Na Mídia

27/04/2021 | LexLatin

As novas versões dos manuais de funcionamento do open banking no Brasil

Fabio de Almeida Braga*

Normas fixam requisitos técnicos e procedimentos operacionais específicos para cada função.

Etiquetas:

o que é open banking? Normas de transparência Instrução normativa Banco Central Brasil

O Banco Central deu continuidade ao processo de definição regulatória visando a orientar os trâmites de implementação do Sistema Financeiro Aberto no Brasil (o open banking brasileiro), editando cinco Instruções Normativas (INs) dedicadas a temas específicos.

Seguindo, então, o previsto no artigo 3º da Resolução BCB 32/20, o Banco Central estabeleceu por meio das referidas INs o detalhamento de requisitos operacionais para a implementação do open banking, os quais deverão constar dos seguintes manuais: manual de escopo de dados e serviços, manual de APIs, manual de serviços prestados pela estrutura responsável pela governança do open banking, manual de segurança e manual de experiência do cliente no Open Banking.

Manual de APIs. Nesse passo, a IN 95 divulga a versão 2.0 do manual de APIs, incorporando, alterando e aprimorando os requisitos da Fase 2 do open banking e demais seções do manual de APIs do open banking.

Foram, assim, introduzidas novas definições acessórias que deverão ser publicadas pela estrutura responsável pela governança do open banking, no portal do open banking, sob a forma de um guia de estilo de especificações de APIs, contemplando definições e recomendações para:

Estrutura de Uniform Resource Identifiers URIs;

Cabeçalhos HTTP;

Códigos de status HTTP

Convenções de corpo de requisições e respostas;

Convenções de nomenclatura;

Tipos de dados comuns;

Paginação e

Estabilidade de gerência de mudanças.

Por outro lado, considerando a intensa utilização de terminologia própria da área de tecnologia no ambiente de interação entre os participantes, a IN 95 traz definições para expressões comumente empregadas, a saber:

API (Application Programming Interface): que consiste em um conjunto definições sobre como um sistema pode acessar dados ou funcionalidades providos por um outro sistema;

REST (Representational State Transfer): que designa o estilo arquitetural de um software;

API RESTful: como sendo o API que adere às restrições do estilo arquitetural REST;

OpenAPI: que é a linguagem de especificação de APIs RESTful;

Endpoint: elemento de uma especificação OpenAPI sobre o qual podem ser executadas operações para acessar dados ou funcionalidades;

HTTP (Hypertext Transfer Protocol): consistente no protocolo para sistemas hipermídia, distribuídos e colaborativos; e

Operação: que é o elemento de uma especificação OpenAPI que declara uma maneira válida de se acessar um Endpoint, informando, por exemplo, qual método HTTP (GET, POST, etc.) utilizar, nomes e tipos de parâmetros, etc.

Além de aprofundar aspectos inerentes aos elementos de especificação de APIs, a IN 95 adicionou funcionalidades específicas à tabela de APIs do open banking, referentes a “consentimento”, “dados

cadastrais", "cartão de crédito", "contas" e "operações de crédito". O API de Consentimento é descrito como aquele que deverá permitir a criação, consulta e revogação de consentimentos por parte dos clientes e usuários; o API de Dados Cadastrais servirá para permitir o acesso a dados de clientes e seus representantes; o API de Cartão de Crédito propiciará o acesso a dados de contas de pagamento pós-pagas; o API de Contas possibilitará o acesso a dados de contas de depósito à vista, de poupança e pré-pagas e, por fim, o API de Operações de Crédito permitirá acesso a operações do tipo empréstimo, financiamento, adiantamento a depositantes e antecipação de recebíveis (direitos creditórios descontados).

Aspecto igualmente relevante diz respeito à manutenção de uma relação de alterações das APIs, que deverão ter as suas versões já publicadas devidamente listadas no portal do open banking (e respectivos períodos em que estiveram em produção). Desse modo, a estrutura responsável pela governança do open banking deverá estabelecer e publicar no portal do open banking o processo que adotará para gerenciar essas alterações nas especificações de APIs.

Por último, cumpre destacar a inserção no manual da obrigatoriedade de que todas as informações para desenvolvimento, testes e entrada em produção de aplicações ou APIs deverão estar disponíveis em tutoriais no portal do open banking. Cada um desses tutoriais deverá contemplar os passos para o completo desenvolvimento da atividade em questão.

Manual de escopo de dados e serviços do open banking. Pela IN 96, o Banco Central divulgou a versão 2.0 desse manual, que, em particular, introduz mudanças relativas a regras e requerimentos para o compartilhamento de dados cadastrais e transacionais de clientes relacionados a contas de depósito à vista ou de poupança, de pagamento pré-pagas ou pós-pagas e operações de crédito.

As novidades trazidas nesta versão 2.0 do manual estão relacionadas a explicitações contidas ao longo de todos os pontos de observância obrigatória, tais como aquele que se refere à exigência de que o consentimento prévio do cliente, para finalidades e prazos determinados, também seja exigência para o compartilhamento dos dados cadastrais e transacionais de clientes previstos no manual.

De igual modo, o manual atualizado passa a contemplar que, mediante prévio consentimento e desde que observadas finalidades e prazo determinados, os participantes devem observar a obrigatoriedade de compartilhamento de dados sobre cadastros dos clientes. Desse modo, o manual determina que sejam observados requisitos básicos referentes aos dados sobre o cadastro de clientes e de seus representantes, pessoas físicas ou jurídicas.

Em relação a pessoas físicas, assim, devem ser contemplados os seguintes dados:

Identificação, mediante nome completo, CPF, endereço residencial, meios de contato, estado civil e filiação;

Qualificação, mediante indicação de frequência de renda e seu valor e ocupação; e

Relacionamento, mediante indicação da data de início do relacionamento com a instituição, tipos de produtos e serviços mantidos, natureza de conta e identificação do representante, quando for o caso.

Em relação a pessoas jurídicas, assim, devem ser contemplados os seguintes dados:

Identificação, mediante indicação da razão social, seu nome de fantasia, data de constituição, CNPJ, endereço, meios de contato, identificação do representante e sua qualificação (sócio ou administrador);

Qualificação, mediante indicação de ramo de atuação principal e secundária, frequência de faturamento e seu valor (com indicação de seu ano de referência);

Relacionamento, mediante indicação da data de início do relacionamento com a instituição, tipos de produtos e serviços mantidos, natureza de conta e identificação de representante.

No tocante a dados transacionais, o manual prevê que sejam compartilhadas informações concernentes a dados das contas de depósito à vista ou de poupança e de pagamento pré-pagas, mediante indicação de sua identificação, seu saldo disponível, tipos de transações realizadas na conta, valores, datas, identificação de pagadores e recebedores e suas instituições. Além desses dados, devem ainda ser consideradas informações relativas a limites contratados em relação a cheque especial e de operação de adiantamento a depositantes.

Já quanto a contas de pagamento pós-pagas, a nova versão do manual contempla a indicação de tipos de conta, de limites de crédito total associados a cartões de crédito, limites por modalidade de operação associada a cartões de crédito, transações realizadas e pagamento de faturas.

Por fim, quanto a operações de crédito, devem ser consideradas informações a respeito da identificação do contrato, mediante indicação das modalidades de crédito contratadas (se financiamentos, empréstimos, direitos creditórios descontados ou adiantamentos), datas e valores contratados, CET, sistema de amortização e CNPJ do ente consignante, quando aplicável. Tão mais relevantes, ainda, são as informações que deverão ser disponibilizadas sobre tarifas, encargos, taxas de juros remuneratórios e garantias.

Manual de experiência do cliente. Por meio da IN 97, o Banco Central introduziu esse manual de observância obrigatória por parte das instituições participantes, com o propósito de definir princípios básicos sobre o tema, em complemento à regulamentação em vigor, de modo a garantir que a experiência consentida de compartilhamento de dados vivenciada pelos clientes com e entre participantes do open banking seja segura, ágil, precisa e conveniente, de modo a assegurar a confiabilidade no uso de todo o sistema de compartilhamento.

São, assim, fixados como princípios da experiência de compartilhamento a segurança e privacidade, a agilidade, a conveniência e o controle e a transparência. Quanto à segurança e privacidade, é certo que o ambiente de compartilhamento deverá estar cercado de segurança tecnológica que garanta a privacidade dos dados pessoais dos clientes e esteja em conformidade com a legislação de proteção de dados pessoais em vigor.

Quanto à agilidade, o manual prevê que o compartilhamento seja concluído em prazo compatível com o nível de complexidade e os seus objetivos, assegurando meios necessários para a livre escolha e a decisão fundamentada do cliente, quer se trate de jornada simples de compartilhamento de dados, quer se trate de jornada múltipla.

Em relação à conveniência e controle, o manual prescreve que o compartilhamento deverá ser realizado para atendimento de fins específicos e de maneira conveniente e acessível ao cliente, inclusive quanto aos canais de acesso às instituições participantes, sendo garantidas ao cliente as condições de controle de seus próprios dados pessoais quando compartilhados no ambiente do open banking.

O aspecto da conveniência fica ainda mais claro quando se considera a determinação do manual de que o centro da jornada de compartilhamento é o próprio cliente - não qualquer instituição participante -, de modo que se assegure ao cliente a adequação de todo o processo ao seu próprio perfil, às suas necessidades e expectativas quanto aos produtos e serviços, à disponibilização de informações e condições de exercício de sua prerrogativa

de concessão ou revogação de consentimentos, conforme qualquer dessas medidas lhe seja conveniente e oportuna.

Em matéria de transparência, o manual contempla o princípio de que os clientes devem ter à sua plena disposição informações claras e precisas, com objetividade e adequação a propósitos certos durante o compartilhamento de dados. Os clientes devem ser informados, por meio de linguagem simples e compreensível, sobre os dados que serão objeto de compartilhamento e os motivos que justificam o atendimento das finalidades objetivadas, sempre de modo claro, tempestivo e em volume suficiente para a sua tomada de decisão de maneira inequívoca.

Esse novo manual prevê, ainda, a elaboração e disponibilização às instituições participantes e ao público em geral, mediante publicação no portal do open banking, por parte da estrutura responsável pela governança do open banking de guia de experiência do cliente, o qual reunirá procedimentos e requisitos a serem observados por todas as instituições na interação com clientes, ao longo da jornada de compartilhamento.

A estruturação do guia de experiência do cliente deverá se dar de modo coeso e claro, contendo telas de exemplos ilustrativos das etapas da jornada, sendo os seus dispositivos expressos sob a forma de requisitos (com disposições de observância obrigatória) e recomendações que, embora não sejam de observância obrigatória, estejam alinhadas às boas práticas para a experiência do cliente.

O guia de experiência do cliente deverá apresentar conteúdo mínimo que disponha sobre o fluxo das etapas da jornada simples e da jornada múltipla de compartilhamento, com a identificação do cliente, indicação das finalidades relacionadas ao consentimento, da seleção de dados a serem compartilhados e da seleção do prazo de compartilhamento, assim como da seleção da instituição transmissora e do redirecionamento para o ambiente da mesma instituição.

Além disso, devem constar do guia a autenticação do cliente na instituição transmissora e a confirmação de compartilhamento pelo cliente na mesma instituição, acrescido de informação sobre o ambiente de gestão dos consentimentos e a terminologia utilizada pelas instituições ao longo de ambas as modalidades de jornada.

Manual de serviços prestados pela estrutura responsável pela governança do open banking. Por meio da IN 98, o Banco Central tratou de divulgar ao mercado a nova versão desse Manual, cuja importância reside na fixação de requisitos técnicos para a implementação dos elementos de infraestrutura que permitirão a operacionalização do Open Banking, a começar do diretório de participantes, no qual são reunidas as funcionalidades críticas do sistema, tais como o gerenciamento de credenciais dos participantes e o monitoramento das APIs.

Acresça-se a isso o propósito de manterem-se canais de acesso e suporte ao diretório e de encaminhamento de demandas aos participantes, assim como propiciar-se a disponibilização de informações por meio do portal do open banking, com a finalidade de promover a comunicação entre participantes e entre estes e o público em geral.

Outra função de extrema relevância a ser disponibilizada dentre os serviços a serem prestados pela Estrutura Responsável pela governança do open banking consiste na disponibilização de ambiente de testes para APIs em regime de flexibilização temporária de regulação (Sandbox), de modo a tornar possível o apoio a inovações promovidas pelas instituições participantes. Nada obstante, prevê-se que haja, naturalmente, o desenvolvimento de um processo de evolução dos serviços prestados que seja o reflexo da própria evolução do Open Banking no País, razão por que esse manual deverá permanecer em constante estado de revisão e atualização.

A começar pelo diretório de participantes, saliente-se que se trata do ambiente e do repositório de formalização da participação de uma instituição no Open Banking, de modo que possa participar do processo de

compartilhamento de dados e informações, de iniciação de transações de pagamento e de encaminhamento de propostas de operação de crédito por meio das APIs.

No ambiente do diretório, os participantes poderão realizar atividades como o gerenciamento de identidades e acessos, gerenciamento de identidades e autorização de aplicações e gerenciamento de informações do próprio diretório.

Os testes de conformidade e registro de APIs constituem uma novidade introduzida no Manual pela IN 97 e consistem em verificar, por meio de testes, a conformidade de APIs de cada participante, contemplando aspectos funcionais e não funcionais, tais como, respectivamente, avaliações de aderência das implementações às especificações das APIs e a avaliação de atendimento por parte de APIs de requisitos de segurança. Caberá à estrutura de governança certificar os resultados dos testes de conformidade, passando tal certificação a ser considerada uma condição precedente para o registro da implementação da API no ambiente de produção do diretório.

O manual estabelece, também, conteúdo mínimo de acordos de nível de serviço do diretório, assim como de seus padrões de monitoramento de desempenho e de disponibilidade para armazenar e disponibilizar dados estatísticos de desempenho do Open Banking.

Dois outros temas são também tratados pelo manual: o ambiente de service desk e o portal do open banking. Àquele cumprirá centralizar as requisições e a manutenção de tíquetes de suporte técnico relacionado ao diretório, às APIs e aos dados e serviços compartilhados entre os participantes. Já no tocante ao Portal, o manual dispõe sobre as suas diretrizes contemplando acessibilidade, linguagem e tempestividade, segurança, sigilo e proteção de dados, além de contemplar três áreas de interação: área do desenvolvedor, contendo especificações técnicas referentes a vários temas de infraestrutura de funcionamento do Open Banking; área do cidadão, contendo informações voltadas para o aprimoramento da experiência do cliente; área do participante, com informações voltadas a temas de interesse das instituições participantes.

Manual de segurança do open banking. Por derradeiro, o Banco Central cuidou de divulgar a versão 2.0 do Manual de Segurança, editando a IN 99, por meio da qual são introduzidos elementos e medidas técnicas destinados a garantir a operacionalização do Open Banking, mediante o seguro compartilhamento de dados sobre canais de atendimento e produtos e serviços relativos a contas de depósito à vista e poupança, contas pré- e pós-pagas e operações de crédito, além do compartilhamento de dados de cadastro de clientes e de transações relativas aos mesmos produtos e serviços referidos acima.

A versão do manual divulgada pela IN 99 altera disposições a respeito da estrutura de Governança que deve ser mantida pelas instituições participantes quanto à conformidade estrita de suas práticas e procedimentos com a legislação e atos normativos que gerem impacto sobre o gerenciamento de todas as funcionalidades e aspectos de infraestrutura de operação do open banking.

As disposições sobre proteção que passam a constar dessa versão do manual também estão revistas e acrescidas de vários aspectos técnicos relevantes, como segregação lógica de sistemas e APIs dentro do ambiente operacional de cada instituição participante, implementação de criptografia na comunicação com APIs expostas publicamente e desativação das funcionalidades “TLS Session Resumption” e “TL Renegotiation”.

A comunicação com APIs e a assinatura de mensagens deverão ser realizadas mediante certificação digital válida emitida por certificadora que integre o sistema ICP-Brasil, contemplando mecanismos para a proteção dos canais de comunicação e para a assinatura ou criptografia de mensagens entre APIs.

Houve a introdução de nova redação relativa aos critérios de detecção de interações no ambiente do open banking que sejam capazes de permitir o aprofundamento de trilhas de auditoria, assim como relativa à reação por parte das instituições participantes diante de riscos cibernéticos ou da necessidade de tratamento de incidentes em andamento, mediante implementação de bloqueios de acesso às APIs, observada a política de segurança cibernética de cada instituição.

A IN 99 promoveu o acréscimo, por último, de um tópico especificamente voltado para as questões de segurança atinentes à própria estrutura responsável pela governança do open banking. Assim, a estrutura de governança passa a ter de observar requisitos básicos sobre esse tema, tais como, dentre outros, a obrigatoriedade de condicionar à autenticação por múltiplos fatores o acesso às áreas restritas do diretório de participantes, além de implementar e manter uma política de segurança cibernética, a qual deverá levar em conta princípios e diretrizes conducentes à confidencialidade, à integralidade e à disponibilidade de dados e sistemas de informação.

A atualização de todos esses manuais operacionais, fixando requisitos técnicos e procedimentos operacionais específicos para cada função constitui mais outro relevante passo no processo de implementação da experiência do open banking no mercado brasileiro.

***Fabio de Almeida Braga é sócio da área bancária do Demarest Advogados.**