BANCO CENTRAL DO BRASIL

VOTO 88/2025–CMN, DE 18 DE DEZEMBRO DE 2025

Assuntos de Regulação – Propõe a edição de ato normativo que altera a Resolução CMN nº 4.893, de 26 de fevereiro de 2021, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

Senhores Conselheiros,

A Diretoria Colegiada do Banco Central do Brasil, na 3.621ª sessão, aprovou o incluso Voto 185/2025–BCB, de 3 de dezembro de 2025, em que se propõe a edição de ato normativo que altera a Resolução CMN nº 4.893, de 26 de fevereiro de 2021, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

É o que submeto à consideração dos Senhores.

GABRIEL MURICCA GALÍPOLO
Presidente do Banco Central do Brasil

Anexo: 1.

VOTO DO BC 185/2025-BCB/Dinor-Numerado Manualmente

NUP: 18600.131812/2025-69

Descrição: Assuntos de Regulação - Propõe a edição de ato normativo que altera a Resolução CMN nº 4.893, de 26 de fevereiro de 2021, que dispõe sobre a política de segurança cibernética e sobre os requisitos ...

Assinado/Autenticado por: - GILNEU FRANCISCO ASTOLFI VIVAN:38442523049 em 04/12/2025;

BANCO CENTRAL DO BRASIL

VOTO 185/2025–BCB, DE 3 DE DEZEMBRO DE 2025

Assuntos de Regulação – Propõe a edição de ato normativo que altera a Resolução CMN nº 4.893, de 26 de fevereiro de 2021, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

Senhor Presidente e Senhores Diretores,

1. A Resolução CMN nº 4.893, de 26 de fevereiro de 2021, dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil – BCB.

2. Com a crescente digitalização do Sistema Financeiro Nacional – SFN e do Sistema de Pagamentos Brasileiro – SPB nos últimos anos e com a implantação do Pix, que acrescentou tráfego à Rede do Sistema Financeiro Nacional – RSFN, fez-se necessário aprimorar a regulamentação para conferir maior segurança ao funcionamento dessa infraestrutura de comunicação de dados.

3. Nesse sentido, foi editada a Resolução BCB nº 498, de 5 de setembro de 2025, que estabeleceu requisitos, procedimentos e condições para o Provedor de Serviços de Tecnologia da Informação – PSTI, com o objetivo de assegurar a resiliência operacional da RSFN e dos serviços críticos por ela suportados. A referida Resolução BCB estabeleceu obrigações mais rigorosas para a contratação de PSTI e critérios mais robustos de credenciamento, de governança e de gestão de riscos para esses provedores de serviços.

4. Entretanto, desde a entrada em vigor da supracitada Resolução BCB, verificou-se a existência de assimetria regulatória, uma vez que as instituições que acessam a RSFN por meio de PSTI passaram a sujeitar-se a requisitos específicos e mais ampliados de governança e de gestão de risco cibernético do que aquelas que se conectam à mesma infraestrutura por meio de soluções próprias.

5. Diante desse cenário, proponho a alteração da Resolução CMN nº 4.893, de 2021, com o objetivo de uniformizar o ambiente regulatório e conferir maior segurança e higidez ao SFN e às suas infraestruturas de comunicação de dados e sistemas de pagamentos. Cabe ressaltar que, mesmo com a presente proposta, os temas segurança cibernética e requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem continuarão como objeto de estudos por parte deste Banco Central visando a eficiência e o fortalecimento do SFN e do SPB.

6. Primeiramente, proponho incorporar à Resolução CMN nº 4.893, de 2021, requisitos mínimos adicionais aos procedimentos e aos controles que devem ser adotados pelas instituições em sua política de segurança cibernética para reduzir a vulnerabilidade da instituição, em linha com aqueles previstos na Resolução BCB nº 498, de 2025, entre outros, nos seguintes tópicos:

I - gestão dos certificados digitais;
II - requisitos de segurança para a integração de sistemas de informação por meio de interfaces eletrônicas;
III - ações de inteligência no ambiente cibernético;
IV - mecanismos de rastreabilidade de transações e operações;
V - testes de intrusão e detecção de vulnerabilidades;
VI - controles de acesso;
VII - mecanismos de proteção de rede; e
VIII - implementação de perfis de configuração seguros e aplicação regular de correções.

7. Nesse contexto, com o objetivo de ampliar o alcance dos princípios e dos controles de segurança cibernética ao conjunto mais amplo possível de operações realizadas pelas instituições, proponho esclarecer que os referidos procedimentos e controles propostos também se apliquem no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição. A proposta explicita que os referidos procedimentos e controles sejam aplicados, no que couber, aos sistemas de informação adquiridos pela instituição ou desenvolvidos por empresas prestadoras de serviços a terceiros, quando executados com recursos computacionais da própria instituição. Com isso, busca-se evitar que a terceirização do desenvolvimento de sistemas converta-se em lacuna de controle, reforçando a responsabilidade da instituição pela segurança de todos os recursos tecnológicos por ela empregados.

8. Adicionalmente, com o objetivo de fortalecer a proteção da infraestrutura crítica do SFN e do SPB, proponho a inclusão de requisitos adicionais de segurança, como parte integrante dos procedimentos e controles previstos na política de segurança cibernética das instituições, para a comunicação eletrônica de dados com a RSFN, abrangendo, em especial, os ambientes Pix e o Sistema de Transferência de Reservas – STR. Tais requisitos envolvem, entre outros aspectos, uso de múltiplos fatores de autenticação para acesso administrativo aos ambientes Pix e STR, isolamento físico e lógico desses ambientes dos demais sistemas da instituição, monitoramento de credenciais e de certificados digitais, mecanismos de validação da integridade fim a fim de transações e vedação do acesso de empresas prestadoras de serviços a terceiros às chaves privadas da instituição associadas a certificados digitais. Acrescente-se que a proposta contempla, como requisito para a conexão da instituição como participante de Sistemas do Mercado Financeiro – SMF, a implementação de controles de segurança para a prevenção, detecção e resposta a fraudes, a serem observados pela instituição.

9. Proponho, ainda, acrescentar ao relatório que as instituições devem elaborar anualmente sobre a implementação do plano de ação e de resposta a incidentes os resultados dos testes de intrusão e dos testes, varreduras e análises periódicas para detecção de vulnerabilidades e os planos de ação estabelecidos para as suas correções.

10. Com relação aos testes de intrusão, proponho exigir que as instituições assegurem que os mencionados testes sejam realizados, no mínimo, anualmente, com independência e imparcialidade por pessoa natural ou empresa especializada contratada pela instituição para essa finalidade, sem prejuízo da realização de testes por equipes da própria instituição, e que os resultados da execução desses testes sejam documentados, especialmente as eventuais vulnerabilidades que forem identificadas e os planos de ação estabelecidos para suas correções.

A documentação com os resultados da execução de testes de intrusão e os planos de ação estabelecidos para as correções de vulnerabilidades identificadas devem ficar à disposição deste Banco Central pelo prazo de cinco anos, contado o prazo a partir da data de execução dos testes.

11. Complementarmente, proponho qualificar o serviço prestado para a comunicação eletrônica de dados na RSFN como serviço relevante para fins de contratação de serviços de processamento, armazenamento de dados e computação em nuvem, segundo regras previstas na citada Resolução CMN nº 4.893, de 2021, independentemente da forma de conexão utilizada e incluindo os casos em que o prestador de serviços fornece serviço de processamento de mensagens no âmbito do SFN e do SPB. Com isso, assegura-se que tais serviços estejam sujeitos a padrões mais rigorosos de gestão de riscos, diligências pré-contratuais, cláusulas contratuais mínimas e monitoramento e supervisão pelo BCB, compatíveis com sua relevância sistêmica.

12. Por fim, à competência do Banco Central em poder adotar as medidas necessárias para cumprimento do disposto na regulamentação, proponho acrescentar que esta Autarquia possa estabelecer a especificação dos requisitos de segurança para integração de sistemas de informação por meio de interfaces eletrônicas, devendo observar, em sua regulamentação, os princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, bem como que os requisitos a serem especificados sejam aqueles necessários e adequados para subsidiar a integração dos sistemas, acompanhando as inovações tecnológicas, a fim de manter sua aptidão como um dos procedimentos e controles para implementação da política de segurança cibernética em cenários futuros.

13. Considerando a necessidade de adequação das instituições reguladas às alterações ora propostas na regulamentação, proponho estabelecer prazo até 1º de março de 2026 para que as instituições em funcionamento façam as adaptações necessárias para viabilizar o cumprimento da resolução CMN.

14. Por força do art. 5º da Lei nº 13.874, de 20 de setembro de 2019, as propostas de edição e de alteração de atos normativos de interesse geral de agentes econômicos ou de usuários dos serviços prestados, editadas por órgão ou entidade da administração pública federal, incluídas as autarquias e as fundações públicas, serão precedidas da realização de análise de impacto regulatório – AIR, que conterá informações e dados sobre os possíveis efeitos do ato normativo para verificar a razoabilidade do seu impacto econômico.

15. Por sua vez, o Decreto nº 10.411, de 30 de junho de 2020, que regulamenta a Lei nº 13.874, de 2019, em seu art. 4º, inciso V, alíneas “b” e “c”, estabelece que poderão ser dispensados da AIR, desde que haja decisão fundamentada do órgão ou da entidade competente, os atos normativos que visem a preservar a liquidez, a solvência ou a higidez dos mercados financeiros, de capitais e de câmbio, ou dos sistemas de pagamentos.

16. Desse modo, a realização de AIR não se aplica à resolução CMN ora proposta, por se tratar de ato normativo destinado a preservar a higidez do mercado financeiro, em especial da RSFN e dos sistemas de pagamentos por ela suportados. As alterações propostas visam a reforçar controles de segurança cibernética das instituições financeiras e das demais instituições autorizadas a funcionar pelo Banco Central, padronizar requisitos para acesso à RSFN e reduzir

vulnerabilidades operacionais, contribuindo para a continuidade e para a confiabilidade do SFN e do SPB.

17. Assim, com base no disposto nos arts. 11, inciso IV, alínea “a”, e 20, inciso VI, alíneas “c” e “k”, do Regimento Interno deste Banco Central, trago o assunto à consideração deste colegiado na forma da anexa minuta de resolução CMN, para, após aprovação desta Diretoria Colegiada, ser submetido ao Conselho Monetário Nacional.

GILNEU FRANCISCO ASTOLFI VIVAN
Diretor de Regulação

Anexo: 1.

BANCO CENTRAL DO BRASIL

RESOLUÇÃO CMN Nº , DE DE DE 2025

Altera a Resolução CMN nº 4.893, de 26 de fevereiro de 2021, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

O Banco Central do Brasil, na forma do art. 9º da Lei nº 4.595, de 31 de dezembro de 1964, torna público que o Conselho Monetário Nacional, em sessão realizada em de de 2025, com base nos arts. 4º, *caput*, inciso VIII, da referida Lei, 7º e 23, *caput*, alínea "a", da Lei nº 6.099, de 12 de setembro de 1974, 1º, *caput*, inciso II, da Lei nº 10.194, de 14 de fevereiro de 2001, e 1º, § 1º, da Lei Complementar nº 130, de 17 de abril de 2009,

R E S O L V E U :

Art. 1º A Resolução CMN nº 4.893, de 26 de fevereiro de 2021, publicada no Diário Oficial da União de 1º de março de 2021, passa a vigorar com as seguintes alterações:

"Art. 3º .....

.....

§ 2º Os procedimentos e os controles de que trata o inciso II do *caput* devem abranger, no mínimo:

I - a autenticação;

II - os mecanismos de criptografia;

III - os mecanismos de prevenção e detecção de intrusão;

IV - os mecanismos de prevenção de vazamentos de informações;

V - os mecanismos de proteção contra *softwares* maliciosos;

VI - os mecanismos de rastreabilidade;

VII - a gestão de cópias de segurança dos dados e das informações;

VIII - a avaliação e a correção de vulnerabilidades dos recursos computacionais e dos sistemas de informação;

IX - os controles de acesso;

X - a definição e implementação de perfis de configuração segura de ativos de tecnologia;

XI - os mecanismos de proteção da rede;

XII - a gestão de certificados digitais;

XIII - os requisitos de segurança para a integração de sistemas de informação por meio de interfaces eletrônicas; e

XIV - as ações de inteligência no ambiente cibernético, incluindo o monitoramento de informações de interesse da instituição na internet, na *Deep Web* e na *Dark Web*, além de grupos privados de comunicação.

§ 3º Os procedimentos e os controles citados no inciso II do *caput* devem ser aplicados, inclusive:

I - no desenvolvimento de sistemas de informação seguros; e

II - na adoção de novas tecnologias empregadas nas atividades da instituição.

.....

§ 6º A instituição deve verificar o disposto no inciso I do § 3º, no que couber, nos casos de sistemas de informação por ela adquiridos ou desenvolvidos por empresas prestadoras de serviços a terceiros, executados com a utilização de recursos computacionais da própria instituição.

§ 7º Os mecanismos de rastreabilidade de que trata o inciso VI do § 2º devem abranger a rastreabilidade de transações e operações, contemplando, 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 comportamentos atípicos, bem como subsidiar análises;

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

III - retenção segura das trilhas de auditoria.

§ 8º A avaliação e a correção de vulnerabilidades de que trata o inciso VIII do § 2º deve contemplar, no mínimo:

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

II - varreduras periódicas dos recursos tecnológicos com o objetivo de identificar dispositivos indevidamente conectados à rede corporativa que possam estabelecer conexão com ativos de tecnologia externos à instituição;

III - análises periódicas dos recursos tecnológicos com o objetivo de identificar vulnerabilidades que possam comprometer a segurança dos ativos de tecnologia da instituição;

IV - testes de intrusão; e

V - correção tempestiva das vulnerabilidades identificadas.

§ 9º Os controles de acesso de que trata o inciso IX do § 2º devem incluir, no mínimo:

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

II - revisão periódica e tempestiva das permissões de acesso, em especial de colaboradores terceirizados com acesso aos recursos computacionais da instituição; e

III - implementação de múltiplos fatores de autenticação para acesso à rede corporativa a partir de ambientes externos à instituição.

§ 10. A definição e implementação de perfis de configuração segura de que trata o inciso X do § 2º devem prever, no mínimo:

I - a gestão do ciclo de vida dos recursos computacionais da instituição;

II - a aplicação regular de correções de segurança;

III - a configuração adequada dos serviços a serem suportados pelos recursos computacionais; e

IV - a alteração de senhas e de outros padrões que possam ser utilizados para acessos indevidos aos recursos computacionais.

§ 11. Os mecanismos de proteção da rede de que trata o inciso XI do § 2º devem contemplar, no mínimo:

I - a segmentação de rede de computadores, resguardando, em especial, o ambiente de produção e os recursos computacionais que suportam processos críticos de negócio;

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

III - a definição de critérios para o estabelecimento e o monitoramento de conexões com ambientes externos, em especial em horário noturno e em dias não úteis;

IV - as medidas para identificar e prevenir conexões indevidas com ambientes externos à instituição oriundas de recursos tecnológicos da instituição;

V - a implementação e manutenção de processos e ferramentas para identificação, análise, tratamento e controle de eventos atípicos no ambiente de produção da instituição, abrangendo, como exemplos, o estabelecimento de *virtual private networks* – VPN e tentativas de acesso privilegiado a recursos computacionais, especialmente em horário noturno e em dias não úteis; e

VI - o estabelecimento de medidas para restringir o acesso a redes corporativas apenas a dispositivos ou ativos de tecnologia devidamente autorizados.

§ 12. A gestão de certificados digitais de que trata o inciso XII do § 2º deve prever, no mínimo:

I - o monitoramento do uso de certificados e assinaturas digitais, contemplando a implementação dos mecanismos de rastreabilidade de que trata o § 7º;

II - os procedimentos para a guarda de informações, abrangendo os controles de acesso físico e lógico a chaves privadas sob responsabilidade da instituição;

III - procedimentos e ferramentas para evitar o compartilhamento indevido das chaves privadas associadas a certificados digitais da instituição; e

IV - a validação tempestiva de certificados revogados perante as autoridades certificadoras." (NR)

"Art. 3º-A As instituições referidas no art. 1º devem estabelecer os seguintes requisitos de segurança adicionais, como parte integrante dos procedimentos e controles previstos em sua política de segurança cibernética de que trata o art. 3º:

I - no caso de comunicação eletrônica de dados na Rede do Sistema Financeiro Nacional – RSFN:

a) uso de múltiplos fatores de autenticação para o acesso administrativo aos ambientes Pix e Sistema de Transferência de Reservas – STR;

b) isolamento físico e lógico do ambiente Pix dos demais sistemas da instituição, mantendo instância dedicada e apartada dos demais ambientes nos casos de uso de serviços de computação em nuvem contratados;

c) isolamento físico e lógico do ambiente STR dos demais sistemas da instituição, mantendo instância dedicada e apartada dos demais ambientes nos casos de uso de serviços de computação em nuvem contratados;

d) monitoramento do uso de credenciais e certificados digitais, bem como estabelecimento de controles para a guarda dessas informações, especialmente as utilizadas no âmbito do Sistema de Pagamentos Instantâneos – SPI;

e) implementação de mecanismos de validação da integridade fim a fim das transações pela instituição antes da assinatura digital das mensagens associadas, assegurando que os dados não tenham sido corrompidos ou manipulados durante o processo de geração dessas mensagens; e

f) vedação do acesso de empresas prestadoras de serviços a terceiros às chaves privadas associadas a certificados digitais utilizados pela instituição para a assinatura de mensagens; e

II - no caso de conexão como participante de Sistemas do Mercado Financeiro – SMF autorizados a operar, a implementação de controles de segurança para prevenção, detecção e resposta a fraudes, a serem observados pela instituição.

Parágrafo único. As instituições devem observar este artigo de forma compatível com o disposto:

I - nesta Resolução;

II - na regulamentação em vigor; e

III - em 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." (NR)

"Art. 8º .....

§ 1º .....

.....

III - os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;

IV - os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes; e

V - os resultados dos testes de intrusão e dos testes, varreduras e análises periódicas para detecção de vulnerabilidades de que trata o art. 3º, § 8º, e os planos de ação estabelecidos para as suas correções, observado o disposto no art. 22-A, *caput*, inciso III.

....." (NR)

"Art. 22-A. As instituições devem assegurar que os testes de intrusão mencionados no art. 3º, § 8º, inciso IV, devem:

I - ter periodicidade mínima anual;

II - ser realizados com independência e imparcialidade por pessoa natural ou empresa especializada contratada pela instituição para essa finalidade, sem prejuízo da realização de testes por equipes da própria instituição; e

III - ter os resultados de sua execução documentados, especialmente as eventuais vulnerabilidades que forem identificadas e os planos de ação estabelecidos para suas correções." (NR)

"Art. 22-B. O serviço prestado para a comunicação eletrônica de dados na RSFN, de que trata o art. 3º-A, *caput,* inciso I, é considerado relevante para fins da aplicação do disposto nesta Resolução sobre a contratação de serviços de processamento, armazenamento de dados e computação em nuvem.

§ 1º Aplica-se o disposto no *caput* independente da forma de conexão com a RSFN.

§ 2º O serviço de que trata o *caput* inclui os casos em que o prestador de serviços fornece serviço de processamento de mensagens no âmbito do SFN e do Sistema de Pagamentos Brasileiro – SPB." (NR)

"Art. 23. .....

.....

VIII - os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle de que trata o art. 21, contado o prazo referido no *caput* a partir da implementação dos citados mecanismos;

IX - a documentação com os critérios que configurem uma situação de crise de que trata o art. 20, parágrafo único; e

X - a documentação com os resultados da execução de testes de intrusão e os planos de ação estabelecidos para as correções de vulnerabilidades identificadas de que trata o art. 22-A, *caput*, inciso III, contado o prazo a partir da data de execução dos testes." (NR)

"Art. 24. .....

.....

III - os prazos máximos de que trata o art. 20, *caput*, inciso II, para reinício ou normalização das atividades ou dos serviços relevantes interrompidos;

IV - a especificação dos requisitos de segurança para integração de sistemas de informação por meio de interfaces eletrônicas, de que trata o art. 3º, § 2º, inciso XIII; e

V - os requisitos técnicos e procedimentos operacionais a serem observados pelas instituições para o cumprimento desta Resolução.

§ 1º Na regulamentação de que trata o *caput*, o Banco Central do Brasil deverá observar os princípios e diretrizes referidos no art. 2º, *caput*.

§ 2º Na regulamentação de que trata o inciso IV do *caput*, o Banco Central do Brasil deverá observar, também, as seguintes diretrizes gerais:

I - os requisitos a serem especificados serão aqueles necessários e adequados para subsidiar a integração dos sistemas referida no art. 3º, § 2º, inciso XIII; e

II - o conteúdo dispondo sobre os requisitos deverá acompanhar as inovações tecnológicas, a fim de manter sua aptidão como um dos procedimentos e controles para implementação da política de segurança cibernética em cenários futuros." (NR)

Art. 2º As instituições em funcionamento na data da entrada em vigor desta Resolução devem promover as adaptações necessárias à adequação ao disposto nesta Resolução até 1º de março de 2026.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

GABRIEL MURICCA GALÍPOLO
Presidente do Banco Central do Brasil