



Na Mídia

19/09/2024 | [Finsiders Brasil](#)

Bancos digitais são seguros? Entenda

Assim como os bancos tradicionais, essas instituições são reguladas e fiscalizadas pelo Banco Central (BC)

Redação Finsiders Brasil



Imagem: Adobe Stock

Seis a cada dez brasileiros optaram por bancos digitais na hora de abrir contas no ano passado. É o que diz levantamento anual feito pela empresa de gestão de identidade digital idwall.

Mas afinal, bancos digitais são seguros? Para responder a pergunta, vamos abordar neste texto dois aspectos:

- Respaldo regulatório
- Segurança cibernética

Meu dinheiro pode sumir?

Bancos digitais podem ser a versão digital de um banco físico, ou então nascerem digitais. Neste segundo caso, eles têm toda a sua estrutura 100% digital. Ou seja, não existem agências bancárias físicas acessíveis a clientes.

Dessa forma, todos os processos, transações e acessos ocorrem pela internet — geralmente, por aplicativos de smartphones.

Isso não significa que o dinheiro dos clientes pode simplesmente “sumir” em caso de fraude, por exemplo. Assim como as instituições financeiras tradicionais, os bancos digitais são regulados e supervisionados pelo Banco Central (BC). Geralmente, essas empresas atuam como instituições de pagamento (IP), que devem seguir a regulamentação do BC conforme a Lei nº 12.865/2013.

Algumas começam como IP e na medida em que crescem, adquirem licenças de financeira ou banco múltiplo (casos do Nubank e do PicPay). E alguns outros que atuam como bancos digitais são usuários de softwares de terceiros. Neste caso, são conhecidos no mercado como banking as a service (BaaS), ou banco como serviço. Estes, por sua vez, são obrigatoriamente no mínimo uma IP.

Ser regulado pelo BC significa que precisam prestar informações e manter controles dos balanços, ter capital para garantir problemas de liquidez e outras obrigações.

Regras de segurança

Em qualquer caso, todos precisam seguir normas relacionadas à segurança cibernética, aponta Fabio Braga, sócio da área de Direito Bancário e Financeiro do Demarest Advogados. Quem define essas regras são o BC e o Conselho Monetário Nacional (CMN). Isso significa que, em tese, os clientes deles podem ficar tranquilos. Se ocorrer algum problema, ao menos têm como reclamar e serem ressarcidos.

A Resolução CMN 4.893/21, por exemplo, define como deve ser a política de segurança cibernética da instituição. Além disso, estabelece os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Essas regras podem ser acessadas pelos clientes a partir dos sites oficiais das instituições. Elas servem para garantir a proteção das informações dos clientes. Definem, por exemplo, o nível de segurança que cada informação deve receber.

A política de segurança cibernética de cada banco também precisa definir critérios para resolver casos de ataques cibernéticos que eventualmente ocorram.

A política de segurança cibernética deve contemplar:

- Os objetivos de segurança cibernética da instituição;
- Os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética;
- Os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;
- O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição.