NOVEMBRO

digital money inform

CENÁRIO DO NOVO ECOSSISTEMA FINANCEIRO DIGITAL

Pix

Até que ponto os dados são seguros?

Com o início do funcionamento do Pix, o mercado financeiro se volta para a proteção contra as fraudes. A participação de instituições não financeiras no Open Banking também requer cuidados adicionais na segurança de dados.

Cadastro Positivo

Birôs de crédito se mostram otimistas

Milhões de brasileiros começam a construir o seu histórico de crédito. Quanto mais informações disponíveis sobre o tomador de crédito, mais eficiente se torna a avaliação de risco e, por consequência, mais negócios podem ser realizados. Mesmo em tempos de crise, a expectativa é positiva para o mercado.

momento EDITORIAL

APRESENTAÇÃO

Com a entrada em funcionamento do Pix os modelos de segurança de dados precisam de novos parâmetros, tecnologias mais robustas e esse é o desafio do mercado financeiro. A criatividade do fraudador no Brasil é muito grande e desafia as instituições financeiras permanentemente.

Esse é o tema de capa do terceiro caderno do E-book Digital Money Inform, que traz as visões e opiniões do Banco Central, da Febraban, e de responsáveis pela segurança de empresas como IBM Brasil, Kryptus e Fortinet.

O cadastro positivo também é abordado neste terceiro caderno do Digital Money *Inform. Em entrevista exclusiva, Elias Sfeir, presidente da Associação Nacional* dos Bureaus de Crédito (ANBC) fala sobre a importância dos consumidores construírem seu histórico de crédito para ter prazos maiores e juros melhores e do papel disruptivo que a criação de uma moeda digital com características globais trará para os meios de pagamento, acelerando a economia e gerando bem estar e empregos.

O objetivo é abordar as questões mais importantes que envolvem o novo ecossistema de pagamento instantâneo, o Pix, e do Open Banking. O Digital Money ainda conta com mais um caderno a ser divulgado ainda neste ano. Leia e acompanhe!

Equipe Tele.Síntese.

EXPEDIENTE

momento EDITORIAL

Editora-Executiva
Miriam Aquino

Edição
Cândida Bittencourt

Reportagem
Vera Franco

Edição de Arte
Rael Lamarques

Imagens/Ilustrações
Freepik | Banco de imagens das empresas entrevistadas

Publicidade
Zélia Maria
ZMC Representações
F.: (61) 99986.2467
zelia@zmcrepresentacoes.com

Web e Suporte de Rede
Ricardo Oliveira

Administrativo
Adriana Rodrigues

Distribuição
Camila Carvalho

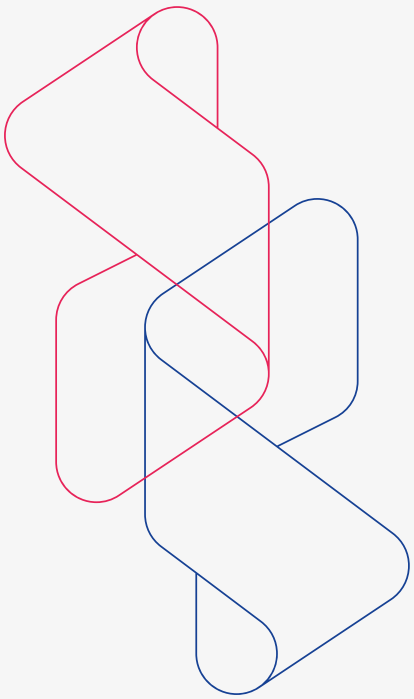
surf

Conheça a nova onda.

INCLUSÃO DIGITAL ÚNICA:
SERVIÇOS DE **CONEXÃO**
E SOLUÇÕES **FINANCEIRAS**.

surf CONNECT

Fazemos de uma marca, **uma nova operadora**.



surf FINTECH

Uma conta digital com **cartão de crédito**, **serviços financeiros** e **empréstimo**.

surf.com.br

SEGURANÇA NO PIX

É DESAFIO PARA MERCADO FINANCEIRO

A indústria financeira brasileira tem sistemas de segurança evoluídos, mas a dúvida é para o tipo de fraude que pode ocorrer com o pagamento instantâneo e com o open banking.

Por Vera Franco

A transformação digital, intensificada com a chegada da pandemia do coronavírus, acelerou a descentralização da tecnologia da informação no sistema financeiro brasileiro. Hoje, a mesma solução oferecida por grandes bancos, instituições de menor porte e fintechs entregam para o cliente o mesmo nível tecnológico de serviço, segundo Rafael Pereira, presidente da Associação Brasileira de Crédito Digital (ABCD). A democratização da tecnologia traz segurança mais barata e com muitos players envolvidos. Começamos a conviver com serviços distribuídos e uma maior variedade e circulação de dados expostos em muitos pontos de contato.

O movimento de descentralização ganhou massa crítica com a chegada do novo sistema de pagamento instantâneo do Banco Central, Pix, que promove a redução de custo das transações de pagamento, e open banking, a simetria da informação. Antes pautado para aumentar a competitividade, o sistema financeiro volta-se agora para dar mais poder ao usuário, especialmente com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD). Com isso, aumenta a quantidade de opções de informações espalhadas por todos os cantos e, potencialmente, os riscos de segurança.

O setor bancário brasileiro investe R$ 24,6 bilhões por ano em tecnologia da informação para a modernização de sua infraestrutura, processos e sistemas tecnológicos. Desse total, cerca de 10% são dirigidos à segurança, segundo a Federação Brasileira dos Bancos (Febraban).

A digitalização durante o período da pandemia expandiu a quantidade de golpes, especialmente os tradicionais de engenharia social. O Whatsapp foi um dos meios mais usados por fraudadores, fazendo com que alguém desse por vontade própria suas informações pessoais a outrem. Não ocorreram, no entanto, muitos ataques por ransomware no país, quando os servidores são sequestrados.

"Embora a segurança do sistema financeiro brasileiro seja bem evoluída, o grande desafio enfrentado com a entrada em operação do Pix e open banking é não sabermos que tipo de fraude vem pela frente", explica Alberto Miyazaki, CTO da IBM Brasil. Segundo ele, as instituições precisam ter uma visão unificada da tecnologia de segurança que considere pessoas treinadas e processos atualizados.

Detecção demorada

Os crimes cibernéticos já começam a ser contratados como campanhas de phishing, por exemplo, e há casos de malware negociados no Brasil e desenvolvidos no exterior, afirma João Rocha, head de security da IBM Brasil.

> *"Embora a segurança do sistema financeiro brasileiro seja bem evoluída, o grande desafio enfrentado com a entrada em operação do Pix e open banking é não sabermos que tipo de fraude vem pela frente."*
>
> **Alberto Miyazaki**
> CTO da IBM Brasil.

A média para detectar a violação de dados é de 280 dias e 115 para conter, conforme o estudo IBM 2020 que analisou 524 violações ocorridas em organizações de diferentes portes, em 17 países, no período de agosto de 2019 a abril deste ano. Existe uma demora muito grande para correlacionar o roubo. “O atacante não quer quebrar a janela da casa. Quanto mais silencioso mais bem sucedido será em sua investida de extorquir a vítima”, explica Rocha.

A maioria dos gastos com violação são relacionados a perda de negócio e 27% das empresas recuperam mais rápido quando dispõem de ferramentas de inteligência artificial e automação dentro de casa. Se a resposta é mais rápida consegue-se estancar o sangramento. Durante a pandemia, o número de incidentes aumentou 40%.

Na avaliação de Rocha, o Brasil encontra-se hoje em uma posição pior que a média global em relação à sua proteção de segurança bancária. “Demora mais para detectar a fraude devido ao baixo investimento realizado em postura de segurança e treinamento de pessoas qualificadas”, diz.

O setor bancário brasileiro é muito bem regulado e controlado. O Banco Central tem uma regra que obriga a manutenção dos registros bancários pelo período de 20 anos e existe um respaldo maior em

> *Em um ecossistema com vários participantes dividindo a base de clientes multiplica-se o número de novos ataques e a configuração do risco de um para cinco bancos passa a ser de um para mil fintechs.*
>
> **Roberto Gallo**
> CEO da Kryptus

O brasileiro tem muita tolerância ao risco, o que se reflete em redução de medidas preventivas, e a legislação brasileira é muito ruim na hora de punir.

relação aos controles. O que preocupa o mercado é a chegada de instituições não financeiras participantes das novas plataformas Pix e open banking. As lojas de comércio eletrônico, por exemplo, não têm qualquer tipo de regulamentação.

“Um site de entrega de flores, por exemplo, tem o security by design, que é um check list de segurança enquanto o open banking e Pix lidam com riscos sistêmicos. A preocupação dos riscos sistêmicos e os controles do BC versus outros segmentos que não têm esse risco de maturidade e controle”, afirma.

Para Marcelo Branquinho, CEO da TI Safe, a participação de empresas não financeiras na plataforma aberta open banking representa risco garantido. “Os grandes bancos contam com equipe de TI bem estruturada, plataformas e aplicativos com segurança, ambiente de desenvolvimento seguro em compliance com a LGPD e distribuição de dados privados. Enquanto as empresas de menor porte dispõem de estruturas bem menores e menos parrudas”, explica.

A empresa pode ter o aplicativo mais seguro do mundo, se não tiver uma boa arquitetura da infraestrutura de segurança há chance de ocorrer problemas. Atualmente, 51% dos incidentes de segurança são relacionados à falta de conhecimento do usuário e configuração da arquitetura. De acordo com pesquisa da Carnegie Mellon University, mais da metade dos problemas de segurança estão na arquitetura e não nos aplicativos.

“O mercado hoje é concentrado em cinco bancos, portanto, se há um problema de segurança no portal do banco A, a capacidade de causar estragos é multiplicada pelo tamanho do player. Em um ecossistema com vários participantes dividindo a base de clientes multiplica-se o número de novos ataques e a configuração do risco de um para cinco bancos passa a ser de um para mil fintechs”, diz Roberto Gallo, CEO da Kryptus. Os players estão saindo de um ambiente no qual controlam tudo para outro em que é preciso confiar no parceiro.

Nesse cenário é importante considerar a segmentação da fraude, pois para passar dados de um ponto para o outro é preciso criptografar. Para Gallo, o Hardware Security Model (HSM) é o padrão de ouro para a indústria financeira por oferecer segurança extra para o armazenamento de chaves criptográficas. O padrão HSM funciona como um cofre digital que possui recursos invioláveis e autodestrutivos que são ativados em caso de tentativa de fraude.

Em termos de segurança, a Europa baseia-se no mercado suíço, considerado o mais maduro. Lá é preciso criptografar em nuvem para proteção, tornando o ambiente mais preventivo em termos de tecnologias e de processos. O objetivo é deixar as fraudes em níveis aceitáveis. Se aperta demais pode denegrir a transação financeira.

"Existem muitos pontos de atenção. A ponta para dentro do sistema e a ponta para fora, o consumidor. O problema catastrófico é quando um criminoso consegue a chave criptográfica que assina a transação financeira", afirma. O Sistema de Pagamento Brasileiro (SPB) do Banco Central já usa o padrão ouro (Golden Standard). Segundo ele, no Sistema de Pagamento Instantâneo (SPI) é recomendado o padrão ouro, que permite maior interoperabilidade.

Como uma em cada mil transações é fraudulenta, Gallo defende a metrificação de fraudes, em que as perdas financeiras estejam relacionadas a um valor específico. No International Banking, por exemplo, o risco da fraude está embutido no custo das transações. "Sempre há tensão entre fraude e perda da receita da transação", diz.

A tecnologia de segurança vem se modernizando nos últimos seis anos. Isso significa que do lado dos bancos e instituições financeiras a modernização ocorre na mesma proporção para o fraudador, que fica monitorando seu comportamento.

Daniel Bortolazo
Engenheiro de segurança da Palo Alto Networks.

Gallo chama atenção para três pontos que devem ser considerados: os investimentos em TI no Brasil são três vezes menores do que na Europa e nos Estados Unidos, o brasileiro tem muita tolerância ao risco, o que se reflete em redução de medidas preventivas, e a legislação brasileira é muito ruim na hora de punir.

Supostas fraudes no Pix

Roubo de chaves privadas, golpes de QR Code – emitir um QR Code sem sentido, ataque semelhante ao do boleto, muda o código de barra e permanece o nome do pagador – e invasão de celulares são alguns dos supostos riscos de fraude na plataforma Pix. A Kryptus conta com solução HSM kNet com certificado FIPS (Federal Information Processing Standards), tanto em nuvem como on premise, que protege aplicativos críticos, chaves e softwares sensíveis. FIPS são padrões desenvolvidos pelo National Institute of Standards and Technology (NIST), para uso em sistemas de computador por agências do governo americano não-militares e contratantes do governo.

A Febraban, em parceria com a Associação Brasileira de Bancos (ABBC), gerencia um comitê de riscos cibernéticos do qual participam mais de 30 bancos. De acordo com Cláudio Guimarães, diretor executivo da ABBC, mensalmente, são compartilhadas experiências, melhores práticas de segurança, possíveis riscos cibernéticos, reclamações de clientes e monitoramento dos principais acontecimentos internacionais na área de cibersegurança. Os bancos já consideram soluções de IoT e 5G, além das ferramentas de inteligência artificial, machine learning e analytics, que já são amplamente utilizadas, segundo Guimarães.

Cibersegurança

Os investimentos mundiais em tecnologia e serviços de segurança da informação e gestão de risco fecharam 2020 com crescimento de apenas 2,4%, o equivalente a US$ 123,8 bilhões, comparado a 2019. Esse total está bem abaixo dos 8,7% previstos pelo Gartner.

Há 10 anos, vender uma solução de cibersegurança exigia muito convencimento por parte do fornecedor, pois as instituições só viam riscos fora do Brasil. Com a digitalização, o impacto cresceu e agora começam a fazer a correlação da segurança com a saúde do negócio, conforme Alexandre Bonatti, diretor de engenharia da Fortinet, especializada na integração de soluções de segurança para o mercado financeiro.

A estratégia de solução de segurança híbrida em nuvem é uma das mais recomendadas para o mercado financeiro, pois permite melhor controle de custo e valor para o cliente.

Antigamente, para cada nova ameaça havia uma solução específica de proteção de segurança. A contratação de soluções pontuais implicava em investimentos elevados e alta vulnerabilidade, além da gestão e controle de diferentes plataformas que não se integravam. “No mundo cyber o problema não é sofrer um ataque, mas ter agilidade de resposta, daí a importância de uma solução integrada fim a fim”, diz Bonatti. As vantagens para as empresas se refletem em redução de custos de treinamento, ganho operacional e previsibilidade de licenciamento. Segundo ele, grandes bancos como o Itaú Unibanco, por exemplo, têm mais de 5 mil pessoas na área de tecnologia da informação e segurança e não delegam para terceiros a gestão dos serviços de segurança. Além do custo operacional elevado, há controle de licenciamento dos produtos.

“A tecnologia de segurança vem se modernizando nos últimos seis anos. Isso significa que do lado dos bancos e instituições financeiras a modernização ocorre na mesma proporção para o fraudador, que fica monitorando seu comportamento. Trata-se de uma briga travada entre dois robôs para ver qual é mais rápido e eficiente”, afirma, Daniel Bortolazo, engenheiro de segurança da Palo Alto Networks.

Na área de cibersegurança, a solução SOAR – prática de orquestração, automação e reconciliação – tem sido muito utilizada pelo setor financeiro em mercados mais maduros. A solução ajuda na automatização de uma atividade-chave desempenhada por uma única pessoa, permitindo que o conhecimento seja amplamente compartilhado. “Com a orquestração é possível ter visibilidade de todas as etapas de um determinado processo, permitindo que o cliente reaja mais rápido a um incidente de segurança”, diz Miyazaki.

A indústria financeira é considerada pela IBM como a mais demandante de serviços de tecnologia se segurança. As experiências tecnológicas desenvolvidas para ela entregam três diferenciais: processos de backoffice, soluções da plataforma Watson de Inteligência

Artificial e área de pesquisa propriamente dita. Muitas tecnologias nascem por meio de estudos em criptografia homomórfica, que visa desenvolver algoritmos de criptografia para proteger dados e desenvolver pesquisa para bancos brasileiros.

Em alta nuvem

A pandemia do coronavírus impulsionou a demanda por serviços em nuvem. Pesquisa da Associação Brasileira das Empresas de Software (Abes) e da IDC aponta que a nuvem pública no Brasil deve alcançar US$ 3,5 bilhões em 2020, crescimento acima de 36% em relação ao ano passado. IoT deverá crescer 20%, chegando a US$ 9,9 bilhões, e analytics e IA avançarão quase 12%, atingindo US$ 548 milhões. De acordo com a pesquisa, o setor de TI deverá crescer 10% em 2021.

O open banking está levando muitas instituições financeiras a aderirem às soluções em nuvem. Segundo especialistas, esse movimento já vem ocorrendo em outros países. Nos Estados Unidos, o Bank of America chegou a desenvolver uma cloud para serviços financeiros. Trata-se de uma camada de segurança no padrão National Institute Standards in Technology (IST), que atende diferentes demandas específicas da indústria, como a regulatória, entre outras.

> *“No mundo cyber o problema não é sofrer um ataque, mas ter agilidade de resposta, daí a importância de uma solução integrada fim a fim.”*
>
> **Alexandre Bonatti**
> Diretor de engenharia da Fortinet.

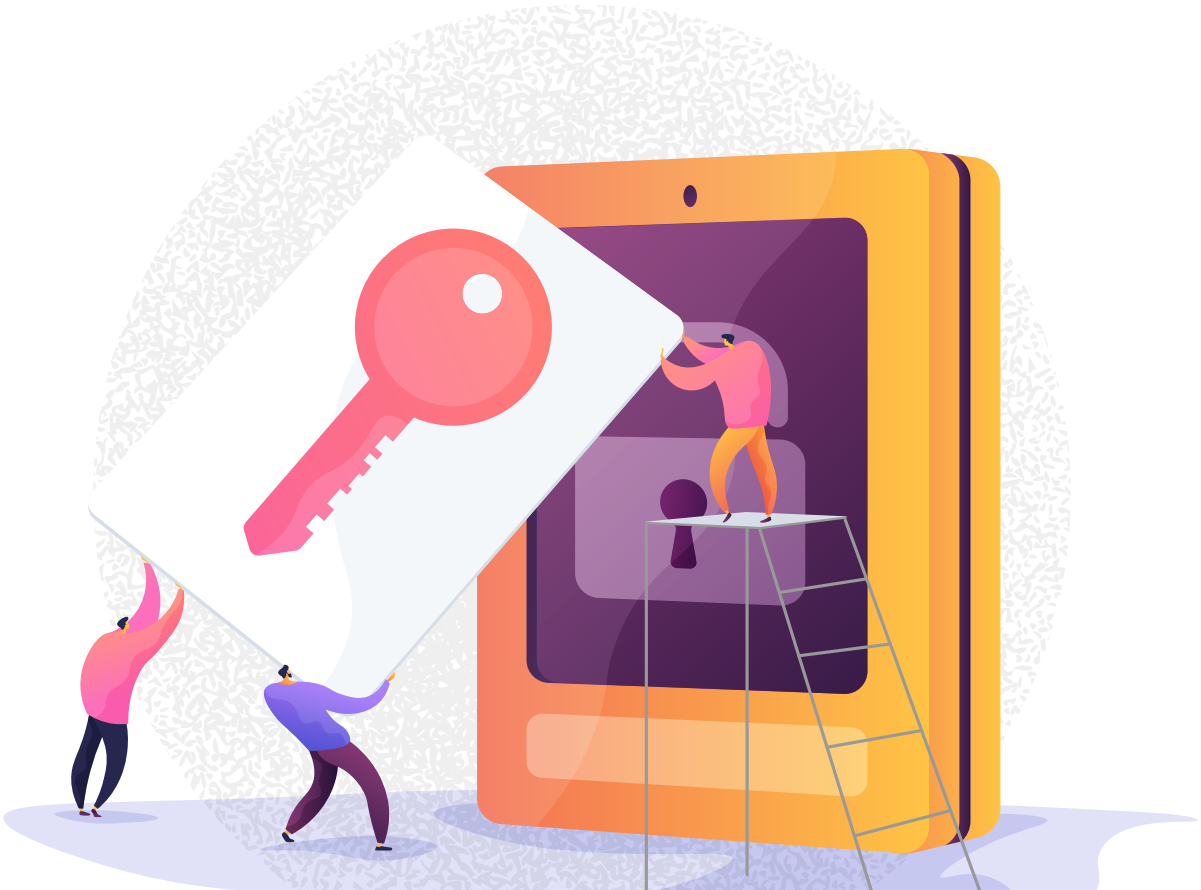
Para especialistas, a atribuição de papeis e responsabilidades é aconselhável. API's têm suas práticas de segurança, assim como as clouds para finanças contam com tecnologias robustas de segurança. A Bring your own key (traga sua própria chave) tem sido uma das práticas mais implementadas pelo provedor. Com a tecnologia de superproteção (Hyper Protec) o mercado passa a contar com uma nova classe. Trata-se de uma ferramenta de segurança tão poderosa que o provedor e nem a própria IBM conseguem intervir no serviço em nuvem. A FIPS 140 – 2 nível 4 é o padrão do mercado que bloqueia qualquer acesso além da própria instituição financeira ou bancária.

Em geral, as instituições financeiras operam com várias clouds – CRM, e-mails, serviços privados, entre outros – o que aumenta o risco de segurança. O desafio é manter a gestão e balancear as diferentes nuvens de forma a manter o ambiente seguro. A estratégia de solução de segurança híbrida em nuvem é uma das mais recomendadas para o mercado financeiro, pois permite melhor controle de custo e valor para o cliente.

Muitas instituições contratam cloud pública certas de que as soluções de segurança ficarão a cargo do fornecedor. "É um grande engano porque entrar no ambiente de segurança compartilhada garante apenas a disponibilidade do serviço. A nuvem exige o mesmo nível de proteção da solução on premise, que considera a segurança dos dados", observa Alexandre Bonatti, diretor de engenharia da Fortinet, especializada na integração de soluções de segurança para o mercado financeiro.

Open banking

Na avaliação de Roberto Gallo, o open banking será um grande marketplace, onde cada elemento da cadeia de supply



chain terá visibilidade mais ou menos parcial do que está acontecendo com o consumidor na ponta. Caso ocorra algo à transação, não se conhece o histórico do cliente. Como o produtor do serviço financeiro dará acesso a quem está na ponta da linha, as chances de fraude serão mais previsíveis. “Quanto maior o número de nós, a chance de vazamento será aumentada”, diz.

Em alguns mercados como o europeu, por exemplo, o open banking nasceu para atender ao órgão regulador e foi concebido para proteger os dados dos cidadãos. Na Ásia, baseou-se na competição, conforme estudo realizado pela IBM em 50 países abordando o processo de adoção do open banking. “Sempre que faço uma reunião com o cliente pergunto como ele vê o open banking, se quer atender ao órgão regulador ou se tem uma estratégia de negócio. A maioria das empresas tem dúvidas quanto à monetização da oportunidade”, diz.

A IBM adota uma prática chamada Zero Trust Framework, framework de confiança zero, que parte da premissa que não se deve confiar em ninguém. A partir daí são criadas uma série de perímetros de forma que o controle seja mais granular, com validação em todos os momentos, garantindo que o acesso é devido e que a informação acessada deveria mesmo ter sido acessada. A implementação dessas práticas garantirá que o acordado nos contratos seja cumprido

BANCO CENTRAL

DEFENDE ROBUSTEZ NA SEGURANÇA

O órgão regulador acredita que o processo de discussão com o mercado e a cocriação de regras contribuíram para tornar o Pix mais resistente à fraude.

Apesar de amplas discussões no mercado financeiro sobre os riscos de segurança do ambiente em nuvem, o Banco Central não descarta a possibilidade de utilizar sistemas de nuvem pública, caso necessite de mais escalabilidade no Pix, que adotou a estratégia de nuvem privada.

"Se necessário, em algum momento, faremos os testes de cenário, mas por enquanto não há nada contratado e nem transação Pix na nuvem pública", diz Caio Moreira Fernandes, chefe-adjunto do departamento de TI do Banco Central. Segundo ele, os sistemas de nuvem pública são muito robustos no que diz respeito à segurança.

O modelo de segurança para prevenção de fraudes do Pix foi construído pelo BC em conjunto com o mercado. Baseado nas informações fornecidas pelo órgão regulador, as instituições ligam o motor de risco, onde já estão associados os seus processos de fraude, que se utilizam de recursos de

"O novo sistema de pagamento instantâneo foi totalmente desenvolvido pelo BC com a expectativa de movimentar cerca de duas mil transações por segundo de pico."

Caio Moreira Fernandes
Chefe-adjunto do departamento de TI do Sistema Financeiro do (RBSFN) do Banco Central.

Inteligência Artificial e Machine Learnig, entre outras tecnologias de ponta. “Não teria muito sentido fazermos uma primeira análise no BC e eles outra, correndo o risco de os sistemas se chocarem”, explica.

Inspirado em experiências internacionais, o novo sistema de pagamento instantâneo foi totalmente desenvolvido pelo BC com a expectativa de movimentar cerca de duas mil transações por segundo de pico, como previsto inicialmente pela área de negócio do banco. “O tempo vai nos dizer o volume, mas os testes de carga mostraram que a capacidade está bem superior a isso, logo na saída”, diz Fernandes.

O BC não é novo na experiência de transação eletrônica e o Pix manteve todos os procedimentos de segurança bem sucedidos do Sistema de Pagamento Brasileiro (SPB), que é centrado no BC. As TEDs hoje já movimentam o equivalente a 1 PIB a cada quatro dias, em operações que vão de renda variável à troca de numerário entre instituições financeiras. Isso mostra o nível de complexidade do Sistema de Transferência de Reserva do Banco Central (STRF), considerado muito superior ao Sistema de Pagamento Instantâneo (SPI) desenvolvido para o Pix. A centralização da base de identificação de usuários no BC, no entanto, tem incomodado o mercado, especialmente os bancos.

“É normal que players estabelecidos reajam, mas nossa leitura é que o sistema financeiro trabalhou muito forte com o BC para a criação de um sistema de pagamento instantâneo moderno e direcionado às necessidades do país”, afirma. O Pix traz mudanças no ecossistema financeiro ao oferecer mais serviços, possibilidade de transação em tempo real e a associação de chaves.

Hoje, as TEDs podem cursar na Câmara Interbancária de Pagamentos (CIP) – instituição que processa transações financeiras, de pagamentos e compras como parte do SPB, desde de 2001 – ou no STR, considerado o coração do sistema financeiro. As TEDs no valor acima de R$ 1 milhão são necessariamente de curso forçado no STR. As demais podem ser no STR, que roda dentro do BC, ou na CIP e, posteriormente, liquidadas.

O Pix traz mudanças no ecossistema financeiro ao oferecer mais serviços, possibilidade de transação em tempo real e a associação de chaves.

Tipicamente, as Instituições de Pagamentos (IPs) não cursavam as transações via CIP, mas direto no BC. Segundo Fernandes, há um volume de transações de TED no STR muito próximo ao que hoje é trilhado na CIP e necessariamente liquidado no STR. “Temos a CIP de liquidação e as que cursaram direto no STR, já era um sistema centrado no BC desde o início”, diz.

Segurança Pix

O dado armazenado criptografado é um diferencial do Pix. Todas as mensagens assinadas são enviadas ao BC por um canal criptografado para garantir a privacidade do dado que está sendo transitado. A comunicação do BC com a instituição detentora da conta é feita por uma rede privada (RSFN), apartada da internet, já utilizada no SPB. Essa segregação física do tráfego representa uma outra camada de segurança, conforme Fernandes.

“Para garantir o alto nível de privacidade em relação a chave, implantamos mecanismo de criptografia no dado armazenado que só o sistema consegue ler e agrega ferramentas de proteção antiscam. Nem o administrador de banco de dados do BC tem acesso à informação”, diz. Foram incorporados também ao Pix padrões de prevenção de ataque de leitura, evitando as tentativas do fraudador de montar uma base a partir de celulares e CPFs aleatórios. Nesses casos, o BC controla o número de consultas sem liquidação e bloqueia por um tempo a pessoa e as consultas inválidas.

Quanto à prevenção de fraudes nas chaves de cadastramento, o BC fornece à instituição financeira uma chave de endereçamento do Pix. Além de o dado da chave, constam informações complementares como a data de criação, conta, volume transacionado e percentual de vezes em que foi envolvida em disputa. Essas informações permitem a instituição fazer um score de risco da chave e potencial fraude da transação. Caso identifique divergência do comportamento padrão da transação é solicitado de 30 a 60 minutos de tempo extra para análise antifraude.

Essas determinações foram discutidas pelo GT SEG do BC, grupo de prevenção de fraude e vazamento de informação dedicado a zelar pela robustez da segurança no ecossistema Pix. “Esse processo de discussão com o mercado e a cocriação de regras, sem dúvida,

contribuíram para tornar o Pix mais resistente à fraude. O grupo permanecerá ativo para dar prosseguimento às evoluções necessárias", diz.

Open banking

As instituições participantes do open banking terão de cumprir com os regulamentos de segurança estabelecidos na resolução número 4658 do BC. Por se tratar de um modelo cocriado com o mercado, a preocupação com segurança tem sido considerada. Para Fernandes, o projeto do open banking tem desafios próprios e por isso acaba gerando regras a mais. Para autenticação será utilizado o CIBA, protocolo de segurança usado no modelo britânico da OpenID Foundation.

A participação de instituições não financeiras na plataforma open banking, como operadoras de telefonia e empresas do varejo, implicará no cadastro prévio no BC, segundo Fernandes. "Por envolver diferentes áreas, o processo será analisado com cuidado para avaliar potenciais riscos à plataforma", diz (VF)

SETE CHAVES
CONTRA AS FRAUDES

Todo investimento que as instituições financeiras realizaram no upgrade de seus sistemas de segurança será utilizado no Pix.

Com a entrada em operação do Pix, em 16 de novembro, pela primeira vez em sua história, os bancos terão as transações interbancárias disponíveis em arranjo aberto, fora do horário comercial. Os robôs, que normalmente estão acostumados a funcionar baseados no perfil dos usuários – transferência de TED até às 17h e DOC 22h –, terão que assimilar o novo comando, 24 horas durante os sete dias da semana, para detectar os pagamentos no padrão Pix.

“Os modelos de segurança dos bancos costumam ser bem assertivos, o grande ponto será aprender esse novo ciclo transacional que se inicia, a nova necessidade dos clientes”, afirma Ivo Mósca, coordenador da Subcomissão do Grupo de Segurança (GT SEG) da Federação Brasileira dos Bancos (Febraban). Segundo ele, a autorização do Banco Central para a instituição marcar a chave fraudada quando identificada, de forma que as demais tomem conhecimento, contribuirá para a aprendizagem rápida do processo.

O Pix passa a ser um novo caminho transacional. Toda a sua infraestrutura foi desenvolvida com o potencial de substituir o DOC e TED, em operação há quase duas décadas. Uma das vantagens do novo sistema de pagamento instantâneo do Banco Central é reduzir o custo da transferência. Será gratuito para pessoa física e com algumas tarifas de serviços cobradas para pessoa jurídica, entre elas a emissão e a manutenção dos QR Codes dinâmicos, que oferecem uma série de funcionalidades. Ainda assim, o Pix vai ser um meio de pagamento mais barato que o cartão de débito, ou mesmo, a transmissão de um boleto de cobrança.

Para Mósca, as empresas orientadas à redução de custos logo migrarão para esse meio de pagamento. A questão da disponibilidade 24x7x365, além da liquidação imediata, independentemente da hora em que o pagamento for realizado, o recurso é creditado instantaneamente.

> *“A evolução da experiência para o cliente somada à facilidade transacional de usar apenas um dado – celular, email ou CPF – facilitará o processo de adesão.”*
>
> **Ivo Mósca**
> Coordenador da Subcomissão do Grupo de Segurança (GT SEG) da Federação Brasileira dos Bancos (Febraban).

A tendência é convivermos com TED e DOC até que os usuários se acostumem ao Pix.

"A evolução da experiência para o cliente somada à facilidade transacional de usar apenas um dado – celular, email ou CPF – facilitará o processo de adesão", diz. O manual de experiência mínima do usuário publicado pelo BC, com a padronização de toda a experiência do mercado, garantirá que todas as instituições participantes falem a mesma linguagem com o cliente. Dessa forma, a disseminação do conhecimento fluirá mais rápido, assim como a curva de adoção ao produto.

DOC e TED

Bancos, fintechs e instituições de pagamentos investiram na adequação de uma série de sistemas que utilizam o Pix e que deverão permanecer em operação. "O Pix facilita essa migração ao permitir que da mesma forma que se faz um DOC e TED pode-se fazer um Pix, colocando todas as informações como agência, conta, CPF e instituição bancária", diz.

Mósca acredita que a tendência é convivermos alguns anos com ambos os produtos, até que os usuários se acostumem ao novo serviço. "Mesmo sendo digitais, alguns clientes preferem ir à boca do caixa pegar o comprovante de um depósito ou transferência em papel, por considerar mais importante do que o digital." Diferente do DOC e TED que têm limite máximo, o Pix não tem limitação de valor.

Nas últimas décadas, instituições financeiras de grande e médio portes têm investido na evolução de seus sistemas de segurança, sejam próprios ou fornecidos por empresas especializadas, para complementar e dar mais robustez ao seu portfólio. Essa vantagem passa a ser aplicada também ao Pix. Os dados em uma transação de DOC e TED, ou mesmo no cartão de débito, coleta informações, como a localização do cliente no ambiente internet ou celular. Todo esse motor de aprendizado pode ser reutilizado no Pix para garantir segurança.

Segurança cibernética

A criatividade do fraudador no Brasil é muito grande e desafia os bancos todos os dias. A grande preocupação das instituições financeiras, atualmente, é com a fraude de engenharia social, que responde por 70% dos ataques ocorridos, segundo pesquisa da Febraban. O fraudador se aproveita da falta de conhecimento do usuário e sugere que ele siga com a transação e, sem que perceba, acaba entregando informações confidenciais, como senhas de bancos e número de cartões.

Em se tratando do Pix, os fraudadores não estão preocupados em cadastrar ou roubar a chave do usuário. “Eles pedem suas informações como você estivesse cadastrando a sua chave, mas na prática estão acessando sua conta e iniciando uma transação”, explica Mósca. Entre os golpes mais famosos no período da quarentena estão as tentativas de ataque de phishing (pescaria digital), que respondem por 80% das fraudes. A Febraban já detectou uma série de links falsos falando sobre o Pix.

Até as instituições participantes do Pix adquirirem mais desenvoltura para lidar com o novo ambiente, o BC atendeu a demanda encaminhada pelo grupo GT SEG reduzindo os limites do valor das transações, entre R$ 3 mil a R$ 5 mil por dia, no cartão de débito. Enquanto a TED ficou na faixa de R$ 50 mil e, a partir desse montante, para pessoa jurídica. “São esses tipos de mecanismos que somados garantirão a segurança de todo ecossistema”, afirma Mósca.

Um outro ponto de alerta dos bancos com relação à segurança do novo ecossistema trata-se da entrada de muitos players, em torno de mil, sendo algumas instituições não financeiras participantes da nova plataforma. De acordo com o coordenador de segurança da Febraban, o onboarding de clientes é o grande cuidado a ser tomado, pois um processo seguro de entrada reduz a possibilidade de transações fraudulentas. “Da mesma forma que tentamos fechar todas as portas a sete chaves para garantir a segurança, o fraudador tenta descobrir a fechadura mais frágil”, diz.

A grande preocupação das instituições financeiras, atualmente, é com a fraude de engenharia social, que responde por 70% dos ataques ocorridos.

Basta uma ou duas instituições, percentual pequeno diante do todo, terem fragilidades na entrada dos clientes para refletir em todo ecossistema, o que obrigará o mercado a ajustar rapidamente seus processos de segurança. Empresas especializadas em soluções de segurança e participantes diretos estão aptos a oferecer os serviços adicionais para os novos entrantes.

Fraude no open banking

O open banking envolve transferência de dados e comandos de transações. Trata-se de uma infraestrutura aberta por onde as informações vão trafegar. O diretório de participantes em que todas as instituições, obrigadas ou não a participar, terão que se cadastrar, certificar e passar por uma rede segura. A conexão dos dados em si deverá ser entre as instituições doadora e receptora, sem passar por um ente financeiro.

Todo o sistema de segurança cibernética vai ser pensado para garantir uma conexão segura para evitar qualquer tipo de vazamento de informações. É o mesmo tipo de fraude por cadastramento do Pix. O fraudador acha um canal falso, tipo um link, para ter acesso a sua conta. Uma pessoa não vai conseguir obter seus dados para transferir para a conta de um terceiro (VF)

O onboarding de clientes é o grande cuidado a ser tomado nas novas plataformas, pois um processo seguro de entrada reduz a possibilidade de fraudes.

FEBRABAN INVESTE EM SEGURANÇA CIBERNÉTICA

A Federação Brasileira de Bancos (Febraban) lançou, em setembro, o Laboratório de Segurança Cibernética com o objetivo de fortalecer a defesa dos bancos, que aumentaram a migração das transações financeiras para os canais digitais durante o período da pandemia. Os bancos investem por ano R$ 2 bilhões em sistemas voltados para a segurança da informação, segundo a Febraban.

"Trata-se do primeiro laboratório setorial da América Latina, o que mostra a vanguarda do setor bancário em proteção de dados e segurança cibernética", afirmou Leandro Vilain, diretor executivo de Inovação, Produtos e Serviços Bancários da Febraban, durante a live de inauguração.

Com investimento de R$ 6 milhões – que envolve montagem, compra de equipamentos, software e consultoria – o projeto permitirá que instituições financeiras treinem seus profissionais, troquem conhecimento e desenvolvam mecanismos mais robustos para enfrentar as ameaças e possíveis ataques que se sofisticam cada vez mais.

"O setor bancário regulado e até mesmo fiscalizado, ainda mais agora com a entrada da Lei Geral de Proteção de Dados (LGPD), demanda mão de obra qualificada", disse Vilain. A expectativa é que o número de transações financeiras por meios eletrônicos via internet banking e mobile banking, que chegaram a 63% no ano passado, aumentem cerca de 30%, em 2020.

A Accenture, vencedora da proposta, compartilhará com a Febraban as experiências realizadas em laboratórios localizados em Londres, Washington e Tel Aviv, além do arquivo com programas de simulação de ataques em tempo real ocorridos ao redor do mundo.

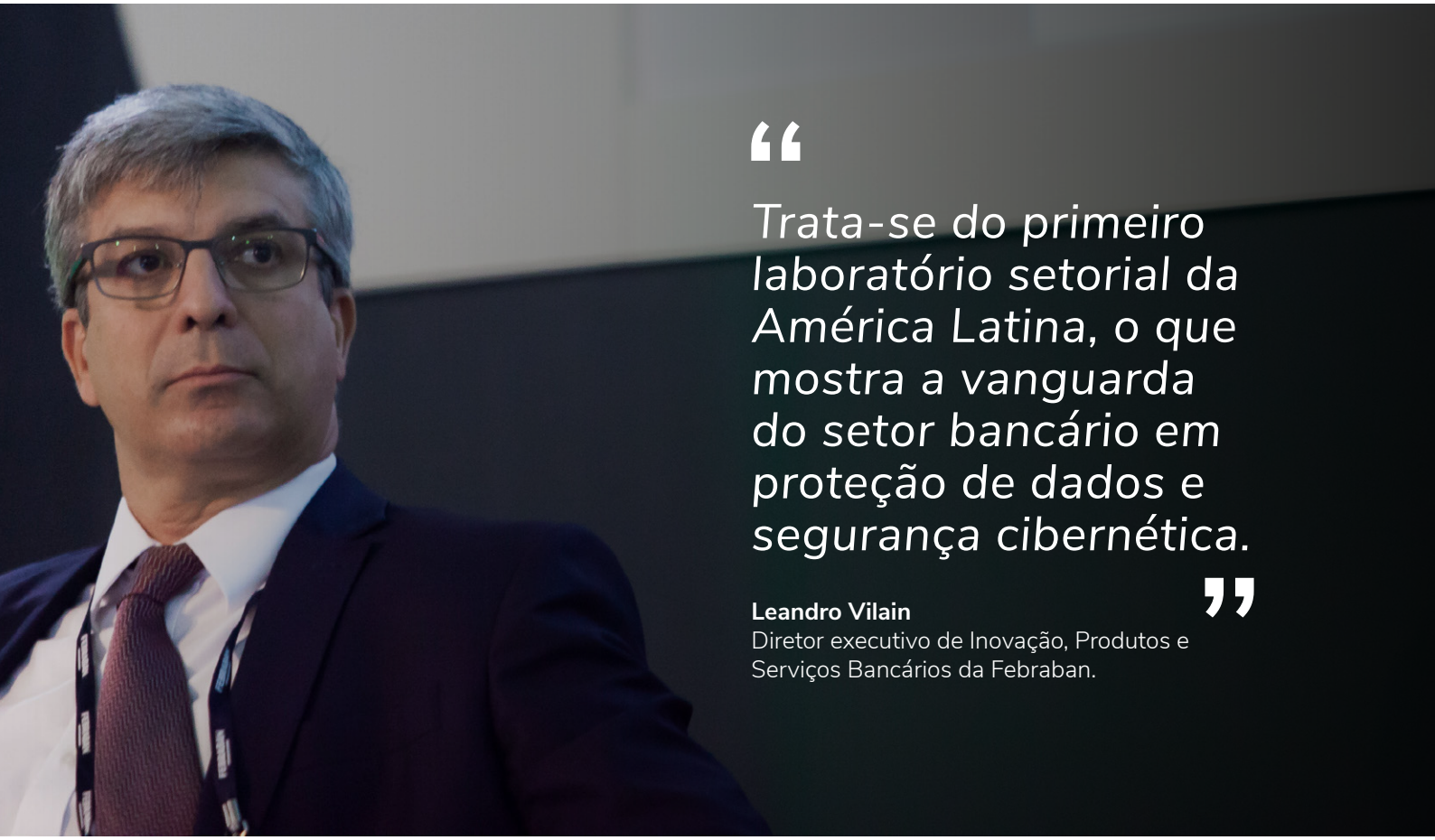
A ideia de criar o laboratório surgiu no conselho diretor da Febraban em 2019, antes do aumento das transações digitais com a pandemia. Seu funcionamento baseia-se em três pilares de atuação: treinamento, simulações de ataques e inteligência de análise.

O treinamento em segurança cibernética primeiramente será montado para os bancos que participam da Comissão Executiva de Segurança Bancária e, na medida em que ganhe ritmo, se estenderá para todas as instituições financeiras associadas à Febraban.

Ataque e defesa

A intenção é fazer também treinamentos específicos, conforme o nível de conhecimento de cada grupo. A previsão é que sejam treinadas entre 60 e 80 pessoas por ano. “A ideia é capacitar o profissional para que ele possa migrar de setor dentro da própria instituição bancária”, explica.

Para a área de inteligência, que trata da detecção e antecipação de riscos, o objetivo é ajudar os bancos a se precaverem contra possíveis acidentes



> *“Trata-se do primeiro laboratório setorial da América Latina, o que mostra a vanguarda do setor bancário em proteção de dados e segurança cibernética.”*

Leandro Vilain
Diretor executivo de Inovação, Produtos e Serviços Bancários da Febraban.

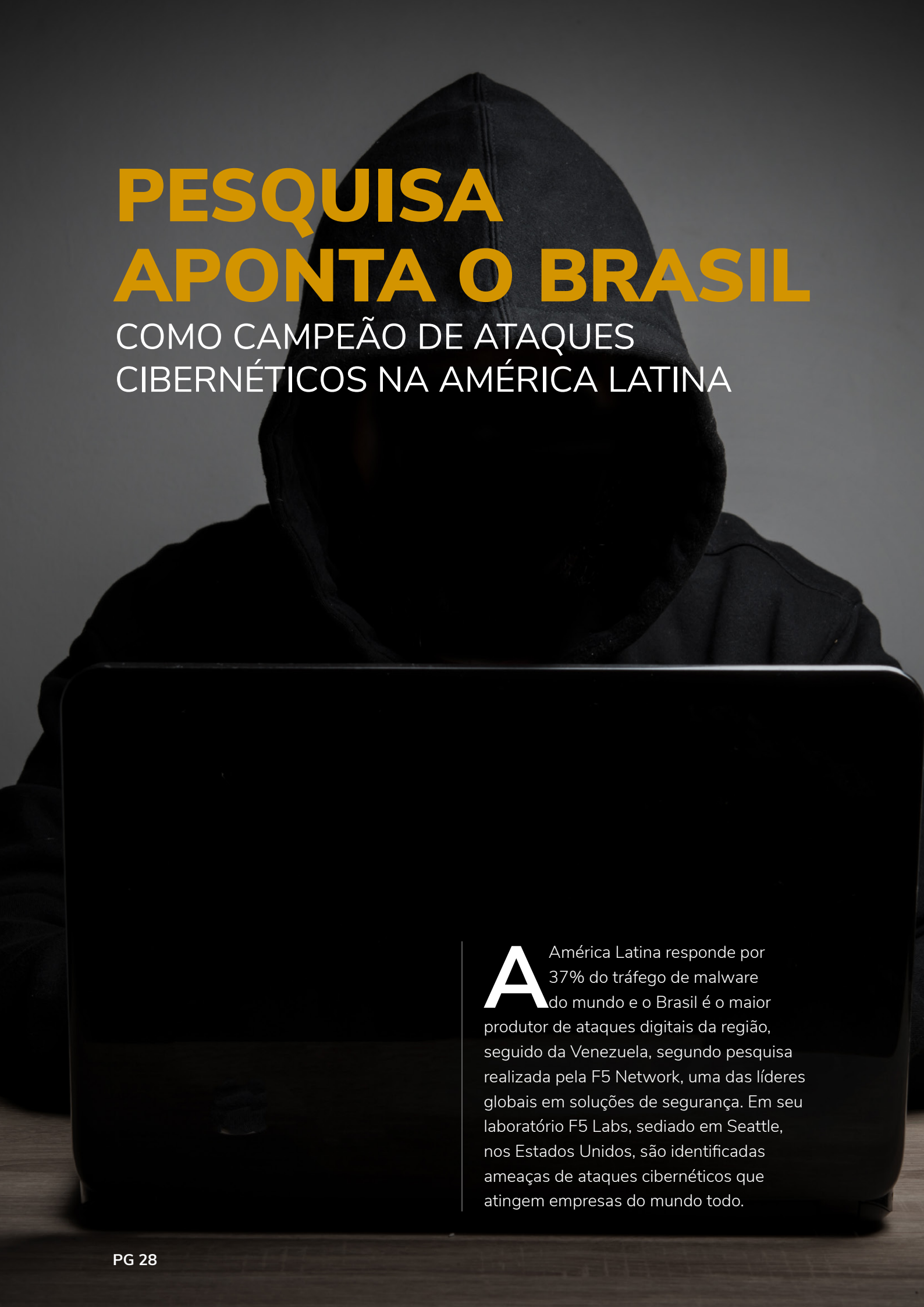
O laboratório servirá também de espaço para simular diversos tipos de testes de ataque e defesa, além de monitorar e alertar os bancos em relação aos casos mais sofisticados.

digitais. O laboratório servirá também de espaço para simular diversos tipos de testes de ataque e defesa, além de monitorar e alertar os bancos em relação aos casos mais sofisticados.

“Cada banco tem sua estrutura própria e larga experiência em fazer monitoramento, mas se identificarmos vantagens de eficiência para o setor poderemos fazer o monitoramento de forma centralizada no futuro”, explica Vilain.

Para o diretor da Febraban, a segurança cibernética e de proteção de dados são temas que transcendem à entrada em operação de novos sistemas no mercado financeiro, como o Pix e open banking. “Nosso propósito é cuidar do sistema bancário como um todo, sem focar em um determinado sistema específico”, diz.

Embora geograficamente o Brasil não fique muito na rota dos fraudadores – como os Estados Unidos, Europa e Ásia – todo cuidado é pouco, pois os ataques que ocorrem por aqui já são bem sofisticado ▧ (VF)



PESQUISA APONTA O BRASIL

COMO CAMPEÃO DE ATAQUES CIBERNÉTICOS NA AMÉRICA LATINA

A América Latina responde por 37% do tráfego de malware do mundo e o Brasil é o maior produtor de ataques digitais da região, seguido da Venezuela, segundo pesquisa realizada pela F5 Network, uma das líderes globais em soluções de segurança. Em seu laboratório F5 Labs, sediado em Seattle, nos Estados Unidos, são identificadas ameaças de ataques cibernéticos que atingem empresas do mundo todo.

A América Latina também é alvo de ataques de outras nações: EUA, Holanda, Moldávia, China e Rússia invadem sistemas na região. O Brasil ataca tanto a América Latina como outros continentes. “O tráfego malicioso disparado de endereços IP brasileiros foi identificado nas redes de todos os países, o que mostra a agressividade do código dos ataques gerados no Brasil”, diz Hilmar Becker, country manager da F5 Networks Brasil. Venezuela e Argentina, por outro lado, somente atacam a América Latina. Para apoiar os clientes a enfrentar o crime digital, a F5 Network entrega aos gestores de segurança a lista dos endereços IP – computador ou equipamento de rede, tradicional ou virtual – de onde partem os ataques e o tipo de porta de comunicação – e-mail, navegador Web etc. – mais vulnerável a eles. Conforme o nível da investigação, chega a revelar a razão social das empresas que disparam o malware. “As operadoras de Telecom, presentes em todo o contexto mapeado pelo F5 Labs, informam a razão social das empresas para quem entregam endereços IP. Essa regra traz visibilidade sobre a instituição responsável pelo ataque”, detalha Becker. Da lista das 50 maiores fontes de ataques digitais, o Brasil apresenta sete empresas identificadas como LTDA, ME ou Eirelle, que conforme a legislação brasileira representam pequenas empresas ou de apenas um único dono. “Muitas vezes a fonte de ataques pode ser um equipamento comprometido, sob o controle de hackers. Criminosos digitais

“O tráfego malicioso disparado de endereços IP brasileiros foi identificado nas redes de todos os países, o que mostra a agressividade do código dos ataques gerados no Brasil.”

Hilmar Becker
Country manager da F5 Networks Brasil.

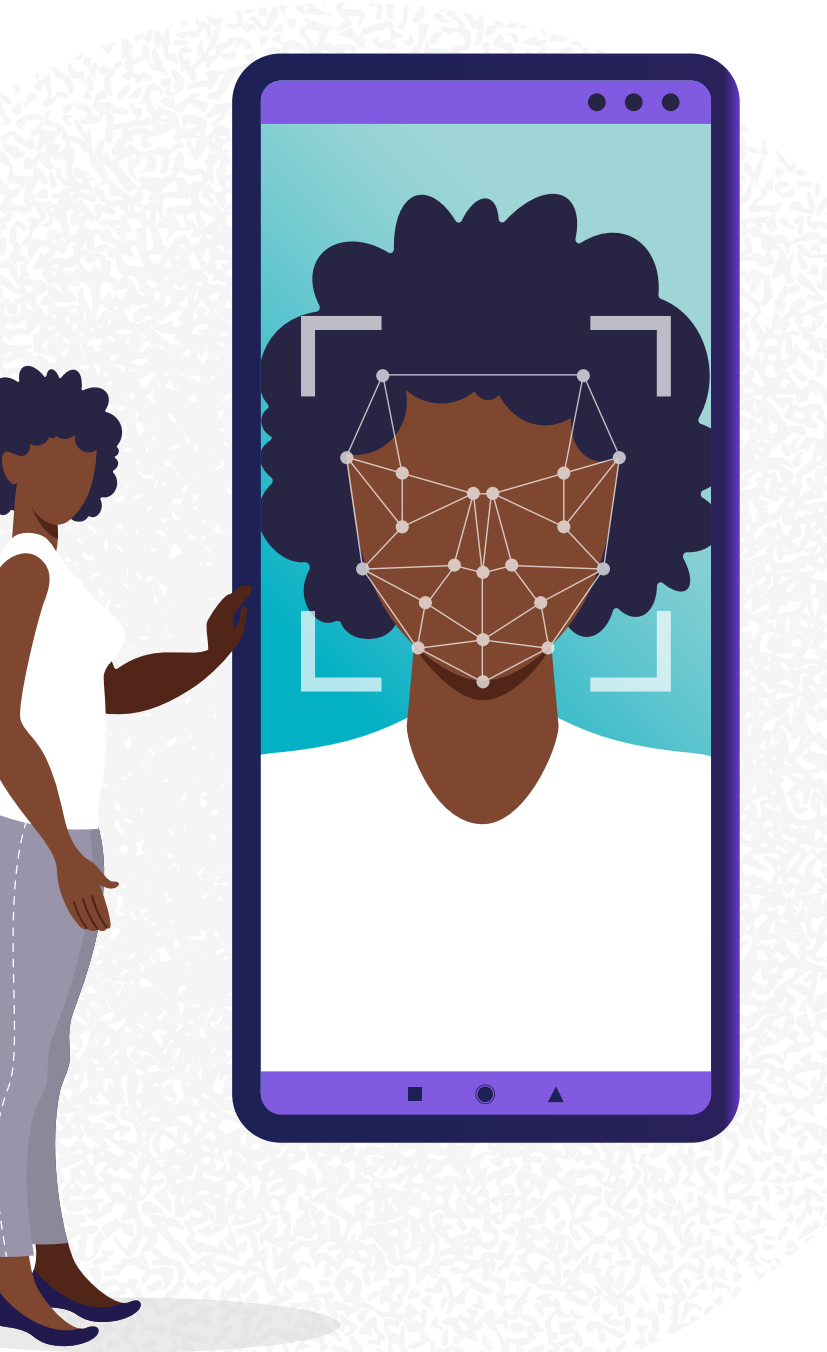
As operadoras de Telecom, presentes em todo o contexto mapeado pelo F5 Labs, informam a razão social das empresas para quem entregam endereços IP. Essa regra traz visibilidade sobre a instituição responsável pelo ataque.

podem, ainda, mascarar o IP real de origem com o uso de proxies (intermediários entre o usuário e seu servidor)", explica. O grande objetivo costuma ser a extração de informações críticas como dados sobre clientes, detalhes estratégicos sobre novos produtos etc. Um outro foco dos criminosos digitais identificado pela pesquisa foram as portas padrão SMB 445 – uma das mais usadas em ambientes corporativos, comum em drives de computadores e de dispositivos de rede. Por uma questão de política corporativa, muitas portas costumam ser configuradas só após um ataque. "Para vencer esse desafio é fundamental rever a política de senhas de dispositivos e de gerenciamento de identidades da empresa usuária", afirma. O relatório mostra, ainda, que uma das portas mais visadas é a MySQL 3306, presente tanto em ambientes com grandes bases de dados de aplicações tradicionais às milhares de Web Applications sendo lançada no mercado, como em dispositivos IoT. A infraestrutura IoT é um dos alvos preferenciais dos criminosos digitais na América Latina. "Internet Banking, e-Commerce e portais de notícias são alvo de ataques em que portas vulneráveis permitem o acesso a bases de dados SQL, algo que produz estragos muito grandes ao negócio", diz Becker. Essa vulnerabilidade segue presente mesmo quando a empresa usuária utiliza firewalls de rede tradicionais, que tendem a bloquear a porta para evitar acessos. Isso pode deixar do lado de fora clientes, investidores etc. Segundo Becker, a solução para esse impasse é a tecnologia WAFs Web Application Firewalls (WAFs), baseada em inteligência artificial, que filtra as demandas da aplicação que suportam o negócio, identifica o acesso válido e bloqueia o ataque. "O acesso à base de dados SQL passa a acontecer a partir de um critério mais refinado, sem que portas de acesso sejam bloqueadas de forma massiva", explica Becker (VF)

BANCO ORIGINAL

SEGURANÇA EM UM CLICK

Por ter nascido 100 % digital, uma segurança inovadora sempre foi prioridade para o banco.



A solução de reconhecimento facial do Banco Original, considerada uma das pioneiras do mercado para a abertura de contas, passa agora a ser usada na prevenção de fraudes e validação de transações de altos valores. Além de reforçar a segurança do cliente nas operações de TED e pagamento de contas, o banco aposta na ferramenta para massificação do novo sistema de pagamento instantâneo do Banco Central.

"A solução permite fazer uma transação de alto valor no Pix usando a biometria facial como confirmação dupla, garantindo mais segurança e facilidade ao consumidor", afirma Leandro Bartolassi, superintendente executivo de segurança corporativa do Banco Original. Segundo ele, esse modelo de biometria traz muito mais segurança que as tradicionais senhas.

Para Bartolassi, validar a comunicação com o Banco Central não é problema no novo sistema de pagamento instantâneo. "O mais difícil é garantir que quem está retirando o dinheiro via Pix é o cliente", diz. No Original, 70% do processo de abertura de conta são feitos de forma digital, sem interferência humana, em até sete minutos. Com o Pix funcionando 24X7X365, o banco contará com uma equipe extra, pois o Service Level Agremment (SLA) acordado precisa tratar possíveis problemas em até uma hora.

No Original, 70% do processo de abertura de conta são feitos de forma digital, sem interferência humana, em até sete minutos.

Por ter nascido 100% digital, o conceito de segurança inovadora sempre foi um pilar importante para o Original.
"A evolução de soluções para proteção a ataques cibernéticos e fraudes envolve várias camadas de defesa e é uma constante em nosso negócio", diz. O Plano Diretor de Segurança de Informação (PDSI), que baliza a execução das ações de segurança das organizações, reconhece o nível de maturidade do Original por adotar as melhores práticas de segurança necessárias ao mercado financeiro.

O Base Point, quando a fraude impacta no resultado do banco, no Banco Original é de 0,001 pontos percentuais, segundo Bartolassi. Há um ano, o banco implantou os testes de Read Team, equipe vermelha, e Blue Team, equipe azul, em parceria com empresas e consultorias especializadas para simular ataques reais de segurança a uma empresa. Os testes de penetração, Read Team, são realizados em diferentes sistemas e níveis de programas de segurança. Enquanto o Blue Team identifica possíveis vulnerabilidades e previne os controles de segurança. Enquanto o Blue Team, equipe azul, identifica possíveis vulnerabilidades e previne os controles de segurança.

Com 3,9 milhões de clientes e 730 mil chaves cadastras no Pix, o Original mantém a operação e gestão de segurança no próprio banco, realizada por sua equipe de 110 pessoas. Atualmente o banco funciona como um hub de tecnologia que desenvolve soluções de segurança para outras empresas (VF)

"O mais difícil é garantir que quem está retirando o dinheiro via Pix é o cliente."

Leandro Bartolassi
Superintendente executivo de segurança corporativa do Banco Original.

BIRÔS DE CRÉDITO
ESTÃO OTIMISTAS APESAR DA CRISE

Elias Sfeir
Presidente da Associação Nacional
dos Bureaus de Crédito (ANBC)

Por Vera Franco

O cadastro positivo passa a ganhar visibilidade a partir de acordos estabelecidos com as operadoras de telefonia e concessionárias de energia elétrica. Serão mais 50 milhões de brasileiros a construírem o seu histórico de crédito.

Para Elias Sfeir, presidente da Associação Nacional dos Bureaus de Crédito (ANBC), o novo cadastro positivo, atualmente com 150 milhões de registros, serviu como uma âncora de segurança para milhões de brasileiros atravessarem o período de pandemia.

Em entrevista exclusiva ao Digital Money Inform, Sfeir fala sobre a importância dos consumidores construírem seu histórico de crédito para ter prazos maiores e juros melhores e do papel disruptivo que a criação de uma moeda digital com características globais trará para os meios de pagamento, acelerando a economia e gerando bem estar e empregos.

Qual tem sido a importância do cadastro positivo nesse período da pandemia?

O fato de o cadastro positivo ter sido aprovado no ano passado serviu como uma âncora de segurança para atravessar a pandemia. A formação de um cadastro com informações positivas é um estímulo tanto para quem empresta, por ter mais garantia de recebimento, como para quem toma, pelo acesso ao crédito de forma mais rápida e com taxas de juros mais baixas, além do maior controle sobre as informações. O cadastro positivo já vem surtindo efeitos sobre o crédito. Cabe ao consumidor agora construir o seu score para ter uma nota de crédito conforme seu histórico de bom pagador. Além das obrigações financeiras, o novo sistema passará a considerar o pagamento de contas contínuas, como luz, água, telefone e gás.

Como é para o consumidor construir um bom score?

O score ou nota de crédito, calculada pelo birô com base nos dados enviados pelas fontes, é resultado de uma análise dos hábitos de pagamento e do relacionamento de empresas e consumidores com o mercado. Quanto mais informações chegarem ao banco de dados do cadastro positivo, mais benefícios para os credores. Se não tem informação, não tem como avaliar. É que nem receita de panetone: são muitas variáveis a serem consideradas. Não existe uma fórmula mágica para conseguir um bom score, mas há boas práticas que ajudam a melhorar a pontuação como, renegociar dívidas atrasadas, evitar atrasar pagamentos, colocar ao menos uma conta da casa em seu nome para construir o histórico, manter os dados cadastrais atualizados nos serviços de

proteção ao crédito, acompanhar sua nota de crédito, entre outros. No cadastro positivo o credor consegue automaticamente ver a nota de crédito gratuitamente duas vezes por ano. A consulta grátis cria incentivo para que a pessoas acompanhem a nota.

Atualmente, quantos são os registros no cadastro positivo?

Hoje os birôs dispõem de 100 milhões de registros. O cadastro positivo passa a ganhar visibilidade a partir dos acordos estabelecidos com as operadoras de telefonia e concessionárias de energia elétrica. Com essas adesões a partir de outubro, serão mais 50 milhões de registros. A nossa expectativa é que nos próximos seis meses novos dados serão recebidos, uma vez que a ANBC acaba de firmar acordo com empresas de saneamento, grande varejo e gás. Quanto mais informações disponíveis sobre o tomador de crédito, mais eficiente se torna a avaliação de risco e, por consequência, mais negócios podem ser realizados pelo credor, que passa a identificar com mais assertividade o perfil dos seus clientes, pessoa física ou jurídica. Temos hoje 45 milhões de desbancarizados, pessoas não visíveis pelo sistema financeiro. A visibilidade, no entanto, não significa que esses cidadãos sejam bancarizados.

A entrada em operação do Pix contribuirá para reduzir o número de desbancarizados?

O Pix acelera a forma de pagamento trazendo redução de custo e eficiência ao sistema financeiro brasileiro. O Brasil é ainda um mercado iniciante em transações digitais. Apesar de 60% das transações bancárias brasileiras terem sido realizadas de forma eletrônicas em 2019, o país ainda tem

O Pix e a introdução da moeda digital, entre outras medidas, contribuirão para acelerar a inclusão financeira de pessoas que ainda não são bancarizadas.

muito a crescer, se considerarmos o número de pagamentos eletrônicos em relação à população. No ano passado, em Cingapura foram 831 transações per capta, nos Estados Unidos, 495 e no Brasil, somente 166. Esses números mostram o potencial de crescimento de pagamentos eletrônicos sem moeda. Com a pandemia esse movimento se acelerou. Mudanças que se esperava em cinco anos, foram feitas em 5 meses. O Pix e a introdução da moeda digital, entre outras medidas, contribuirão para acelerar a inclusão financeira de pessoas que ainda não são bancarizadas.

O índice de saída do cadastro positivo tem sido elevado?

No Cadastro Positivo as pessoas podem optar por tirar seu nome, mas o número de saída tem sido muito baixo. Trata-se de um processo cultural, que vem ganhando maturidade e os cidadãos vão evoluir ao longo do tempo. Os birôs desenharam um processo simplificado, alertando aos consumidores para as consequências da saída. Você existe a partir das informações que as pessoas têm sobre você.

O bitcoin não vingou porque não foi aceito socialmente. Existe um movimento global liderado pelos órgãos reguladores de várias nações de criar um padrão monetário econômico.

A ANBC liderou um movimento junto aos birôs e agentes de crédito que reduziu o percentual de negativados durante a pandemia. Como foi esse movimento?

Embora tenha colocado muita gente em situação de dificuldade financeira, a pandemia apresentou um número de negativados inferior, em comparação a 2019. Para minimizar os efeitos provocados pelo isolamento social, criamos uma estratégia baseada em três pilares: a integridade da base de dados para transformar incerteza em risco e, consequentemente, em crédito; abrimos espaço para a renegociação dos contratos; e olhamos a informação de maneira relativa. Os birôs e agentes de mercado concordaram em dar mais tempo para negociações de dívidas. Tradicionalmente, as empresas enviam a informação negativa em 10 dias. Com a pandemia, estendemos o tempo para 45 dias, por um período de três meses. Esse esforço foi exitoso, pois reduziu a negativação. Febrabran e outros entenderam que é melhor repactuar. O auxílio

emergencial permitiu a abertura de crédito para PJ. Esses incentivos para o consumidor, no entanto, são finitos, mas apostamos que o processo de crédito volta, desde a concessão à cobrança. Houve, no entanto, um tipo de inadimplência por questão tecnológica durante a pandemia, por falta de conhecimento de uso das ferramentas digitais, especialmente por parte dos idosos.

Qual é a estimativa de negativados no país atualmente?

O Brasil tem hoje 66 milhões de pessoas negativadas nos birôs e outras 6 milhões de empresas também nessa situação de inadimplência. No mesmo período de 2019, eram cerca de 63 milhões. O total da dívida é de R$ 250 bilhões entre pessoas físicas e R$ 110 bilhões jurídicas.

Como tem sido a relação do crédito sobre o PIB em outros países?

O crédito tem relação com o PIB que, ligado à velocidade da circulação do dinheiro do capital passivo para o capital ativo, acaba alavancando a economia. Nos Estados Unidos, a relação de crédito com o PIB é de 150%, enquanto no Brasil, no período pré-pandemia, era de 47,7%. A economia americana é forte por causa do crédito. No pós-guerra, houve a modernização do crédito por meio do cartão de crédito. O problema não é dever, mas pagar o que se deve, e o cadastro positivo está mudando essa visão, pois permite entender o comportamento do consumidor e não considerar apenas uma ação pontual.

Como os birôs estão se posicionando em relação a criação da moeda digital no país anunciada pelo Banco Central?

Os birôs de crédito que operam no Brasil estão otimistas com a perspectiva de surgimento de uma moeda 100% digital no Brasil. A moeda digital tem três características: ser aceita socialmente, facilitar a transação e a economia e acumular. O bitcoin não vingou porque não foi aceito socialmente. Existe um movimento global liderado pelos órgãos reguladores de várias nações de criar um padrão monetário econômico. Hoje, o custo para manter uma moeda física no país é da ordem de R$ 60 bilhões. A partida para a criação dessa moeda no país já foi dada pelo Banco Central, em 21 de agosto, ao anunciar a formação de um grupo de trabalho que estudará o assunto e traçará as diretrizes que vão orientar o funcionamento do sistema de pagamentos brasileiro baseado na moeda eletrônica. Será algo disruptivo. Para os birôs, ainda que a digitalização plena demore, resultará em crescimento econômico. Primeiro, porque vai economizar o dinheiro do Estado. É algo que trará uma economia de R$ 90 bilhões/ano para o BC, com custos de gerenciamento dos meios de pagamento e outras transações. É importante, no entanto, que o BC adote práticas equivalentes às de outros países que também estão digitalizando suas moedas

CADASTRO POSITIVO

JÁ É REALIDADE NO BRASIL

Oito anos após a sua criação, o cadastro positivo entrou em funcionamento e já conta com o histórico de crédito de milhões de brasileiros.

Por Vera Franco

Com a adesão das bases de dados das operadoras de telefonia e distribuidoras de energia elétrica, o cadastro positivo atinge 150 milhões de registros e estará operando a pleno vapor até meados de 2021, conforme estima Roque Pellizzaro, presidente do SPC Brasil. A expectativa é beneficiar 137 milhões de brasileiros com melhores condições em empréstimos. Desse total, 22,6 milhões de pessoas, que estão fora do mercado de crédito, podem obter pela primeira vez crédito e financiamento com base no histórico de pagamentos de contas de luz, gás e telefone.

A inclusão desses dados nos cadastros contribui para reduzir a assimetria de informações e permite a universalização da concessão de crédito de forma equilibrada e de qualidade, conforme Otávio Damaso, diretor de Regulação do Banco Central.

Com o cadastro positivo em funcionamento as pessoas serão levadas a construir o seu histórico de crédito para ter prazos maiores e juros menores. “Mesmo que muitas vezes o consumidor tenha condições de realizar uma compra à vista, é aconselhável agora optar pelo parcelamento”, diz Pellizzaro. Para ele, o score passa a ser um ativo importante na vida do cidadão e tanto o cadastro positivo como o open banking permitirão que o consumidor faça melhores negociações.

O novo cadastro positivo, que começou a ter as consultas liberadas em janeiro deste ano, tem potencial de injetar R$ 1,3 trilhão na economia brasileira nos próximos sete anos, incrementando o Produto Interno Bruto (PIB) em 0,54% ao ano, segundo a Associação Nacional dos Bureaus de Crédito (ANBC). Trata-se de um dos principais projetos da agenda BC#, conjunto de diretrizes de modernização do sistema financeiro implementado pelo Banco Central.

A expectativa do órgão regulador é que o novo cadastro contribua para a redução do spread bancário – a diferença entre o custo de captação do dinheiro pelos bancos e as taxas aplicadas aos clientes. A pontuação elevada do histórico de crédito dos clientes pode levar os bancos a considerar a oferta de linhas de crédito mais atrativas e personalizadas, além de acirrar a disputa das instituições financeiras pelo cliente.

Baseado em experiências internacionais, o histórico de informação sobre os tomadores de crédito compartilhado com todos potenciais credores tem sido fundamental para o bom funcionamento do mercado, segundo João Manoel Pinho de Mello, diretor de organização do sistema financeiro e resolução do BC. No Brasil, o cadastro positivo é operado por quatro birôs de crédito – SPC Brasil, Serasa Experian, Boa Vista SCPC e Quod – autorizados pelo Banco Central a reunir as informações dos consumidores e classificá-las.

"Em vários países do mundo, a lei do cadastro positivo ajudou a conceder o crédito. O dado negativo foi importante, mas não suficiente para reduzir a simetria de informação que propicia melhor análise do crédito", afirma Ricardo Thomaziello, diretor executivo de dados e analytics da Quod, birô de crédito dos principais bancos brasileiros, que já nasceu com o propósito de operar o cadastro positivo.

De acordo com pesquisa do International Finance Corporation (IFC), a implantação do cadastro positivo nos Estados Unidos praticamente duplicou o percentual de consumidores que passaram a ter acesso ao crédito, chegando a 80%; e cerca

"Mesmo que muitas vezes o consumidor tenha condições de realizar uma compra à vista, é aconselhável agora optar pelo parcelamento."

Roque Pellizzaro
Presidente do SPC Brasil.

de 50% dos americanos ficaram mais propensos a pagar em dia ao saber que o histórico de pagamentos influenciaria o score de crédito. Enquanto na Argentina, o uso das informações positivas gerou uma redução de 75% da inadimplência. Na China o crédito atingiu 150% do PIB, impactando no desenvolvimento econômico, com o banco de dados positivo.

A queda do número de inadimplentes e endividados vem sendo acompanhada pela área de gestão de riscos e birôs de crédito do IFC, instituição do Banco Mundial que acompanha a implantação do banco de dados com informações positivas pelo mundo.

Oito anos para a lei vigorar

O cadastro positivo é um mecanismo de pontuação (score) onde os bancos de dados autorizados pelo órgão regulador ranqueiam o consumidor por meio da análise de seus pagamentos e não mais daquilo que deixou de pagar. Foi criado em julho de 2011, mas a legislação passou a determinar seu funcionamento de maneira automática só oito anos depois, em julho de 2019.

“Em vários países do mundo, a lei do cadastro positivo ajudou a conceder o crédito. O dado negativo foi importante, mas não suficiente para reduzir a simetria de informação que propicia melhor análise do crédito.”

Ricardo Thomaziello
Diretor executivo de dados e analytics da Quod, birô de crédito dos principais bancos brasileiros.

Conforme especialistas, o projeto ficou parado por falta de posicionamento do Congresso Nacional frente às alterações trazidas pelo projeto de lei número 54/19. A abertura do cadastro positivo estava condicionada à autorização prévia do cadastro (modelo opt-in). A lei determinou que os cidadãos, logo após entrarem no cadastro positivo, devem ser informados da inclusão e contam com a opção de solicitar sua exclusão a qualquer momento aos birôs de crédito, que terão dois dias úteis para atender e comunicar aos demais birôs.

"Quando a lei entrou em vigor em 2013, ainda com o carácter de opt-in, havia 15 milhões de registros. Em 2018, com a aprovação da nova regulação, saímos de 10 milhões para 100 milhões de empresas e PJs", afirma Thomaziello. Além da inclusão automática dos consumidores no cadastro, a reformulação da lei estabeleceu o score de crédito, permitiu ao consumidor o acesso a seus dados, constatação das informações e proibição do uso de dados pessoais sensíveis, como preferência sexual, raça e distinção da classe social.

Por força da regulação bancária internacional, no cadastro negativo os bancos são obrigados a consultar sempre dois birôs para evitar problemas. Para o cadastro positivo, as instituições bancárias recebem as informações abertas dos quatro Gestores de Banco de Dados (GBD) e vão interpretando.

Para Pellizzaro, o mercado de crédito era muito semelhante ao de seguro no modelo antigo, por precificar o risco e só levar em conta o bem assegurado, sem apresentar informações suficientes para a avaliação do risco de crédito. "Temos que considerar que o risco da operação do seguro de um carro é diferente para uma pessoa de 50 anos, que já tem histórico de crédito, de outra, de 19 anos, que está começando a vida", afirma Pellizzaro. As seguradoras hoje passaram a personalizar o risco, precificando a base de cálculo, o valor do bem mais o percentual aplicado para fazer a média.

O valor do score

O score mede a probabilidade do consumidor pagar a conta em dia. Em geral a pontuação de um score vai de 0 a mil. Para as pessoas que nunca tomaram crédito, o score costuma ser baixo. Um score mediano fica na faixa de 500 a 750 pontos. Se o consumidor atingir a faixa dos 800 poderá usar essa nota como moeda de troca em qualquer banco. A empresa é que vai decidir o crédito, análise de dado, o apetite a risco de diferentes perfis de clientes e combinar com outras informações financeiras para traçar o histórico do crédito.

A expectativa é que nos próximos anos as pessoas comecem a construir seu score para trazer vantagens à sua vida financeira.

Os critérios para montar a pontuação do score costumam variar de um birô para o outro. Mas é comum todos tomarem como base itens considerados neutralizadores na avaliação, como pontualidade de pagamento, assiduidade, manutenção de residência, profissão e análise macroeconômica. O perfil de risco e a aprovação do crédito dependem da análise macroeconômica.

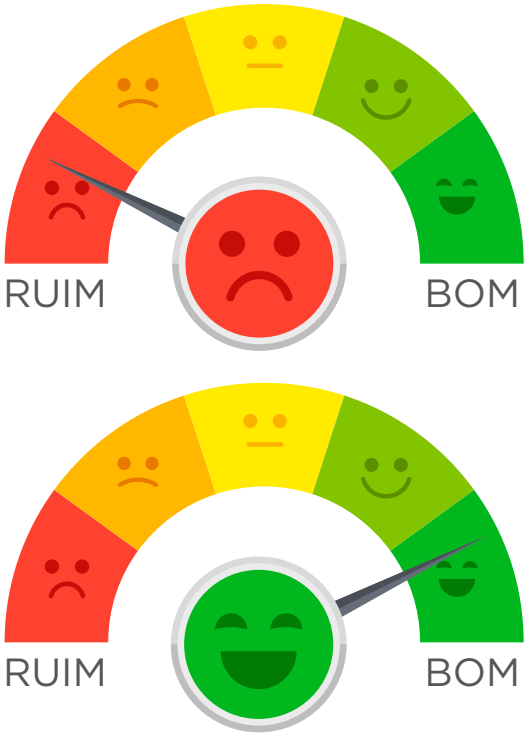
Caso um segmento da economia atravesse um momento de dificuldade, poderá comprometer na avaliação do histórico de crédito do consumidor. “A pandemia afetou o setor de aviação, certamente essa situação refletirá no score de um piloto. Como a área de engenharia civil está aquecida, o pedreiro leva mais chance de ter seu score melhorado”, diz Pellizzaro.

Se o cidadão apresenta um histórico de 10 anos de pagamento pontual, a interpretação dos sistemas de dados o considera um bom gestor de seu orçamento e que, certamente, não se arriscará a tomar empréstimos caso perca seu emprego. O fato de o consumidor ter regularidade de pagamento de suas dívidas, neutraliza todas as variáveis traçadas para a avaliação. Se o seu histórico de crédito apresenta um acúmulo de dívida mensal de R$ 3 mil, a solicitação de um empréstimo de R$ 15 mil já vai acender o alerta.

Muitas empresas e bancos customizam seu score e não compartilham com o mercado. Uma loja que vende móveis, por exemplo, pode assumir riscos diferentes da que comercializa aparelho de celular,

que muitas vezes é comprado para acertar dívidas. A análise de concessão de crédito costuma ser subjetiva pelo risco, margens e alto apetite, segundo Pellizzaro. “O score é a fórmula da coca-cola, cada um tem a sua, mas não conheço caso de alguém ser mal avaliado em um birô e bem avaliado no outro.”

A Câmara Interbancária de Pagamento (CIP) do Banco Central, responsável por controlar as milhões de transações financeiras realizadas no comércio eletrônico brasileiro, funciona como um hub para os birôs de crédito, que por determinação legal, são obrigados a dar acesso ao score de forma gratuita.



Percepção das vantagens

O brasileiro comum ainda não vê valor na pontuação do histórico de crédito. Enquanto birôs e instituições financeiras já começam a utilizar ferramentas de alta tecnologia para entender em profundidade o comportamento do consumidor e chegar a um score que seja bom e tenha aderência. A expectativa é que nos próximos dois anos as pessoas comecem a construir seu score para trazer vantagens à sua vida financeira.

Como há dados que não são extraídos de nenhum score, os gestores e bancos de dados apostam na tendência de o consumidor depositar voluntariamente informações que considere relevantes para melhorar a pontuação de seu cadastro, como o Imposto de Renda, explica o presidente da SPB Brasil. Aliás, essa prática já é comum em alguns países. Nos Estados Unidos, que já operam com score há 30 anos, a maior parte da receita dos birôs de crédito americanos atualmente vem de informações que os cidadãos pedem para colocar em seus cadastros.

Na Quod, os cientistas de dados estatísticos usam ferramentas de analytics e machine learning em larga escala. A jornada de inteligência analítica já começa a interagir com clientes e segurança da informação. Segundo Thomaziello, o score pode ser consultado no portal do birô por Interfaces de Programação de Aplicações (API’s). Indicadores de negócio permitem fazer segmentação de mercado e persona de cobrança.

O score mede a probabilidade de o consumidor pagar a conta em dia. Vai de 0 a 1000.

O diferencial da Quod é o tratamento do dado e sua especialização é fazer a gestão de informação para as empresas. “O crédito é um ciclo composto de concessão, gestão e fraude, que é a parte mais importante. Na pandemia, houve clientes que começaram a trabalhar com os sistemas em agência de ponto de venda e nos consultavam para tomar decisão”, diz. Uma vez processado, o dado torna-se disponível para o consumidor em até 60 dias.

Para aprimorar suas soluções de análise de crédito e prevenção à fraude, a Quod fechou uma parceria com a TIM, que permitirá a verificação e autenticação das informações de forma mais rápida, prática e segura. A iniciativa beneficiará, especialmente, os clientes da operadora que terão a análise de pedidos de crédito, empréstimo e financiamento concluídas com mais velocidade e segurança em todo país.

Queda da inadimplência

Com atuação em 2 mil municípios, a maior base do SPC Brasil é o pequeno varejo de baixa renda, localizado no interior. Como os níveis de transações reduziram muito durante o período de pandemia, a inadimplência caiu. Mas só a partir de janeiro, quando encerrar o prazo de recebimento do auxílio emergencial concedido pelo governo, será possível ter uma visão mais assertiva sobre o comportamento do mercado.

“Tivemos um forte impacto na receita durante o isolamento social, pois o pequeno comércio não usou os birôs”, diz Pellizzaro. O consumidor paga por informação, que são tabeladas com valores diferenciados. As informações de cartório e de protesto costumam ser bancadas pelo próprio birô. Na hora de consultar, o pequeno lojista se limita a levantar os dados da Junta Comercial. O birô, então, compra a informação e disponibiliza para ele ao custo que varia de R$ 2 a R$ 40 cada