



Novas regras para a segurança cibernética no setor financeiro

Resolução CMN nº 5.274 e Resolução BCB nº 538

Em um cenário global cada vez mais desafiador em termos de segurança cibernética, o Banco Central do Brasil (BACEN) tem se mostrado proativo na proteção do Sistema Financeiro Nacional (SFN).

Diante da crescente digitalização do setor e da complexidade dos riscos em ambientes digitais, que culminaram em ataques hackers de proporções inéditas em 2025, o BACEN tem intensificado sua atuação na regulamentação da segurança cibernética no ambiente financeiro. Nesse movimento, o regulador tem reforçado requisitos de governança, controles e procedimentos das instituições integrantes do SFN.

Esse incremento no rigor regulatório teve início com a publicação de um conjunto de normativos em setembro de 2025, voltados ao reforço da segurança do SFN, em especial à atuação de prestadores de serviços de tecnologia e instituições de pagamento não autorizadas.

Dando prosseguimento ao processo de endurecimento de medidas e aumento do nível de exigência, o BACEN publicou, em dezembro de 2025, a **Resolução CMN nº 5.274** e a **Resolução BCB nº 538**. Juntas, fazem parte desse esforço de atualização do arcabouço normativo, promovendo mudanças nas principais normas sobre a política de segurança cibernética e sobre os requisitos de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Quais são os principais impactos dos novos normativos?

1

Procedimentos e controles obrigatórios para redução de vulnerabilidades e atendimento dos objetivos de segurança

As políticas de segurança cibernética devem abranger, necessariamente, os procedimentos e controles mínimos listados pelo regulador. Esses procedimentos e controles incluem, mas não se limitam a:

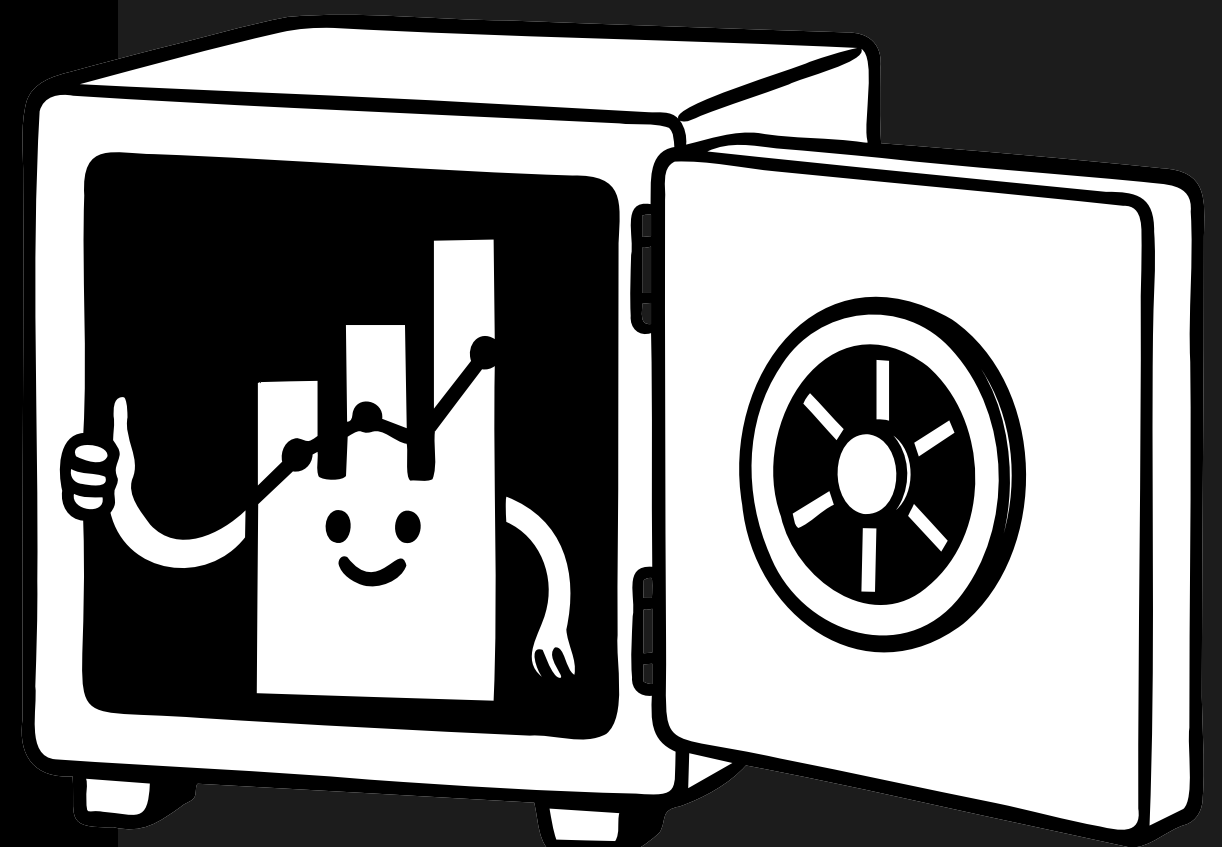
- Mecanismos de criptografia;
- Mecanismos de prevenção e detecção de intrusões;
- Mecanismos de prevenção de vazamento de informações;
- Mecanismos de proteção contra softwares maliciosos;
- Controles de acesso;
- Mecanismos de proteção da rede;
- Gestão de certificados digitais;
- Requisitos de segurança para integração de sistemas;
- Ações de inteligência no ambiente cibernético.



2

Requisitos de segurança adicionais para comunicação eletrônica de dados na Rede do Sistema Financeiro Nacional (RSFN)

- Uso de múltiplos fatores de autenticação para acesso administrativo ao ambiente Pix e Sistema de Transferência de Reservas (STR);
- Isolamento físico e lógico do ambiente do Pix;
- Isolamento físico e lógico do ambiente do STR;
- Monitoramento do uso de credenciais e certificados digitais;
- Implementação de mecanismos de validação da integridade das transações antes da assinatura digital;
- Vedação do acesso de empresas prestadoras de serviços a terceiros às chaves privadas associadas a certificados digitais.



3

Realização de testes de intrusão

As instituições deverão promover, com **periodicidade mínima anual**, testes de intrusão, realizados com independência e imparcialidade por **especialista** contratado para essa finalidade. Os resultados dos testes deverão ser documentados, especialmente as eventuais vulnerabilidades identificadas e os planos de ação para correção.

4

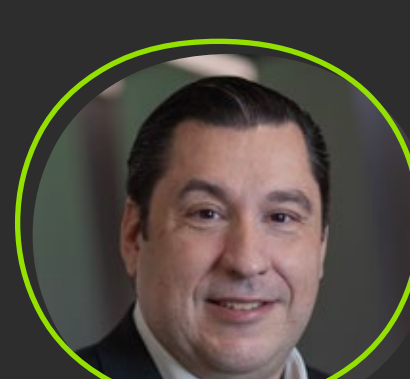
Enquadramento de fornecedores relevantes

Os serviços prestados para comunicação eletrônica de dados na RSFN serão considerados relevantes, independentemente da forma de conexão com a RSFN. **Isso inclui os prestadores de serviços que fornecem serviços de processamento de mensagens no âmbito do SFN e do Sistema de Pagamentos Brasileiro (SPB).**



As recentes mudanças regulatórias reforçam a necessidade de que as instituições revisitem seus procedimentos e normativos de segurança cibernética, garantindo aderência às novas diretrizes do Banco Central do Brasil. O apoio de uma assessoria jurídica especializada, nessa etapa, poderá contribuir para um processo de adequação mais fluido, seguro e eficiente.

Este conteúdo foi elaborado pela equipe de especialistas em inovação em serviços financeiros do Opice Blum.



MARCOS BRUNO
Sócio
mbruno@opiceblum.com.br
+55 11 4040-9751



FLORENCE TERADA
Sócia
florence.terada@opiceblum.com.br
+55 11 4040-9751