BANCO CENTRAL DO BRASIL

Resolução BCB nº 498 de 5/9/2025

RESOLUÇÃO BCB Nº 498, DE 5 DE SETEMBRO DE 2025

Disciplina, no âmbito do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro, os requisitos, os procedimentos e as condições para o credenciamento de Provedor de Serviços de Tecnologia da Informação – PSTI e dá outras providências.

A Diretoria Colegiada do Banco Central do Brasil, em sessão realizada em 3 de setembro de 2025, com base no art. 10 da Lei nº 4.595, de 31 de dezembro de 1964, e no art. 10 da Lei nº 10.214, de 27 de março de 2001,

R E S O L V E :

Art. 1º Esta Resolução estabelece os requisitos, os procedimentos e as condições para o credenciamento de Provedor de Serviços de Tecnologia da Informação – PSTI para a prestação de serviço de processamento de dados, para fins de acesso à Rede do Sistema Financeiro Nacional – RSFN.

Parágrafo único. O credenciamento de que trata esta Resolução não configura autorização para o funcionamento da atividade econômica de PSTI, tampouco altera os deveres legais e contratuais do PSTI perante seus clientes e parceiros.

Art. 2º Para fins do disposto nesta Resolução, considera-se:

I - comunicação eletrônica de dados: processo de transferência de informações entre sistemas computacionais;

II - RSFN: estrutura de comunicação de dados que tem por finalidade amparar o tráfego de informações no âmbito do Sistema Financeiro Nacional – SFN para serviços autorizados; e

III - PSTI: entidade credenciada apta a prestar serviços de processamento de dados, para fins de acesso à RSFN, às instituições financeiras e às demais instituições supervisionadas pelo Banco Central do Brasil.

CAPÍTULO I
DO CREDENCIAMENTO

Art. 3º O credenciamento de PSTI no Banco Central do Brasil fica sujeito ao atendimento, pelo solicitante, dos seguintes requisitos:

I - adesão aos princípios e às regras da RSFN;

II - comprovação da constituição regular do PSTI;

III - comprovação de não enquadramento nas vedações estabelecidas no art. 6º;

IV - comprovação de capacidade técnico-operacional para prestar os serviços de processamento de dados, para fins de acesso à RSFN, observando os requisitos estabelecidos nesta Resolução e os padrões técnicos referentes à comunicação eletrônica de dados no âmbito do SFN, estabelecidos pelo Departamento de Tecnologia da Informação – Deinf do Banco Central do Brasil;

V - 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, 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*;

VI - 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;

VII - atendimento das condições previstas no art. 5º desta Resolução, por parte do controlador, dos integrantes do grupo de controle e dos administradores do PSTI;

VIII - comprovação de capital social realizado e de patrimônio líquido no valor mínimo de R$15.000.000,00 (quinze milhões de reais), podendo o Banco Central do Brasil 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 Comissão de Valores Mobiliários;

IX - comprovação do estabelecimento de mecanismos de governança corporativa e de gestão de riscos previstos no Capítulo III;

X - comprovação de capacidade técnico-operacional para prestação de informações ao Banco Central do Brasil de que trata o Capítulo IV;

XI - comprovação de obtenção e manutenção de certificação de segurança da informação em norma reconhecida internacionalmente, ou asseguração independente aceita pelo Banco Central do Brasil;

XII - comprovação da contratação de auditoria externa anual independente em segurança da informação e, quando aplicável, em prevenção à lavagem de dinheiro e financiamento do terrorismo, com envio dos relatórios ao Banco Central do Brasil e às instituições contratantes;

XIII - comprovação da contratação de seguro de responsabilidade civil e de riscos operacionais, com cobertura mínima definida pelo Banco Central do Brasil, incluindo incidentes de fraude e segurança cibernética; e

XIV - elaboração e manutenção de Plano de Continuidade de Negócios e de testes periódicos de contingência, com comprovação anual ao Banco Central do Brasil.

§ 1º A adesão de que trata o inciso I do *caput* se dará por meio da celebração de Termo de Adesão e Responsabilidade, firmado pelo representante legal do PSTI mediante uso de certificado digital emitido por autoridade certificadora da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

§ 2º O PSTI deve comprovar anualmente, na forma e na data estipuladas pelo Banco Central do Brasil, que permanecem atendidos os requisitos fixados nos incisos I a XIII do *caput*.

§ 3º O PSTI que descumprir a obrigação prevista no § 2º ficará sujeito ao descredenciamento de que trata o art. 7º, *caput*, inciso II.

Art. 4º O PSTI deve manter capacidade econômico-financeira compatível com a natureza crítica dos serviços prestados e com os riscos operacionais assumidos.

Art. 5º São condições para que pessoa natural seja controladora ou integre grupo de controle do PSTI, direta ou indiretamente, ou exerça função de administrador:

I - possuir reputação ilibada;

II - comprovar qualificação técnica ou experiência profissional compatível com as atribuições do cargo ou função, considerada a complexidade e o porte do PSTI;

III - não ter sido declarada falida ou insolvente, salvo se reabilitada; e

IV - comprovar, mediante certificado de auditor independente registrado na Comissão de Valores Mobiliários, situação cadastral regular na Receita Federal e ausência de restrições graves em cadastros de inadimplentes que comprometam sua capacidade de gerir ou controlar o PSTI.

Art. 6º É vedado o credenciamento como PSTI:

I - às operadoras de serviço de comunicação contratadas para a operação da RSFN;

II - aos prestadores de serviço contratados para o gerenciamento e o monitoramento da RSFN;

III - às instituições financeiras e demais instituições supervisionadas pelo Banco Central do Brasil, ressalvado o disposto no § 1º;

IV - às partes relacionadas das instituições referidas nos incisos I a III; e

V - às entidades cujos controladores ou administradores não atendam às condições de idoneidade, reputação e qualificação técnica previstas nesta Resolução.

§ 1º As instituições de que trata o inciso III do *caput* poderão atuar como PSTI exclusivamente para atender às demais instituições integrantes do mesmo conglomerado financeiro, desde que mantida a segregação operacional e observados os requisitos técnicos e de segurança aplicáveis.

§ 2º O disposto no § 1º não afasta o dever das instituições atendidas pela instituição mencionada no inciso III do *caput* e que atuem como PSTI de observarem a regulamentação em vigor para a contratação de serviços de processamento, armazenamento de dados e computação em nuvem.

CAPÍTULO II
DO DESCREDENCIAMENTO

Art. 7º O descredenciamento do PSTI poderá ocorrer:

I - a pedido do PSTI; e

II - de ofício, pelo Banco Central do Brasil, nas hipóteses previstas nesta Resolução.

Art. 8º O PSTI que pretenda ingressar com pedido de descredenciamento no Banco Central do Brasil deve comunicar formalmente às instituições contratantes, por meio de correspondência específica, com antecedência mínima de trinta dias da data do referido pedido, devendo apresentar ao Banco Central do Brasil plano de descontinuidade e de transição dos serviços prestados.

Art. 9º O Banco Central do Brasil poderá promover o descredenciamento de que trata o art. 7º, *caput*, inciso II, quando verificar, a qualquer tempo, o descumprimento grave ou recorrente dos requisitos estabelecidos nesta Resolução, especialmente em relação:

I - ao credenciamento no Banco Central do Brasil;

II - à governança corporativa, à gestão de riscos e à segurança da informação;

III - à prestação de informações ao Banco Central do Brasil;

IV - à manutenção dos requisitos de capital, seguro e certificações de segurança exigidos;

V - a falhas operacionais ou incidentes de segurança que comprometam de forma significativa a integridade, a disponibilidade ou a confiabilidade da RSFN ou dos serviços de pagamento por ela suportados;

VI - à prática de atos que caracterizem fraude, dolo ou má-fé na condução das atividades do PSTI;

VII - ao não atendimento, no prazo fixado, de determinações ou medidas preventivas impostas pelo Banco Central do Brasil nos termos desta Resolução; e

VIII - a situações que evidenciem perda das condições de idoneidade, reputação ou qualificação técnica de controladores e administradores do PSTI.

Art. 10. O descredenciamento, em qualquer uma das hipóteses previstas no art. 7º, será precedido da implementação do plano de saída ordenada previsto no art. 20.

CAPÍTULO III
DA GOVERNANÇA CORPORATIVA E DA GESTÃO DE RISCOS

Seção I
Da governança corporativa

Art. 11. O PSTI deve possuir 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.

§ 1º A estrutura de governança deve assegurar, no mínimo:

I - segregação de funções entre gestão executiva, gerenciamento de riscos, *compliance*, segurança da informação e auditoria interna, de forma a evitar conflitos de interesse e concentração de poderes;

II - existência de órgão de administração colegiado (conselho de administração ou equivalente), com participação proporcional de membros independentes, sempre que o porte ou relevância sistêmica do PSTI assim justificar;

III - elaboração e divulgação de políticas formais de governança corporativa, incluindo gestão de riscos, segurança cibernética, *compliance*, auditoria interna e continuidade de negócios;

IV - mecanismos que assegurem a transparência societária, incluindo divulgação pública da estrutura societária, identificação de controladores e beneficiários finais, e comunicação tempestiva de alterações relevantes ao Banco Central do Brasil;

V - avaliação prévia e contínua da idoneidade, reputação e experiência profissional dos controladores, administradores e principais executivos, conforme critérios estabelecidos nesta Resolução; e

VI - existência de Comitê de Gestão de Crises Operacionais, amparado por estrutura, papéis e responsabilidades formalmente definidos.

§ 2º Os administradores e os membros dos órgãos societários do PSTI devem ser profissionais de reconhecida competência técnica e estratégica na matéria, aptos a desempenhar seus múltiplos papéis na busca pelo cumprimento dos objetivos estratégicos.

§ 3º O PSTI deve instituir, no âmbito da alta administração, diretores responsáveis por funções críticas, incluindo, no mínimo:

I - Diretor de Segurança da Informação e Cibernética, responsável pela implementação de políticas de cibersegurança e pela gestão de incidentes operacionais;

II - Diretor de Riscos e *Compliance*, responsável pela supervisão da conformidade regulatória e pela efetividade dos controles internos;

III - Diretor responsável pelo relacionamento com o Banco Central do Brasil, responsável pela prestação de informações e interlocução regulatória; e

IV - Diretor responsável pela gestão de crises operacionais e pela coordenação do Comitê de Gestão de Crises Operacionais.

Art. 12. O Comitê de Gestão de Crises Operacionais, estabelecido no âmbito da estrutura de governança do PSTI, deve:

I - deliberar sobre o acionamento do plano de gestão de crises previsto na política de que tratam os arts. 21 e 22;

II - declarar o encerramento das crises operacionais;

III - prestar informações tempestivas ao Banco Central do Brasil sobre a crise operacional; e

IV - registrar informações e evidências que suportaram a tomada de decisões durante a gestão da crise operacional.

Seção II
Da gestão de riscos

Art. 13. O PSTI deve segregar 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.

Art. 14. O PSTI deve estabelecer 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.

Art. 15. O PSTI deve estabelecer políticas de gestão de riscos voltadas a tratar, no mínimo, de:

I - segurança da informação e cibernética;

II - continuidade de negócios;

III - gestão de crises operacionais;

IV - gestão de fraudes;

V - controles internos e conformidade; e

VI - auditoria interna.

Parágrafo único. As políticas de que trata o *caput* devem ser aprovadas pelo conselho de administração ou, se inexistente, pela diretoria prevista em estatuto ou contrato social, e revisadas, no mínimo, anualmente, ou sempre que houver alteração relevante na estrutura ou no perfil de risco do PSTI.

Art. 16. O PSTI deve implementar e manter política de segurança da informação e cibernética formulada com base 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.

Art. 17. A política de segurança da informação e cibernética de que trata o art. 16 deve contemplar, no mínimo, os seguintes aspectos:

I - mecanismos de criptografia, de prevenção e detecção de intrusão, de prevenção de vazamentos de informações e de proteção contra *softwares* maliciosos;

II - mecanismos de rastreabilidade de transações;

III - gestão de cópias de segurança dos dados e das informações;

IV - avaliação e correção de vulnerabilidades do ambiente computacional e dos sistemas de informação utilizados na prestação de serviços;

V - controle de acesso;

VI - aplicação regular de correções de segurança;

VII - mecanismos de proteção da rede;

VIII - segregação dos ambientes computacionais, limitando-se o acesso ao ambiente de produção e aos recursos computacionais críticos;

IX - isolamento físico e lógico do ambiente Pix dos demais sistemas da instituição, caso seja também provedor de *software* como serviço para participante desse ecossistema de pagamentos, mantendo instância dedicada e apartada dos demais ambientes nos casos de uso de nuvem pública;

X - isolamento físico e lógico do ambiente Sistema de Transferência de Reservas – STR dos demais sistemas da instituição, caso seja também provedor de *software* como serviço para participante desse ecossistema de pagamentos, mantendo instância dedicada e apartada dos demais ambientes nos casos de uso de nuvem pública;

XI - gestão de certificados digitais;

XII - controles específicos para integração com outras partes por meio de interfaces eletrônicas;

XIII - certificação técnica das soluções de tecnologia da informação utilizadas por instituições financeiras e outras instituições supervisionadas pelo Banco Central do Brasil para integrar, por meio de interfaces eletrônicas, com os serviços providos pelo PSTI; e

XIV - ações de inteligência cibernética, incluindo o monitoramento de informações de interesse (clientes, chaves, credenciais, vulnerabilidades etc.) na Internet, Deep e Dark Web, além de grupos privados de comunicação.

§ 1º O PSTI não deverá ter acesso às chaves privadas utilizadas para a assinatura das mensagens no âmbito dos arranjos e sistemas de pagamento providos pelo Banco Central do Brasil.

§ 2º Os mecanismos de rastreabilidade de transações de que trata o inciso II do *caput* devem contemplar, no mínimo:

I - 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;

II - definição de tempo de retenção de informações de acordo com o tipo de processamento realizado;

III - retenção segura das trilhas de auditoria; e

IV - acesso às trilhas de auditoria pelas instituições que utilizam os serviços providos pelo PSTI, para fins de conciliação ou gestão de riscos.

§ 3º A avaliação e a correção de vulnerabilidades de que trata o inciso IV do *caput* deve contemplar, no mínimo:

I - testes e análises periódicas para detecção de vulnerabilidades em sistemas de informação;

II - varreduras físicas periódicas do ambiente tecnológico que possibilitem identificar dispositivos indevidamente conectados à rede corporativa que possam estabelecer conexão com ativos de tecnologia externos;

III - análises periódicas do ambiente tecnológico com o objetivo de identificar vulnerabilidades que possam comprometer a segurança dos ativos de tecnologia do PSTI; e

IV - testes de intrusão periódicos.

§ 4º O controle de acesso de que trata o inciso V do *caput* deve incluir, ao menos:

I - mecanismos para limitar o acesso à rede corporativa a usuários e dispositivos autorizados;

II - revisão periódica e tempestiva das permissões de acesso, em especial, de colaboradores terceirizados com acesso ao ambiente computacional da instituição;

III - estabelecimento de múltiplos fatores de autenticação para acesso à rede corporativa a partir de ambientes externos; e

IV - para os ambientes Pix e STR, o acesso administrativo deve ser realizado sempre utilizando múltiplos fatores de autenticação.

§ 5º Os mecanismos de proteção da rede de que trata o inciso VII do *caput* devem contemplar, no mínimo:

I - estabelecimento de regras de firewall, assim como o monitoramento de conexões, evitando-se tentativas de conexão com sistemas críticos provenientes de ativos de tecnologia localizados fora da rede corporativa da instituição;

II - definição de critérios para o estabelecimento e o monitoramento de conexões com ambientes externos, em especial em horário noturno ou não convencional;

III - mecanismos para identificar e prevenir conexões indevidas com ambientes externos a partir do ambiente computacional do PSTI; e

IV - implementação e manutenção de processos e ferramentas para identificação, análise e tratamento de eventos atípicos no ambiente do PSTI, a exemplo da abertura de *virtual private networks* – VPN e de tentativas de acesso privilegiado, especialmente em horário noturno ou não convencional, assim como avaliação da implantação de controles mais robustos que mitiguem riscos de acessos indevidos nessas ocasiões.

§ 6º A gestão de certificados digitais de que trata o inciso XI do *caput* deve prever, no mínimo:

I - o monitoramento do uso de certificados digitais e controles para a guarda dessas informações; e

II - a validação de certificados revogados junto às autoridades certificadoras.

§ 7º Os controles específicos para integração com outras partes por meio de interfaces eletrônicas, de que trata o inciso XII do *caput,* devem considerar, no mínimo:

I - a definição de requisitos de segurança específicos para o fornecimento de serviços por meio de interfaces eletrônicas, garantindo a segurança e a integridade das operações;

II - a definição de requisitos operacionais e de segurança a serem implementados por instituições financeiras e pelas demais instituições supervisionadas pelo Banco Central do Brasil que almejem utilizar serviços fornecidos pelo PSTI por meio de interfaces eletrônicas;

III - o estabelecimento de mecanismos de monitoramento de operações, possibilitando a análise comportamental e detecção de operações atípicas;

IV - o estabelecimento de mecanismos de conciliação que permitam validar as operações processadas;

V - o estabelecimento de requisitos não funcionais relacionados ao fornecimento de serviços por meio de interfaces eletrônicas, bem como a realização de testes para validar a implementação desses requisitos;

VI - o estabelecimento de métricas e indicadores para monitoramento do desempenho dos serviços fornecidos por meio de interfaces eletrônicas;

VII - o monitoramento do desempenho dos serviços fornecidos por meio de interfaces eletrônicas;

VIII - o estabelecimento de mecanismos para detectar e inibir tentativas de uso indevido, tentativas de manipulação de comportamento e tentativas de extração de dados dos serviços fornecidos por meio de interfaces eletrônicas; e

IX - a definição, o estabelecimento e o monitoramento de limites operacionais para os serviços fornecidos por meio de interfaces eletrônicas.

§ 8º A certificação técnica de que trata o inciso XIII do *caput* deve considerar, no mínimo, a definição e a execução periódica de testes destinados a certificar que os sistemas computacionais utilizados por instituições financeiras e demais instituições supervisionadas pelo Banco Central do Brasil para integrar, por meio de interfaces eletrônicas, aos serviços providos pelo PSTI estão em conformidade com os requisitos operacionais e de segurança estabelecidos.

Art. 18. O PSTI deve implementar e manter política de continuidade de negócios para assegurar a continuidade das atividades da instituição e limitar os impactos decorrentes da interrupção dos processos críticos de negócio.

Art. 19. A política de continuidade de negócios de que trata o art. 18 deve contemplar, no mínimo, o seguinte:

I - 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;

II - testes e revisões dos planos de continuidade de negócios com periodicidade mínima anual;

III - instalação e operação de centro de processamento secundário, sujeito a conjunto de riscos diferentes do centro de processamento principal, capaz de processar volumes no mínimo iguais ao maior volume verificado nos últimos duzentos e cinquenta e dois dias úteis, acrescido de um percentual de segurança, e com replicação de dados do centro de processamento principal; e

IV - procedimentos de emergência, no caso de impedimento simultâneo dos centros de processamento principal e secundário.

Art. 20. O PSTI deve elaborar plano de saída ordenada, contendo medidas a serem implementadas para o encerramento de suas atividades.

Parágrafo único. O plano de que trata o *caput* deve priorizar a mitigação do impacto sobre as instituições financeiras e demais instituições supervisionadas pelo Banco Central do Brasil que utilizam os serviços providos pelo PSTI, bem como sobre o regular funcionamento do Sistema de Pagamentos Brasileiro – SPB.

Art. 21. O PSTI deve implementar e manter política de gestão de crises operacionais para orientar o tratamento de situações atípicas que possam comprometer sua operação, com impactos potenciais para o regular funcionamento do SPB.

Art. 22. A política de gestão de crises operacionais de que trata o art. 21 deve contemplar, no mínimo, as seguintes medidas:

I - definição de papéis e responsabilidades necessários para a gestão de crises operacionais, incluindo a previsão de órgãos de governança e alçadas para a tomada de decisões;

II - definição de critérios objetivos para caracterização de situações de crise e direcionamento da análise de cenários;

III- diretrizes para elaboração, revisão e teste de planos de gestão de crises; e

IV - diretrizes para elaboração, revisão e teste de planos de comunicação.

Art. 23. O PSTI deve estruturar processos e procedimentos para gestão de incidentes operacionais, tecnológicos e de segurança, especificando a integração entre esses processos e o processo de gestão de crises operacionais nas situações em que há agravamento de incidentes, em linha com as práticas observadas na indústria.

Parágrafo único. O PSTI deve implementar plano de resposta a incidentes compatível com o perfil de risco da instituição, testado e atualizado, pelo menos, anualmente, com a definição clara de funções e responsabilidade e dos procedimentos de resposta e recuperação a serem adotados para mitigação dos efeitos dos incidentes operacionais sobre a operação da instituição.

Art. 24. O PSTI deve implementar e manter política de gestão de fraudes para mitigar situações atípicas que possam comprometer o regular funcionamento do SPB.

Art. 25. A política de gestão de fraudes de que trata o art. 24 deve contemplar, no mínimo, as seguintes medidas:

I - estabelecimento de canal para reporte de indícios de fraudes;

II - estabelecimento de mecanismos de prevenção a fraudes, incluindo disponibilização de dados para conciliação de informações, acesso a trilhas de auditoria e definição de limites operacionais;

III - monitoramento em tempo integral, vinte e quatro horas por dia, sete 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) aos valores transacionados;

b) ao volume de transações; e

c) à quantidade de transações por unidade de tempo;

IV - avaliação de atipicidades em etapa anterior ao processo de encaminhamento de uma transação ao Banco Central do Brasil;

V - definição de mecanismos de validação da integridade das transações durante as etapas de processamento;

VI - existência de mecanismo de interrupção do fluxo completo de transações em caso de grave suspeita de comprometimento; e

VII - estabelecimento de canal que possibilite a comunicação tempestiva de indícios de fraude com instituições financeiras e demais instituições supervisionadas pelo Banco Central do Brasil que possam ser impactadas por esses eventos.

Art. 26. O PSTI deve implementar e manter política abrangente de controles internos e conformidade, considerando todos os riscos do negócio, inclusive aqueles decorrentes da terceirização de serviços relevantes, e assegurando a implantação de controles internos efetivos em todas as áreas.

Art. 27. A política de controles internos e conformidade de que trata o art. 26 deve contemplar, no mínimo, os seguintes controles:

I - testes e revisão periódica de controles internos e das medidas de contingência; e

II - mecanismo para garantir a conformidade com os dispositivos desta Resolução e com todos os requisitos técnicos da RSFN previstos no Catálogo de Serviços do SFN, no Manual de Redes do SFN e no Manual de Segurança do SFN publicados pelo Banco Central do Brasil.

Art. 28. O PSTI deve implementar e manter política de auditoria interna que reúna as responsabilidades, a composição e a forma de atuação da auditoria interna, observando, inclusive, as melhores práticas associadas ao tema.

Art. 29. A política de auditoria interna de que trata o art. 28 deve prever, no mínimo, os seguintes aspectos:

I - linha de reporte da auditoria interna ao conselho de administração ou, se inexistente, à diretoria prevista em estatuto ou contrato social;

II - segregação das unidades de negócio e dos órgãos de gestão de riscos, controles internos e conformidade;

III - definição de uma estrutura de auditoria interna compatível com a natureza, porte, complexidade, estrutura e perfil de risco do PSTI;

IV - elaboração de plano anual de auditoria interna, com aprovação pelo conselho de administração ou, se inexistente, pela diretoria prevista em estatuto ou contrato social, baseado na avaliação de riscos de auditoria e contendo, pelo menos, os processos que farão parte do escopo da atividade de auditoria interna, a classificação desses processos por nível de risco e a proposta de alocação dos recursos disponíveis; e

V - possibilidade de contratação de auditoria externa independente, para validar ou complementar a auditoria interna, com compartilhamento dos relatórios com o Banco Central do Brasil e instituições contratantes.

CAPÍTULO IV
DA PRESTAÇÃO DE INFORMAÇÕES AO BANCO CENTRAL DO BRASIL

Art. 30. O PSTI deve prestar ao Banco Central do Brasil as seguintes informações:

I - demonstrações financeiras anuais, auditadas por empresa de auditoria independente registrada na Comissão de Valores Mobiliários;

II - certificação técnica requerida no art. 3º, *caput*, inciso XI sempre que renovada ou atualizada;

III - quaisquer alterações do quadro societário da instituição, na estrutura de controle ou na composição de seus administradores, no prazo de até dez dias contados da ocorrência;

IV - incidentes operacionais ou de segurança da informação que possam comprometer a integridade, a disponibilidade ou a confidencialidade dos serviços prestados, imediatamente após a ciência da ocorrência, acompanhados de relatório no prazo de até dez dias;

V - alterações relevantes da arquitetura de serviços ou do ambiente computacional do PSTI;

VI - início ou encerramento de relacionamento com instituições financeiras e demais instituições supervisionadas pelo Banco Central do Brasil;

VII - início de provimento de outros serviços de processamento de dados;

VIII - informações necessárias para o monitoramento da regular operação do PSTI;

IX - relatórios anuais de auditoria interna e, quando houver, de auditoria externa independente, contemplando os principais achados, os planos de ação e o acompanhamento das correções; e

X - relatório de auditoria externa independente, emitido por empresa registrada na Comissão de Valores Mobiliários, atestando o atendimento integral, pelo PSTI, de todos os procedimentos e requisitos previstos nesta Resolução e nos instrumentos normativos da RSFN, a ser apresentado ao Banco Central do Brasil com periodicidade anual.

CAPÍTULO V
DAS MEDIDAS CAUTELARES

Art. 31. Fica o Banco Central do Brasil autorizado a adotar medida cautelar em relação ao PSTI nas seguintes situações:

I - ocorrência de incidentes operacionais, tecnológicos ou de segurança, incluindo os originados por ataque cibernético ou evento de fraude, os que possam impactar o regular funcionamento do SPB, ou os relacionados a situações em que não há causa-raiz identificada ou comprovação de resolução definitiva do problema;

II - deficiências relevantes de controles que possam trazer implicações para a segurança, a integridade ou a disponibilidade de dados, informações ou sistemas de informação geridos pelo PSTI;

III - descumprimento grave ou reiterado das obrigações de reporte e de transparência previstas nesta Resolução; ou

IV - falhas operacionais que comprometam a integridade, a disponibilidade ou a confiabilidade da RSFN ou dos serviços por ela suportados.

Art. 32. Na ocorrência das hipóteses previstas no art. 31, o Banco Central do Brasil poderá exigir, de forma isolada ou cumulativa, a adoção das seguintes medidas cautelares:

I - observância de limites operacionais mais restritivos, inclusive quanto ao volume de transações processadas, aos valores máximos das transações ou à quantidade de instituições atendidas;

II - suspensão da conexão à RSFN, total ou parcial, até a comprovação da resolução definitiva do problema;

III - suspensão de serviço específico provido pelo PSTI no âmbito da RSFN, total ou parcial, até a comprovação da resolução definitiva do problema;

IV - determinação de reforço imediato em requisitos técnicos de segurança, governança ou continuidade de negócios, com prazos definidos para comprovação;

V - exigência de auditoria independente extraordinária, às expensas do PSTI, para verificar a efetividade das medidas corretivas adotadas;

VI - imposição de plano de ação corretivo, com prazos e metas específicas de cumprimento, a ser acompanhado pelo Banco Central do Brasil;

VII - restrição à contratação de novos clientes ou à ampliação de serviços até a comprovação do saneamento das deficiências identificadas;

VIII - execução total ou parcial do plano de saída ordenada; e

IX - adoção de outras medidas proporcionais e necessárias para resguardar a integridade, a estabilidade e a confiabilidade da RSFN e dos serviços de pagamento por ela suportados.

Parágrafo único. As medidas cautelares de que trata este artigo têm caráter preventivo, não substituindo o procedimento voltado ao descadastramento do PSTI, na forma prevista nesta Resolução.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 33. O PSTI deve adotar como premissa, para o fornecimento de serviços para instituições financeiras e demais instituições supervisionadas pelo Banco Central do Brasil, a manutenção da segurança e do regular funcionamento do SPB.

Parágrafo único. A observância da premissa estabelecida no *caput* deve ser amparada por:

I - utilização de sistemas de informação projetados com mecanismos para garantir a resiliência operacional, a segurança e a integridade das informações, bem como prevenir a ocorrência de fraudes;

II - utilização de ambientes computacionais, incluindo os de contingência, com capacidade adequada para suportar os sistemas de informação e o adequado provimento de serviços às instituições financeiras e às demais instituições supervisionadas pelo Banco Central do Brasil; e

III - estabelecimento de processos de monitoramento e tratamento de eventos que possam impactar o adequado provimento de serviços.

Art. 34. O Banco Central do Brasil promoverá o monitoramento dos serviços prestados pelos PSTI, podendo deles solicitar informações, esclarecimentos ou documentos adicionais considerados necessários ao exercício das atribuições da Autarquia.

Art. 35. Para acessar a RSFN por meio de PSTI, as instituições financeiras e demais instituições supervisionadas pelo Banco Central do Brasil devem contratar serviços de PSTI devidamente credenciado nos termos desta Resolução.

§ 1º Cabe à instituição contratante de que trata o *caput*:

I - assegurar que os contratos celebrados com o PSTI contemplem as obrigações estabelecidas nesta Resolução e as demais normas aplicáveis;

II - monitorar continuamente a adequação do PSTI contratado aos requisitos de governança corporativa, gestão de riscos, segurança cibernética, gestão de fraudes e continuidade de negócios previstos nesta Resolução;

III - implementar controles de segurança estabelecidos pelo PSTI para utilização dos serviços a serem providos;

IV - manter a posse das suas chaves privadas utilizadas para a assinatura das mensagens e validar a integridade das transações previamente à assinatura, assegurando que os dados não tenham sido corrompidos ou manipulados durante o processo de geração da mensagem;

V - não utilizar o mesmo certificado entre ambientes, como homologação e produção, e função, como assinatura de mensagens e estabelecimento de canal do Pix;

VI - manter à disposição do Banco Central do Brasil a documentação relativa à contratação, monitoramento e supervisão do PSTI, inclusive relatórios de auditoria e de testes de continuidade; e

VII - comunicar de imediato ao Banco Central do Brasil quaisquer falhas relevantes ou descumprimentos identificados na atuação do PSTI contratado.

§ 2º A não observância do disposto neste artigo sujeita a instituição contratante de que trata o *caput* às sanções previstas na legislação em vigor.

Art. 36. O Banco Central do Brasil poderá emitir as instruções complementares que sejam necessárias ao cumprimento do disposto nesta Resolução, inclusive no que se refere aos procedimentos para instrução e avaliação dos processos de credenciamento e de descredenciamento, de que tratam os arts. 3º e 7º, respectivamente, e à prestação de informações de que trata o art. 30, entre outros aspectos.

Art. 37. O PSTI em funcionamento na data da entrada em vigor desta Resolução deve promover as adaptações necessárias à adequação ao disposto nos arts. 17 e 25 desta Resolução, nos termos de cronograma a ser publicado pelo Banco Central do Brasil.

§ 1º O cumprimento de cada uma das fases previstas no cronograma de que trata o *caput* deve ser confirmado por relatório de asseguração razoável, emitido por empresa de auditoria externa independente registrada na Comissão de Valores Mobiliários, atestando o atendimento integral, pelo PSTI, aos procedimentos e requisitos previstos na fase correspondente.

§ 2º O atraso no cumprimento dos prazos fixados no cronograma de que trata o *caput* poderá acarretar o estabelecimento, pelo Banco Central do Brasil, de limites operacionais mais restritivos, nos termos do art. 32, *caput*, inciso I, ou o descredenciamento do PSTI, na forma do art. 7º, *caput*, inciso II.

§ 3º O pedido de credenciamento deve ocorrer em até quatro meses após a entrada em vigor desta Resolução.

§ 4º A não apresentação de pedido de credenciamento no prazo de que trata o § 3º acarretará o descredenciamento de ofício do PSTI, que deverá elaborar e implementar plano de saída ordenada.

§ 5º O PSTI que tenha pedido de autorização pendente de análise ou de homologação na data da entrada em vigor desta Resolução deve apresentar ao Banco Central do Brasil pleito de credenciamento, com base nos critérios estabelecidos nesta Resolução, no prazo previsto no § 3º.

§ 6º Até que concluam o período de adaptação de que trata este artigo, o PSTI poderá ficar sujeito a limites operacionais específicos, na forma prevista na legislação em vigor, sem prejuízo do disposto no § 2º.

Art. 38. Ficam revogados os seguintes dispositivos da Circular nº 3.970, de 28 de novembro de 2019, publicada no Diário Oficial da União de 2 de dezembro de 2019:

I - inciso III do *caput* do art. 2º;

II - art. 6º; e

III - inciso III do *caput* do art. 7º.

Art. 39. Esta Resolução entra em vigor na data de sua publicação.

GILNEU FRANCISCO ASTOLFI VIVAN
Diretor de Regulação

RODRIGO ALVES TEIXEIRA
Diretor de Administração

AILTON DE AQUINO SANTOS
Diretor de Fiscalização

DIOGO ABRY GUILLEN
Diretor de Organização do Sistema Financeiro e de Resolução substituto