ESOLUÇÃO BCB Nº 85, DE 8 DE ABRIL 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 de pagamento autorizadas a funcionar pelo Banco Central do Brasil.~~

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 de pagamento, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

A Diretoria Colegiada do Banco Central do Brasil, em sessão realizada em 8 de abril de 2021, com base nos arts. 9º, 10 e 15 da Lei nº 12.865, de 9 de outubro de 2013, e tendo em vista o art. 14 da Resolução nº 4.282, de 4 de novembro de 2013,

R E S O L V E :

CAPÍTULO I
DO OBJETO E DO ÂMBITO DE APLICAÇÃO

~~Art. 1º Esta Resolução 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 de pagamento autorizadas a funcionar pelo Banco Central do Brasil.~~

Art. 1º Esta Resolução 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 de pagamento, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

CAPÍTULO II
DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Seção I
Da Implementação da Política de Segurança Cibernética

~~Art. 2º As instituições de pagamento devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.~~

Art. 2º As instituições mencionadas no art. 1º devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

§ 1º A política mencionada no caput deve ser compatível com:

I - o porte, o perfil de risco e o modelo de negócio da instituição;

II - a natureza das atividades da instituição e a complexidade dos produtos e serviços oferecidos; e

III - a sensibilidade dos dados e das informações sob responsabilidade da instituição.

~~§ 2º As instituições de pagamento integrantes de conglomerado prudencial podem adotar política de segurança cibernética única do conglomerado prudencial, nos termos da regulamentação em vigor, desde que compatível com o disposto neste Capítulo.~~

§ 2º As instituições integrantes de conglomerado prudencial podem adotar política de segurança cibernética única do conglomerado prudencial, nos termos da regulamentação em vigor, desde que compatível

com o disposto neste Capítulo. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~§ 3º As instituições de pagamento que não constituírem política de segurança cibernética própria em decorrência do disposto no § 2º devem formalizar a opção por essa faculdade em reunião do conselho de administração ou, na sua inexistência, da diretoria da instituição.~~

§ 3º As instituições que não constituírem política de segurança cibernética própria em decorrência do disposto no § 2º devem formalizar a opção por essa faculdade em reunião do conselho de administração ou, na sua inexistência, da diretoria da instituição. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

Art. 3º A política de segurança cibernética deve especificar, no mínimo:

~~I - os objetivos de segurança cibernética da instituição de pagamento;~~

I - os objetivos de segurança cibernética da instituição; (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~II - os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição de pagamento a incidentes e atender aos demais objetivos de segurança cibernética;~~

II - os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética; (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

III - os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;

~~IV - o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição de pagamento;~~

IV - o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição; (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

V - as diretrizes para:

~~a) a elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados;~~

a) a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios; (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~b) a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição de pagamento;~~

b) a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição; (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

c) a classificação dos dados e das informações quanto à relevância; e

d) a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes;

~~VI - os mecanismos para disseminação da cultura de segurança cibernética na instituição de pagamento, incluindo:~~

VI - os mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo: (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

a) a implementação de programas de capacitação e de avaliação periódica de pessoal;

~~b) a prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos; e~~

b) a prestação de informações a clientes e a usuários finais sobre precauções na utilização de produtos e serviços oferecidos; e (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

c) o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética; e

~~VII - as iniciativas para compartilhamento de informações sobre os incidentes relevantes, mencionados no inciso IV, com as instituições de~~

~~pagamento e com as demais instituições autorizadas a funcionar pelo Banco Central do Brasil.~~

VII - as iniciativas para compartilhamento de informações sobre os incidentes relevantes, mencionados no inciso IV, com as instituições mencionadas no art. 1º e com as demais instituições autorizadas a funcionar pelo Banco Central do Brasil. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~§ 1º Na definição dos objetivos de segurança cibernética referidos no inciso I do caput, deve ser contemplada a capacidade da instituição de pagamento para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.~~

§ 1º Na definição dos objetivos de segurança cibernética referidos no inciso I do caput, deve ser contemplada a capacidade de a instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~§ 2º Os procedimentos e os controles de que trata o inciso II do caput devem abranger a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.~~

§ 2º Os procedimentos e os controles de que trata o inciso II do *caput* devem abranger, no mínimo: (Redação dada pela Resolução BCB nº 538, de 18/12/2025.)

I - a autenticação; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

II - os mecanismos de criptografia; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

III - os mecanismos de prevenção e detecção de intrusão; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

IV - os mecanismos de prevenção de vazamentos de informações; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

V - os mecanismos de proteção contra *softwares* maliciosos; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

VI - os mecanismos de rastreabilidade; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

VII - a gestão de cópias de segurança dos dados e das informações; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

VIII - a avaliação e a correção de vulnerabilidades dos recursos computacionais e dos sistemas de informação; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

IX - os controles de acesso; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

X - a definição e implementação de perfis de configuração segura de ativos de tecnologia; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

XI - os mecanismos de proteção da rede; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

XII - a gestão de certificados digitais; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

XIII - os requisitos de segurança para a integração de sistemas de informação por meio de interfaces eletrônicas; e (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

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. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

~~§ 3º Os procedimentos e os controles citados no inciso II do *caput* devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição de pagamento.~~

~~§ 3º Os procedimentos e os controles citados no inciso II do *caput* devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)~~

§ 3º Os procedimentos e os controles citados no inciso II do *caput* devem ser aplicados, inclusive: (Redação dada pela Resolução BCB nº 538, de 18/12/2025.)

I - no desenvolvimento de sistemas de informação seguros; e (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

II - na adoção de novas tecnologias empregadas nas atividades da instituição. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

§ 4º O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes, citados no inciso IV do caput, devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

~~§ 5º As diretrizes de que trata a alínea "b" do inciso V do caput devem contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela própria instituição de pagamento.~~

§ 5º As diretrizes de que trata a alínea “b” do inciso V do caput devem contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela própria instituição. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

§ 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. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

§ 7º Os mecanismos de rastreabilidade de que trata o inciso VI do § 2º devem abranger a rastreabilidade de transações e operações, contemplando, no mínimo: (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

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; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

II - definição de tempo de retenção de informações de acordo com o tipo de processamento realizado; e (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

III - retenção segura das trilhas de auditoria. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

§ 8º A avaliação e a correção de vulnerabilidades de que trata o inciso VIII do § 2º deve contemplar, no mínimo: (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

I - testes e análises periódicos para detecção de vulnerabilidades em sistemas de informação; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

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; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

III - análises periódicas dos recursos tecnológicos com o objetivo de identificar vulnerabilidades que possam comprometer a segurança dos ativos de tecnologia da instituição; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

IV - testes de intrusão; e (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

V - correção tempestiva das vulnerabilidades identificadas. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

§ 9º Os controles de acesso de que trata o inciso IX do § 2º devem incluir, no mínimo: (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

I - mecanismos para limitar o acesso à rede corporativa a usuários credenciados e a dispositivos autorizados; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

II - revisão periódica e tempestiva das permissões de acesso, em especial de colaboradores terceirizados com acesso aos recursos computacionais da instituição; e (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

III - implementação de múltiplos fatores de autenticação para acesso à rede corporativa a partir de ambientes externos à instituição. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

§ 10. A definição e implementação de perfis de configuração segura de que trata o inciso X do § 2º devem prever, no mínimo: (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

I - a gestão do ciclo de vida dos recursos computacionais da instituição; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

II - a aplicação regular de correções de segurança; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

III - a configuração adequada dos serviços a serem suportados pelos recursos computacionais; e (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

IV - a alteração de senhas e de outros padrões que possam ser utilizados para acessos indevidos aos recursos computacionais. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

§ 11. Os mecanismos de proteção da rede de que trata o inciso XI do § 2º devem contemplar, no mínimo: (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

I - a segmentação de rede de computadores, resguardando, em especial, o ambiente de produção e os recursos computacionais que suportam processos críticos de negócio; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

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; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

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; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

IV - as medidas para identificar e prevenir conexões indevidas com ambientes externos à instituição oriundas de recursos tecnológicos da instituição; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

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 (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

VI - o estabelecimento de medidas para restringir o acesso a redes corporativas apenas a dispositivos ou ativos de tecnologia devidamente autorizados. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

§ 12. A gestão de certificados digitais de que trata o inciso XII do § 2º deve prever, no mínimo: (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

I - o monitoramento do uso de certificados e assinaturas digitais, contemplando a implementação dos mecanismos de rastreabilidade de que trata o § 7º; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

II - os procedimentos para a guarda de informações, abrangendo os controles de acesso físico e lógico a chaves privadas sob responsabilidade da instituição; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

III - procedimentos e ferramentas para evitar o compartilhamento indevido das chaves privadas associadas a certificados digitais da instituição; e (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

IV - a validação tempestiva de certificados revogados perante as autoridades certificadoras. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

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: (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

I - no caso de comunicação eletrônica de dados na Rede do Sistema Financeiro Nacional – RSFN: (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

a) uso de múltiplos fatores de autenticação para o acesso administrativo aos ambientes Pix e Sistema de Transferência de Reservas – STR; (Incluída pela Resolução BCB nº 538, de 18/12/2025.)

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; (Incluída pela Resolução BCB nº 538, de 18/12/2025.)

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; (Incluída pela Resolução BCB nº 538, de 18/12/2025.)

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; (Incluída pela Resolução BCB nº 538, de 18/12/2025.)

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 (Incluída pela Resolução BCB nº 538, de 18/12/2025.)

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 (Incluída pela Resolução BCB nº 538, de 18/12/2025.)

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. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

Parágrafo único. As instituições devem observar este artigo de forma compatível com o disposto: (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

I - nesta Resolução; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

II - na regulamentação em vigor; e (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

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. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

Seção II
Da Divulgação da Política de Segurança Cibernética

~~Art. 4º A política de segurança cibernética deve ser divulgada aos funcionários da instituição de pagamento e às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações.~~

Art. 4º A política de segurança cibernética deve ser divulgada aos funcionários da instituição mencionada no art. 1º e às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com

a sensibilidade das informações. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~Art. 5º As instituições de pagamento devem divulgar ao público resumo contendo as linhas gerais da política de segurança cibernética.~~

Art. 5º As instituições mencionadas no art. 1º devem divulgar ao público resumo contendo as linhas gerais da política de segurança cibernética. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

Seção III

Do Plano de Ação e de Resposta a Incidentes

~~Art. 6º As instituições de pagamento devem estabelecer plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética.~~

Art. 6º As instituições mencionadas no art. 1º devem estabelecer plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

Parágrafo único. O plano mencionado no caput deve abranger, no mínimo:

I - as ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

II - as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e

III - a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

~~Art. 7º As instituições de pagamento devem designar diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes.~~

Art. 7º As instituições mencionadas no art. 1º devem designar diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

Parágrafo único. O diretor mencionado no caput pode desempenhar outras funções na instituição, desde que não haja conflito de interesses.

~~Art. 8º As instituições de pagamento devem elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, mencionado no art. 6º, com data-base de 31 de dezembro.~~

Art. 8º As instituições mencionadas no art. 1º devem elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, mencionado no art. 6º, com data-base de 31 de dezembro. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

§ 1º O relatório de que trata o caput deve abordar, no mínimo:

I - a efetividade da implementação das ações descritas no art. 6º, parágrafo único, inciso I;

II - o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes descritos no art. 6º, parágrafo único, inciso II;

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

III - os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; (Redação dada pela Resolução BCB nº 538, de 18/12/2025.)

~~IV - os resultados dos testes de continuidade dos serviços de pagamento prestados, considerando cenários de indisponibilidade ocasionada por incidentes.~~

~~IV - os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)~~

IV - os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes; e (Redação dada pela Resolução BCB nº 538, de 18/12/2025.)

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. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

~~§ 2º O relatório mencionado no caput deve ser apresentado ao conselho de administração ou, na sua inexistência, à diretoria da instituição até 31 de março do ano seguinte ao da data-base.~~

§ 2º O relatório mencionado no caput deve ser: (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

I - submetido ao comitê de risco, quando existente; e (Incluído, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

II - apresentado ao conselho de administração ou, na sua inexistência, à diretoria da instituição até 31 de março do ano seguinte ao da data-base. (Incluído, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~Art. 9º A política de segurança cibernética referida no art. 2º e o plano de ação e de resposta a incidentes mencionado no art. 6º devem ser aprovados pelo conselho de administração ou, na sua inexistência, pela diretoria da instituição de pagamento.~~

Art. 9º A política de segurança cibernética referida no art. 2º e o plano de ação e de resposta a incidentes mencionado no art. 6º devem ser aprovados pelo conselho de administração ou, na sua inexistência, pela diretoria da instituição mencionada no art. 1º. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

Art. 10. A política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser documentados e revisados, no mínimo, anualmente.

CAPÍTULO III
DA CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

~~Art. 11. As instituições de pagamento devem assegurar que suas políticas, estratégias e estruturas para gerenciamento de riscos previstas na regulamentação em vigor, especificamente no tocante aos critérios de decisão quanto à terceirização de serviços, contemplem a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no País ou no exterior.~~

Art. 11. As instituições mencionadas no art. 1º devem assegurar que suas políticas, estratégias e estruturas para gerenciamento de riscos

previstas na regulamentação em vigor, especificamente no tocante aos critérios de decisão quanto à terceirização de serviços, contemplem a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~Art. 12. As instituições de pagamento, previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, devem adotar procedimentos que contemplem:~~

Art. 12. As instituições mencionadas no art. 1º, previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, devem adotar procedimentos que contemplem: (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

I - a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e

II - a verificação da capacidade do potencial prestador de serviço de assegurar:

a) o cumprimento da legislação e da regulamentação em vigor;

b) o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

c) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

d) a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

e) o acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

f) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

~~g) a identificação e a segregação dos dados dos usuários finais da instituição por meio de controles físicos ou lógicos; e~~

g) a identificação e a segregação dos dados dos clientes e dos usuários finais da instituição por meio de controles físicos ou lógicos; e

(Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~h) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da instituição.~~

h) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes e dos usuários finais da instituição. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

§ 1º Na avaliação da relevância do serviço a ser contratado, mencionada no inciso I do caput, a instituição contratante deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado, levando em conta, inclusive, a classificação realizada nos termos do art. 3º, inciso V, alínea "c".

§ 2º Os procedimentos de que trata o caput, inclusive as informações relativas à verificação mencionada no inciso II, devem ser documentados.

§ 3º No caso da execução de aplicativos por meio da internet, referidos no art. 13, inciso III, a instituição deve assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

§ 4º A instituição deve possuir recursos e competências necessários para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso de recursos providos nos termos da alínea "f" do inciso II do caput.

~~Art. 13. Para os fins do disposto nesta Resolução, os serviços de computação em nuvem abrangem a disponibilidade à instituição de pagamento contratante, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:~~

Art. 13. Para os fins do disposto nesta Resolução, os serviços de computação em nuvem abrangem a disponibilidade à instituição contratante, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços: (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

I - processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou executar softwares, que podem incluir

sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;

II - implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou

III - execução, por meio da internet, de aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

~~Art. 14. A instituição de pagamento contratante dos serviços mencionados no art. 12 é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.~~

Art. 14. A instituição contratante dos serviços mencionados no art. 12 é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~Art. 15. A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pelas instituições de pagamento ao Banco Central do Brasil.~~

Art. 15. A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pelas instituições mencionadas no art. 1º ao Banco Central do Brasil. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

§ 1º A comunicação mencionada no caput deve conter as seguintes informações:

I - a denominação da empresa contratada;

II - os serviços relevantes contratados; e

III - a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, definida nos termos do inciso III do art. 16, no caso de contratação no exterior.

§ 2º A comunicação de que trata o caput deve ser realizada até dez dias após a contratação dos serviços.

§ 3º As alterações contratuais que impliquem modificação das informações de que trata o § 1º devem ser comunicadas ao Banco Central do Brasil até dez dias após a alteração contratual.

Art. 16. A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior deve observar os seguintes requisitos:

I - a existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;

~~II - a instituição de pagamento contratante deve assegurar que a prestação dos serviços referidos no caput não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;~~

II - a instituição contratante deve assegurar que a prestação dos serviços referidos no caput não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil; (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~III - a instituição de pagamento contratante deve definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e~~

III - a instituição contratante deve definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~IV - a instituição de pagamento contratante deve prever alternativas para a continuidade dos serviços de pagamento prestados, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.~~

IV - a instituição contratante deve prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~§ 1º No caso de inexistência de convênio nos termos do inciso I do caput, a instituição de pagamento contratante deverá solicitar autorização do Banco Central do Brasil para:~~

§ 1º No caso de inexistência de convênio nos termos do inciso I do caput, a instituição contratante deverá solicitar autorização do Banco Central do Brasil para: (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

I - a contratação do serviço, no prazo mínimo de sessenta dias antes da contratação, observado o disposto no art. 15, § 1º; e

II - as alterações contratuais que impliquem modificação das informações de que trata o art. 15, § 1º, observando o prazo mínimo de sessenta dias antes da alteração contratual.

~~§ 2º Para atendimento aos incisos II e III do caput, as instituições deverão assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso das instituições de pagamento contratantes e do Banco Central do Brasil aos dados e às informações.~~

§ 2º Para atendimento aos incisos II e III do caput, as instituições deverão assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso das instituições contratantes e do Banco Central do Brasil aos dados e às informações. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

§ 3º A comprovação do atendimento aos requisitos de que tratam os incisos I a IV do caput e o cumprimento da exigência de que trata o § 2º devem ser documentados.

Art. 17. Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem conter cláusulas dispondo sobre:

I - a indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

II - a adoção de medidas de segurança para a transmissão e armazenamento dos dados citados no inciso I;

~~III - a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos usuários finais;~~

III - a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes e dos usuários finais; (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

IV - a obrigatoriedade, em caso de extinção do contrato, de:

~~a) transferência dos dados citados no inciso I ao novo prestador de serviços ou à instituição de pagamento contratante; e~~

a) transferência dos dados citados no inciso I ao novo prestador de serviços ou à instituição contratante; e (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

b) exclusão dos dados citados no inciso I pela empresa contratada substituída, após a transferência dos dados prevista na alínea "a" e a confirmação da integridade e da disponibilidade dos dados recebidos;

~~V - o acesso da instituição de pagamento contratante a:~~

V - o acesso da instituição contratante a: (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

a) informações fornecidas pela empresa contratada, visando a verificar o cumprimento do disposto nos incisos I a III;

b) informações relativas às certificações e aos relatórios de auditoria especializada, citados no art. 12, inciso II, alíneas "d" e "e"; e

c) informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados, citados no art. 12, inciso II, alínea "f";

~~VI - a obrigação de a empresa contratada notificar a instituição de pagamento contratante sobre a subcontratação de serviços relevantes para a instituição;~~

VI - a obrigação de a empresa contratada notificar a instituição contratante sobre a subcontratação de serviços relevantes para a instituição; (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

VII - a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;

~~VIII - a adoção de medidas pela instituição de pagamento contratante, em decorrência de determinação do Banco Central do Brasil; e~~

VIII - a adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil; e (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~IX - a obrigação de a empresa contratada manter a instituição de pagamento contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.~~

IX - a obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~Parágrafo único. Os contratos mencionados no caput devem prever, para o caso da decretação de regime de resolução da instituição de pagamento contratante pelo Banco Central do Brasil:~~

Parágrafo único. Os contratos mencionados no caput devem prever, para o caso da decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil: (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

I - a obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso, citados no inciso VII do caput, que estejam em poder da empresa contratada; e

II - a obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

a) a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e

~~b) a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da instituição de pagamento contratante.~~

b) a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da instituição contratante. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

Art. 18. O disposto nos arts. 11 a 17 não se aplica à contratação de sistemas operados por câmaras, por prestadores de serviços de compensação e de liquidação ou por entidades que exerçam atividades de registro ou de depósito centralizado.

CAPÍTULO IV
DISPOSIÇÕES GERAIS

~~Art. 19. As instituições de pagamento devem assegurar que suas políticas previstas na estrutura de gerenciamento de riscos, nos termos da regulamentação em vigor, disponham, no tocante à continuidade dos serviços de pagamento prestados, sobre:~~

Art. 19. As instituições mencionadas no art. 1º devem assegurar que suas políticas previstas na estrutura de gerenciamento de riscos, nos termos da regulamentação em vigor, disponham, no tocante à continuidade dos negócios, sobre: (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

I - o tratamento dos incidentes relevantes relacionados com o ambiente cibernético de que trata o art. 3º, inciso IV;

II - os procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da instituição; e

~~III - os cenários de incidentes considerados nos testes de continuidade de serviços de pagamento prestados de que trata o art. 3º, inciso V, alínea "a".~~

III - os cenários de incidentes considerados nos testes de continuidade de negócios de que trata o art. 3º, inciso V, alínea "a". (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~Art. 20. Os procedimentos adotados pelas instituições de pagamento para gerenciamento de riscos previstos na regulamentação em vigor devem especificar, no tocante à continuidade dos serviços de pagamento prestados:~~

Art. 20. Os procedimentos adotados pelas instituições mencionadas no art. 1º para gerenciamento de riscos previstos na regulamentação em vigor devem especificar, no tocante à continuidade dos negócios: (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

I - o tratamento previsto para mitigar os efeitos dos incidentes relevantes de que trata o art. 3º, inciso IV, e da interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados;

II - o prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos, citados no inciso I; e

~~III – a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, citados no inciso I, que configurem situação de crise pela instituição de pagamento, bem como das providências para o reinício das suas atividades.~~

III - a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, citados no inciso I, que configurem situação de crise pela instituição mencionada no art. 1º, bem como das providências para o reinício das suas atividades. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~Parágrafo único. As instituições de pagamento devem estabelecer e documentar os critérios que configurem a situação de crise de que trata o inciso III do caput.~~

Parágrafo único. As instituições mencionadas no art. 1º devem estabelecer e documentar os critérios que configurem a situação de crise de que trata o inciso III do caput. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

~~Art. 21. As instituições de pagamento devem instituir mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade da política de segurança cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de~~

~~serviços de processamento e armazenamento de dados e de computação em nuvem, incluindo:~~

Art. 21. As instituições mencionadas no art. 1º devem instituir mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade da política de segurança cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, incluindo: (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

I - a definição de processos, testes e trilhas de auditoria;

II - a definição de métricas e indicadores adequados; e

III - a identificação e a correção de eventuais deficiências.

§ 1º As notificações recebidas sobre a subcontratação de serviços relevantes descritas no art. 17, inciso VI, devem ser consideradas na definição dos mecanismos de que trata o caput.

§ 2º Os mecanismos de que trata o caput devem ser submetidos a testes periódicos pela auditoria interna compatíveis com os controles internos da instituição.

~~Art. 22. Sem prejuízo do dever de sigilo e da livre concorrência, as instituições de pagamento devem desenvolver iniciativas para o compartilhamento de informações sobre os incidentes relevantes de que trata o art. 3º, inciso IV.~~

Art. 22. Sem prejuízo do dever de sigilo e da livre concorrência, as instituições mencionadas no art. 1º devem desenvolver iniciativas para o compartilhamento de informações sobre os incidentes relevantes de que trata o art. 3º, inciso IV. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

§ 1º O compartilhamento de que trata o caput deve abranger informações sobre incidentes relevantes recebidas de empresas prestadoras de serviços a terceiros.

§ 2º As informações compartilhadas devem estar disponíveis ao Banco Central do Brasil.

Art. 22-A. As instituições devem assegurar que os testes de intrusão mencionados no art. 3º, § 8º, inciso IV, devem: (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

I - ter periodicidade mínima anual; (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

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 (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

III - ter os resultados de sua execução documentados, especialmente as eventuais vulnerabilidades que forem identificadas e os planos de ação estabelecidos para suas correções. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

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. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

§ 1º Aplica-se o disposto no *caput* independente da forma de conexão com a RSFN. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

§ 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. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 23. Devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

I - o documento relativo à política de segurança cibernética, de que trata o art. 2º;

II - a ata de reunião do conselho de administração ou, na sua inexistência, da diretoria da instituição, no caso de ser formalizada a opção de que trata o art. 2º, § 2º;

III - o documento relativo ao plano de ação e de resposta a incidentes, de que trata o art. 6º;

IV - o relatório anual, de que trata o art. 8º;

V - a documentação sobre os procedimentos de que trata o art. 12, § 2º;

VI - a documentação de que trata o art. 16, § 3º, no caso de serviços prestados no exterior;

VII - os contratos de que trata o art. 17, contado o prazo referido no caput a partir da extinção do contrato;

~~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; e~~

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 a partir da implementação dos citados mecanismos; (Redação dada pela Resolução BCB nº 538, de 18/12/2025.)

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

IX - a documentação com os critérios que configurem uma situação de crise de que trata o art. 20, parágrafo único; e (Redação dada pela Resolução BCB nº 538, de 18/12/2025.)

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. (Incluído pela Resolução BCB nº 538, de 18/12/2025.)

~~Art. 24. As instituições de pagamento que em 1º de setembro de 2019 já tinham contratado a prestação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem devem adequar o contrato para a prestação de tais serviços:~~

~~I - ao cumprimento do disposto no art. 16, incisos I, II, IV e § 2º, no caso de serviços prestados no exterior; e~~

~~II - ao disposto nos arts. 15, § 1º, e 17.~~

~~Parágrafo único. A adequação ao disposto no caput deve ocorrer até 31 de dezembro de 2021.~~

Art. 24. (Revogado, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

Art. 25. O Banco Central do Brasil poderá vetar ou impor restrições para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem quando constatar, a qualquer tempo, a inobservância do disposto nesta Resolução, bem como a limitação à atuação do Banco Central do Brasil, estabelecendo prazo para a adequação dos referidos serviços e dos contratos correspondentes.

Art. 26. Ficam revogados:

I - os arts. 1º a 26 da Circular nº 3.909, de 16 de agosto de 2018; e

II - a Circular nº 3.969, de 13 de novembro de 2019.

Art. 27. Esta Resolução entra em vigor em 1º de agosto de 2021.

Otávio Ribeiro Damaso

Diretor de Regulação