1. FINALIDADE

Este anexo apresenta os requisitos técnicos e funcionais para a contratação de serviços de testes sintéticos para monitoramento de sistemas de meios de pagamentos do Banco do Nordeste do Brasil.

2. REQUISITOS TÉCNICOS

2.1. Funcionalidade Gerais

2.1.1. O serviço deverá contemplar a execução de testes sintéticos de 25 (vinte e cinco) cenários de testes, sendo 10 (dez) cenários para mobile utilizando sistemas baseados em *Android*, 10 (dez) cenários para mobile utilizando sistemas baseados em iOS) e 5 (cinco) para sistemas Web.

2.1.2. O Banco indicará cada cenário de teste durante a fase de implantação.

2.1.3. Os cenários de testes poderão sofrer alterações ao longo da vigência do contrato, devendo o CONTRATADO realizar os ajustes necessários para que os testes automatizados sejam realizados de forma adequada.

2.1.4. Cada cenário poderá, a critério do Banco, ser substituído por outro ao longo da vigência contratual.

2.1.5. Deverão ser realizados testes automatizados de forma contínua durante o período e intervalo de tempo especificado em cada cenário.

2.1.6. A periodicidade de execução dos testes poderá ser definida com intervalo mínimo de 5 (cinco) minutos durante 24 (vinte e quatro) horas por dia. O Banco indicará a janela de horário de execução de teste para cada cenário.

2.1.7. O CONTRATADO deverá providenciar todos os recursos humanos e tecnológicos, além de quaisquer insumos necessários à prestação dos serviços contratados.

2.1.8. Toda a infraestrutura adequada e arquitetura de automação para a prestação do serviço deverá ser executada em ambiente do CONTRATADO, podendo, a critério da mesma, oferecer serviço em ambiente de nuvem.

2.1.9. O CONTRATADO deverá ser responsável pela integralidade dos custos, bem como a administração, conformidade legal, *backups* e disponibilidade do serviço de acordo com os parâmetros determinados pelo BANCO e pela legislação vigente.

2.1.10. O serviço deverá identificar e alertar sobre as falhas, indisponibilidades e problemas relacionados a performance (lentidão) dos sistemas e aplicativos do BANCO objetos dos cenários a serem testados. Dessa forma, deverão ser fornecidas informações pertinentes para melhoria da qualidade dos mesmos.

2.1.11. O serviço deverá contemplar *Device Farm* Física com dispositivos móveis Android e iOS para assegurar a execução com modelos e sistemas operacionais distintos.

2.1.12. O serviço deverá ser executado a partir de múltiplos dispositivos, com variados Sistemas Operacionais, sendo utilizado, pelo menos, as três versões mais recentes de cada fabricante Android e IoS.

2.1.13. Para testes da página web, deverão ser utilizados diferentes navegadores tais como Google Chrome, Edge e Mozila Firefox, nas versões mais recentes.

2.1.14. As versões de sistemas operacionais e navegadores a serem utilizados nos testes devem ser previamente acordados com o Banco.

2.2. Painel de Monitoramento

2.2.1. Deverá ser disponibilizado *dashboard* (painel) de acompanhamento das execuções em tempo real, que mostrem, no mínimo, as seguintes informações: cenário de testes, resultados, informações sobre erros, caso ocorram, volume de execuções com sucesso e com erros, horários e tempo sem incidente.

2.2.2. O dashboard deverá ser acessado por meio de navegador web com uso de requisitos que garantam a segurança, como por exemplo, uso de criptografia na conexão (SSL).

2.2.3. O acesso ao dashboard deverá ser autenticado com a utilização de usuário/senha e que permita múltiplos acessos simultâneos.

2.2.4. Deverá implementar a criação de níveis de acesso (perfis) com limitações e permissões diferenciadas.

2.2.5. As informações apresentadas no dashboard deverão estar disponíveis em língua portuguesa, podendo apresentar informações em outra língua nos casos em que não existam tradução.

2.2.6. Deverá possibilitar consultas ao histórico das execuções dos testes no período dos 6 (seis) últimos meses, com filtros customizados, tais como: por período (mês, semana, dia, hora), sistema, plataforma (Web, Android, iOs), ente outros.

2.3. Relatórios

2.3.1. Deverão ser enviados para o Banco com periocidade diária, relatórios que deverão conter, no mínimo:

2.3.1.1. Cenários com erros;
2.3.1.2. Data/Hora da identificação do erro manual;
2.3.1.3. Data/Hora da notificação ao Banco;
2.3.1.4. Volume de cenários automatizados executados com status: sucesso, falha e em manutenção;
2.3.1.5. Visão de status por cenário, usuários e sistemas (sítios e aplicativos).
2.3.1.6. Quantidade de cenários automatizados executados com sucesso;
2.3.1.7. Quantidade de cenários automatizados executados com erro;
2.3.1.8. Número de defeitos encontrados em comparação com o total de testes realizados.

2.4. Comunicação

2.4.1. Em caso de detecção de mau funcionamento, lentidão ou indisponibilidade de qualquer um dos cenários de testes, deverão ser reportados ao Banco, de acordo com o fluxo de escalada para resolução de incidentes conforme definição durante fase de configuração;

2.4.2. O BANCO disponibilizará os contatos adequados para que os problemas encontrados sejam reportados de acordo com cada cenário/gravidade;

2.4.3. Durante a comunicação o CONTRATADO deverá informar, no mínimo:

2.4.3.1. Código para identificação do erro

2.4.3.2. Descrição do erro

2.4.3.3. Cenário que ocorreu o erro

2.4.3.4. Data/Hora da identificação do erro manual

2.4.3.5. Data/Hora da notificação ao Banco do Nordeste

2.4.3.6. Detalhes do erro (passo a passo)

2.4.3.7. Massa de dados utilizada

2.4.3.8. Browser ou sistema operacional onde ocorreu o erro

2.4.3.9. Modelo do aparelho para o caso de APP

2.4.3.10. Evidência do erro

2.4.4. Deverá possuir motor de gerenciamento de alarmes que permita a configuração de grupos solucionadores para o recebimento de notificações via e-mail em caso de problemas identificados em produção.

2.4.5. Deverá possibilitar integração via API com os serviços de monitoramento já utilizados pelo Banco, permitindo o envio automático dos dados gerados pelos testes.

2.4.6. Deverá possibilitar a abertura automática de chamados, via API, nas ferramentas de gestão de tickets adotadas pelo Banco.

2.4.7. Todas as informações resultantes dos testes serão de propriedade do BANCO, não podendo ser divulgadas ou acessadas por terceiros, devendo o CONTRATADO manter a confidencialidade e segurança da informação;

2.4.8. O CONTRATADO deverá manter a base de dados com resultados dos testes, ficando disponível para o banco para fins de consulta. Ao final do contrato, O CONTRATADO deverá fornecer cópia de segurança (backup) integral dos dados armazenados e *script´*s utilizados e, após aceite do BANCO, providenciar a exclusão dos mesmos.

2.4.9. O CONTRATADO deverá usar Inteligência Artificial com base estatística e preditiva dos dados coletados, a fim de fornecer informações úteis para evitar falhas ou interrupções, identificando padrões de operações tais como

lentidão na conclusão do teste, horários de maior incidência de resultados falhos, entre outros.

2.5. Segurança

2.5.1. Deverão ser observados os regulamentos, normas e instruções de segurança da informação e comunicações adotadas pela CONTRATANTE, incluindo as Políticas e Diretrizes de Governo, normativos associados ou específicos de Tecnologia da Informação, Política de Segurança da Informação e Comunicações – POSIC e Normas Complementares – NC do Gabinete de Segurança Institucional – GSI da Presidência da República – PR;

2.5.2. Deverá estar em conformidade com a ISO/IEC 27001- padrão para sistema de gestão da segurança da informação (ISMS – *Information Security Management System*). Esta norma foi elaborada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Uma solução em nuvem tem que adotar um SGSI e ser certificado nessa norma. A especificação e implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, exigências de segurança, os processos empregados e o tamanho e estrutura da organização.

2.5.3. Deverá estar em conformidade com a ISO/IEC 27017:2015 que fornece orientações quanto aos aspectos de segurança de informações de computação em nuvem, recomendando a implementação de controles de segurança de informações específicas da nuvem que complementam a orientação das normas ISO/IEC 27001. Esse código de práticas disponibiliza instruções de implementação de controles adicionais de segurança da informação específicos para provedores de serviços de nuvem.

2.5.4. Deverá estar em conformidade com a ISO/IEC 27018:2014 que é um código de práticas concentrado na proteção de dados pessoais na nuvem. Ela é baseada no padrão de segurança da informação e fornece orientação sobre a implementação dos controles aplicáveis às Informações de

Identificação Pessoal (PII) de nuvens públicas. Esta Norma estabelece objetivos de controle, controles e diretrizes comumente aceitos para implementação de medidas para proteger as Informações de Identificação Pessoal (PII) de acordo com os princípios de privacidade.

3. CUSTOS E RESPONSABILIDADES

3.1. O Contratado deverá providenciar a abertura e manutenção das contas bancárias utilizadas nos testes.

3.2. As tarifas referentes ao Banco do Nordeste serão isentas, porém, O CONTRATADO deverá prever os custos tarifários do outro Banco utilizado nos testes.

3.3. Os testes deverão utilizar os aplicativos e sítio publicados na internet, arcando com os custos de acesso com links de comunicação, equipamentos, bem como todas os itens necessários para as medições/coletas, acompanhamento e evidências dos resultados dos testes.

3.4. Para os envios e recebimentos, o CONTRATADO deverá manter saldo bancário em ambos os bancos suficiente para a realização de transferências durante todo o período de realização de testes a depender do cenário a ser testado.

3.5. Fica a critério do CONTRATADO o equilíbrio de saldos para que haja saldo suficiente para a realização dos testes.

3.6. O ônus dos saldos será do CONTRATADO.

3.7. Para otimização de custos, sugere-se que os testes sejam executados com PIX no valor de R$ 0,01 (um centavo de Real).

3.8. Para o cenário de testes do TED, será necessário apenas teste de envio para outra instituição, tendo como origem conta do Banco do Nordeste (BNB).

3.8.1.1. Os testes de TED a cada 5 (cinco) minutos deverão ser executados apenas em dias úteis entre o horário das 6h às 16h30.

3.8.1.2. A frequência de envio poderá ser readequada a critério do BANCO, quantas vezes forem necessárias, a fim de não prejudicar às operações da instituição.

4. SERVIÇO DE IMPLANTAÇÃO

4.1. O Contratado deverá cumprir o plano de implantação do serviço está descrito no Anexo III – Plano de implantação.

5. SERVIÇO DE ASSISTÊNCIA E SUPORTE TÉCNICO

5.1. O Contratado deverá prestar Serviço de Assistência e Suporte Técnico conforme especificações previstas no Anexo V – Assistência Técnica e Suporte.