DIREITO DIGITAL E PROTEÇÃO DE DADOS

BCB: NOVAS REGRAS PARA AUMENTAR A CIBERSEGURANÇA DO SFN E DO SPB

09 DE SETEMBRO DE 2025

AUTORES

EDUARDO CASTRO
SÓCIO / SÃO PAULO

JULIANA ABRUSIO
SÓCIA / SÃO PAULO

NEI ZELMANOVITS
SÓCIO / SÃO PAULO

MARCELO DE CASTRO CUNHA FILHO
ADVOGADO / SÃO PAULO

A Resolução BCB 498, publicada em 5 de setembro, estabelece novas regras para garantir maior segurança ao Sistema Financeiro Nacional (SFN) e ao Sistema de Pagamentos Brasileiro (SPB). O conjunto de medidas traz novos requisitos que os provedores de serviço de tecnologia da informação (PSTI) deverão adotar para aumentar a cibersegurança de suas operações. A partir de agora, o Banco Central (BCB) exigirá o credenciamento desses prestadores de serviços para atuarem conectados à rede do Sistema Financeiro Nacional (RSFN).

O credenciamento de PSTIs no BCB deve atender aos seguintes requisitos:

- Adesão aos princípios e às regras da Rede do Sistema Financeiro Nacional;
- Comprovação da constituição regular do PSTI;
- Comprovação de não enquadramento em vedações regulatórias;
- Comprovação de capacidade técnico-operacional para prestar os serviços de processamento de dados, para fins de acesso à RSFN. Devem ser observados os requisitos estabelecidos na resolução e os padrões técnicos referentes à comunicação eletrônica de dados no âmbito do SFN, estabelecidos pelo Departamento de Tecnologia da Informação (Deinf) do BCB;
- Designação de diretor ou diretores responsáveis pela segurança da informação, segurança cibernética e pela gestão de riscos e *compliance*, com capacitação técnica compatível com as atribuições do cargo. Essa capacitação deve ser comprovada com base na formação acadêmica, na experiência profissional na área de atuação ou em conhecimentos técnicos específicos relativos à segurança da informação, à segurança cibernética e à gestão de riscos e *compliance*;
- Designação de diretor ou diretores responsáveis pela gestão de crises operacionais, com capacitação técnica compatível com as atribuições do cargo, comprovada com base na formação acadêmica, na experiência profissional na área de atuação ou em conhecimentos técnicos específicos relativos à gestão de crises operacionais;
- Atendimento de condições específicas previstas na resolução, por parte do controlador, dos integrantes do grupo de controle e dos administradores do PSTI. As condições são: reputação ilibada; comprovação de qualificação técnica ou experiência profissional compatível com as atribuições do cargo ou função, considerada a complexidade e o porte do PSTI; não ter sido declarada falida ou insolvente, salvo se reabilitada; e comprovação, por meio de certificado de auditor independente registrado na Comissão de Valores Mobiliários (CVM), da situação cadastral regular na Receita Federal e da ausência de restrições graves em cadastros de inadimplentes que comprometam sua capacidade de gerir ou controlar o PSTI.
- Comprovação de capital social realizado e de patrimônio líquido no valor mínimo de R$ 15 milhões. O BCB pode exigir montante superior, proporcional ao volume de operações projetado e ao perfil de risco do PSTI, por meio de demonstrações financeiras auditadas por empresa de auditoria independente registrada na CVM;
- Comprovação do estabelecimento de mecanismos de governança corporativa e de gestão de riscos previstos na resolução;
- Comprovação de capacidade técnico-operacional para prestação de informações ao BCB, de acordo com a resolução;
- Comprovação de obtenção e manutenção de certificação de segurança da informação em norma reconhecida internacionalmente ou asseguração independente aceita pelo BCB;
- Comprovação da contratação de auditoria externa anual independente em segurança da informação e, quando aplicável, em prevenção à lavagem de dinheiro e a financiamento do terrorismo, com envio dos relatórios ao BCB e às instituições contratantes;
- Comprovação da contratação de seguro de responsabilidade civil e de riscos operacionais, com cobertura mínima definida pelo BCB, incluindo incidentes de fraude e segurança cibernética; e
- Elaboração e manutenção de plano de continuidade de negócios e de testes periódicos de contingência, com comprovação anual ao BCB.

De acordo com a Resolução BCB 498/25, os PSTIs devem ter estrutura de governança corporativa compatível com sua natureza, porte, complexidade, estrutura e perfil de risco, assegurando processos decisórios transparentes, mecanismos de controle interno eficazes e adequada gestão de riscos.

Além disso, os PSTIs devem instituir, no âmbito da alta administração, diretores responsáveis por funções críticas, como diretor de Segurança da Informação e Cibernética.

Os PSTIs também devem separar as atividades, os ambientes computacionais e os demais recursos necessários à prestação de serviços de processamento de dados para fins de acesso à RSFN dos demais serviços ou atividades eventualmente providos.

Isso deve ser feito com a adoção de **políticas de gestão de riscos** compatíveis com sua natureza, porte, complexidade, estrutura e perfil de risco, amparadas nos princípios e nas melhores práticas de mercado. Essas políticas devem abordar, obrigatoriamente, questões de segurança da informação e cibernética, continuidade de negócios, gestão de crises operacionais, gestão de fraudes, controles internos e conformidade e auditoria interna.

A política de continuidade de negócios deve contemplar, no mínimo:

> procedimentos e prazos estimados para reinício e recuperação das atividades em caso de interrupção dos processos críticos de negócio, bem como as ações de comunicação necessárias;
>
> testes e revisões dos planos de continuidade de negócios com periodicidade mínima anual;
>
> instalação e operação de centro de processamento secundário – sujeito a riscos diferentes do centro de processamento principal –, capaz de processar volumes, no mínimo, iguais ao maior volume verificado nos últimos 252 dias úteis, acrescido de um percentual de segurança, e com replicação de dados do centro de processamento principal; e
>
> procedimentos de emergência, no caso de impedimento simultâneo dos centros de processamento principal e secundário.

Os PSTIs devem, ainda, implementar e manter política de gestão de fraudes para mitigar situações atípicas que possam comprometer o funcionamento regular do SPB. Essa política deve abranger, no mínimo:

> estabelecimento de canal para comunicação de indícios de fraudes;
>
> estabelecimento de mecanismos de prevenção a fraudes, incluindo liberação de dados para conciliação de informações, acesso a trilhas de auditoria e definição de limites operacionais;
>
> monitoramento em tempo integral, 24 horas por dia, 7 dias por semana, para identificação em tempo real, com base em padrões históricos e comportamentais, de transações atípicas ou fraudulentas, avaliando desvios em relação aos parâmetros esperados no que se refere, inclusive, a valores transacionados, volume de transações e quantidade de transações por unidade de tempo;
>
> avaliação de atipicidades em etapa anterior ao processo de encaminhamento de uma transação ao BCB;
>
> definição de mecanismos de validação da integridade das transações durante as etapas de processamento;
>
> existência de mecanismo de interrupção do fluxo completo de transações em caso de grave suspeita de comprometimento; e
>
> estabelecimento de canal que possibilite a comunicação tempestiva de indícios de fraude com instituições financeiras e demais instituições supervisionadas pelo BCB que possam ser impactadas por esses eventos.

As políticas de governança estabelecidas na Resolução BCB 498/25 devem ser aprovadas pelo conselho de administração ou, se inexistente, pela diretoria prevista em estatuto ou contrato social.

Essas políticas deverão ser revisadas, no mínimo, anualmente ou sempre que houver alteração relevante na estrutura ou no perfil de risco do PSTI. O objetivo é manter uma política de segurança da informação e cibernética baseada em princípios e diretrizes que busquem garantir a segurança dos dados, das informações, dos sistemas de informação e dos demais recursos computacionais utilizados, em conformidade com padrões internacionalmente reconhecidos.

A Resolução BCB 498/25 estabelece mecanismos de rastreabilidade de transações, que devem conter, no mínimo:

> trilhas de auditoria do processamento fim-a-fim dos dados e das informações, incluindo a definição e a geração de *logs* que possibilitem identificar falhas de processamento ou comportamento atípicos, bem como subsidiar análises;
>
> definição de tempo de retenção de informações de acordo com o tipo de processamento realizado;
>
> retenção segura das trilhas de auditoria; e
>
> acesso às trilhas de auditoria pelas instituições que utilizam os serviços providos pelo PSTI, para conciliação ou gestão de riscos.

A resolução também dispõe sobre a avaliação e correção de vulnerabilidades exigindo que considerem, no mínimo:

> testes e análises periódicas para detecção de vulnerabilidades em sistemas de informação;
>
> varreduras físicas periódicas do ambiente tecnológico que possibilitem identificar dispositivos indevidamente conectados à rede corporativa que possam estabelecer conexão com ativos de tecnologia externos;
>
> análises periódicas do ambiente tecnológico com o objetivo de identificar vulnerabilidades que possam comprometer a segurança dos ativos de tecnologia do PSTI; e
>
> testes de intrusão periódicos.

É importante ressaltar que o credenciamento de que trata a Resolução BCB 498/25 não configura autorização para o funcionamento da atividade econômica de PSTI nem altera os deveres legais e contratuais do PSTI diante de seus clientes e parceiros.

A resolução reflete o compromisso do BCB em aprimorar a regulação do setor financeiro, garantindo um sistema mais seguro e eficiente para todos os usuários. A norma tem vigência imediata e o prazo para sua adequação pelos PSTIs é de quatro meses a partir de sua publicação.

Para mais informações sobre o tema, contate o time de Tecnologia, Dados e Ciber do Machado Meyer em conjunto com o time da prática Bancária.