
3.9.2.	permitir que seja ativada uma trilha de auditoria para qualquer objeto da aplicação. Deve ser possível ativar esta trilha seletivamente para objetos específicos, sem que haja necessidade de ativá-la para todos os objetos. Uma vez ativada, a trilha deve registrar alterações aos campos do objeto, indicando quem fez a alteração, quando ela ocorreu, qual o valor anterior e qual o novo valor.		
3.9.3.	Possuir conformidade com padrão ICP-Brasil e compatível com a arquitetura e-PING (governo eletrônico) de assinaturas digitais.		

4.9. CONFIABILIDADE

Item	Descrição	Situação de Atendimento do Requisito (1 ou 2)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
3.10.1	A empresa deve informar o usuário com mensagens claras quando há ocorrências de falhas.		

4.10. PERFORMANCE

Item	Descrição	Situação de Atendimento do Requisito (1 ou 2)	Nível de Complexidade da Customização (Simples, Moderada ou Complexa)
3.11.1	A solução deverá ter a capacidade de processar 1.700.000 (hum milhão e setecentos mil) requisições/mês de gerentes de relacionamento e tratar 3 conversações por cliente/mês, devendo ter arquitetura escalável para tratamento do crescimento dos atendimentos		
3.11.2	Permitir que todos os relatórios possam ser: • visualizados em tela; • impressos;		

	• exportados/salvos pelo menos nos formatos .DOC; .DOCX; .XLS; .XLSX; .XLSM; .XML; .CSV; .PDF; .TXT e JSON. txt, Word, Excel (versão 2000 ou superior) html, xml e pdf e; • copiados para a área de transferência do Windows.		
3.11.3	A plataforma deverá ter a capacidade de receber, processar e gerar arquivos nos formatos: .DOC; .DOCX; .XLS; .XLSX; .XLSM; .XML; .CSV; .PDF; .TXT e JSON.		
3.11.4	Disponibilizar funcionalidades ou recursos através de dispositivos móveis, como: tablets, smartphones e notebooks.		