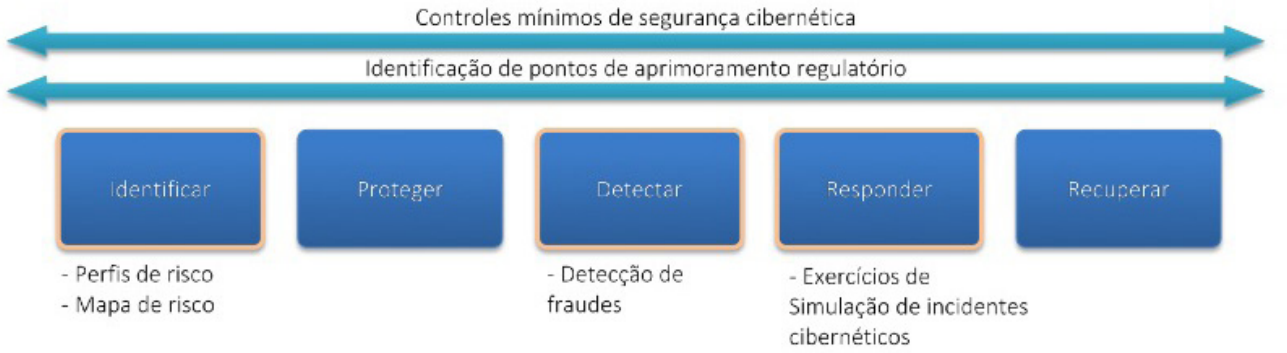
Temas Selecionados

2

2.1 Programa de Aprimoramento da Resiliência Cibernética do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro

O BCB reforça sua atuação no aprimoramento da resiliência cibernética do setor financeiro com a incorporação do Parc à Agenda BC#. O BCB finalizou no início de 2021 a iniciativa "Aprimoramento da supervisão do risco cibernético do SFN" da Agenda BC#, que tinha os objetivos de aprimorar o ferramental de supervisão e de executar ações de fiscalização para verificar a observância da regulamentação vigente pelas instituições financeiras. Entretanto, ciente da necessidade de tratar as implicações do risco cibernético de forma cada vez mais abrangente, o BCB constituiu um grupo de trabalho para definir um conjunto de ações a serem desenvolvidas nos próximos dezoito meses, consolidadas no Parc.

Figura 2.1.1 – Temas tratados nas ações do Parc *versus* funções do *framework* do *National Institute of Standards and Technology* (NIST) para segurança cibernética



O BCB identificou a necessidade de trabalhar questões de resiliência operacional e cibernética de forma ampla, visto que garantir a solidez das instituições individualmente pode não ser suficiente para garantir a solidez do sistema financeiro. Torna-se cada vez mais importante fomentar a integração entre instituições e coordenar ações de forma a se mitigar o risco do "elo mais frágil", assegurando que todas as instituições aprimorem seus controles de forma compatível com suas exposições ao risco cibernético. Além disso, passou a ser cada vez mais crítico tratar as implicações para as IFs, decorrentes de eventos de indisponibilidade de serviços críticos para as atividades do SFN, como serviços providos por IMFs.

Com a implementação do Parc, espera-se que novas capacidades sejam agregadas ao enfrentamento do risco cibernético, possibilitando que o desenvolvimento de projetos estruturantes que empregam inovações tecnológicas não traga implicações para a solidez do SFN. Nos últimos anos, o BCB já vislumbrava que, apesar dos avanços obtidos até então, novas ameaças à resiliência operacional e cibernética demandariam o aprimoramento contínuo dos arcabouços de regulação e de supervisão, seja para endereçar as mudanças no perfil de riscos das instituições em decorrência do processo de transformação digital, seja para implementar mecanismos adequados para o enfrentamento de novas ameaças cibernéticas.

O ano de 2020 certamente ficará registrado na memória das pessoas como um período de grandes transformações no SFN. Foi um ano marcado pelos desafios causados por uma pandemia de grandes proporções e pelo processo de transformação desencadeado pela implantação de projetos tecnologicamente inovadores.

Em um curto período, as IFs precisaram disponibilizar soluções que permitissem que seus colaboradores e clientes pudessem ofertar e demandar serviços remotamente. Para que isso fosse possível, as IFs recapacitaram suas infraestruturas de tecnologia e de telecomunicações, bem como desenvolveram ou adquiriram soluções para prestação de serviços financeiros em um contexto marcado por medidas de distanciamento social. O provimento de serviços financeiros por meio de canais digitais viabilizou a rápida implementação de programas governamentais criados para assistir às famílias e empresas mais impactadas pela crise sanitária.

Não obstante todas as implicações causadas pela pandemia, o ano de 2020 também foi marcado por transformações estruturais no sistema financeiro. O início de operação do Pix foi mais um passo de um processo de transformação que certamente alçará o SFN a um novo estágio, mais tecnológico, mais eficiente e mais acessível para os cidadãos, materializando assim a almejada democratização financeira. O Sistema Financeiro Aberto (Open Banking) e a melhoria do ambiente de garantias[75] são outros projetos altamente intensivos em tecnologia que moldarão o sistema financeiro nas próximas décadas.

Considerando todas as mudanças que estão por vir, o BCB tem uma certeza – a viabilização dessas iniciativas depende do fortalecimento dos controles das IFs. Para enfrentar adequadamente a maior exposição aos riscos tecnológicos e cibernéticos, as IFs devem investir continuamente no aprimoramento de seus controles e na atualização permanente de suas políticas de segurança cibernética, de forma a contemplar a transformação do ambiente onde se inserem.

Os incidentes cibernéticos noticiados nos primeiros meses de 2021 mostraram que o enfrentamento do risco cibernético não será fácil e demandará o aprimoramento contínuo das capacidades de defesa cibernética das IFs. Os participantes do SFN passarão a lidar com fraudadores cada vez mais equipados com informações sobre seus clientes. Os vazamentos massivos de dados pessoais de cidadãos brasileiros chamaram a atenção das IFs para um cenário ainda mais crítico – a utilização de informações obtidas ilegalmente de outras empresas para engendrar fraudes contra o sistema financeiro.

O Parc tem como objetivo assegurar uma visão integrada e sistêmica da exposição das instituições participantes do SFN e do SPB ao risco cibernético. Além disso, esse programa também tem o objetivo de desenvolver ações de prevenção e resposta a: (i) fraudes em sistema de pagamentos; (ii) incidentes cibernéticos que possam acarretar vazamento de informações pessoais ou protegidas por sigilo bancário; e (iii) indisponibilidade dos serviços e funções críticos para estabilidade financeira.

Uma das ações previstas no Parc refere-se ao desenvolvimento de perfis de risco cibernético, possibilitando a concepção de um mapa de risco que consolide a exposição das instituições ao risco cibernético. O mapa da exposição do SFN e do SPB a esse risco possibilitará a identificação de ações focadas em eliminar as fragilidades eventualmente identificadas. Esses perfis também propiciarão o estabelecimento de requerimentos mais aprimorados de controles internos com base na exposição ao risco.

O Parc também prevê o mapeamento de práticas e controles voltados para a detecção de fraudes, com foco inicial em sistemas de pagamento de alto valor. O aperfeiçoamento da capacidade de detecção de fraudes possibilitará o desenvolvimento de mecanismos para prevenir esses eventos, bem como para responder aos incidentes ocorridos.

75 O processo de melhoria do ambiente de garantias abrange iniciativas como: i) a escrituração das duplicatas escriturais; ii) o regramento para a realização de registro de recebíveis decorrentes de transações no âmbito de arranjo de pagamento; e iii) o aprimoramento da interoperabilidade entre os sistemas de registro e de depósito centralizado de ativos financeiros.

Outra ação relevante será o estabelecimento de práticas que viabilizem a resposta tempestiva a incidentes cibernéticos de grande magnitude, colocando o SFN plenamente alinhado às recomendações internacionais. Grandes avanços já foram obtidos com a participação de entidades do setor financeiro em exercícios como o Guardião Cibernético, conduzido pelo Comando de Defesa Cibernética do Exército Brasileiro. O objetivo do Parc é ampliar essa capacidade de resposta por meio da promoção de exercícios direcionados às entidades do sistema financeiro, explorando situações em que a resposta ao incidente demandará articulação de ações entre os participantes dos exercícios.

Uma vez que eventos cibernéticos não respeitam fronteiras, também é nevrálgico que o arcabouço regulatório brasileiro permaneça alinhado às melhores práticas internacionais. É desejável que se evite eventual fragmentação regulatória, de maneira que a cooperação internacional no combate ao risco cibernético ocorra sem maiores fricções.

Nesse sentido, ações relevantes do Parc recaem sobre a identificação e a definição de controles mínimos de segurança cibernética, alinhados aos perfis de risco identificados e às melhores práticas internacionais. Essas ações serão trabalhadas durante todo o desenvolvimento do Parc. Elas buscarão incorporar os avanços mais recentes sobre o tema, incluindo discussões realizadas em organismos internacionais e boas práticas da indústria.

2.2 Mecanismos de segurança do Pix

O Pix é um novo meio de pagamento que permite a transferência de recursos entre contas transacionais,[76] administradas por diferentes instituições ou não, de forma instantânea, simples e segura, estando disponível 24 horas por dia em todos os dias do ano.

O Pix possui três dimensões de segurança para garantir a integridade das transações. A primeira diz respeito à autenticação digital do usuário, a segunda trata da segurança das comunicações e da infraestrutura do sistema e a terceira dimensão se refere aos mecanismos de prevenção à fraude e ao vazamento de dados transacionais.

Todas essas dimensões de segurança foram desenhadas em conjunto com o Grupo de Trabalho sobre Segurança (GT-SEG), que funciona de forma permanente no âmbito do Fórum Pix[77] e que tem a participação dos principais especialistas em segurança das instituições participantes do Pix.

Cabe ainda salientar que, mesmo que porventura haja a materialização de fraude, todas as transações Pix são rastreáveis. A rastreabilidade de todas as transações permite a rápida atuação das autoridades policiais para recuperar recursos que eventualmente tenham sido movimentados de forma criminosa.

Autenticação digital do usuário

As transações Pix só podem ser iniciadas em ambiente seguro que seja acessado por meio de uma senha ou de outros dispositivos de segurança integrados ao telefone celular, como reconhecimento biométrico e reconhecimento facial. Esse requisito minimiza o risco de fraudes, principalmente em transações de comércio eletrônico. A oferta de dispositivos de segurança integrados ao telefone é responsabilidade das instituições participantes do Pix. Observa-se uma crescente oferta e um crescente uso dessas soluções, o que torna o processo de iniciação de um Pix ainda mais seguro.

76 Contas transacionais incluem: contas de depósito à vista, contas de poupança e contas de pagamento pré-pagas.

77 O Fórum Pix é o ambiente de discussões e de coordenação dos diversos agentes de mercado. O objetivo do Fórum é subsidiar o BCB no papel de definidor das regras de funcionamento do Pix.