BANCO CENTRAL DO BRASIL

RESOLUTION CMN 4,893 OF FEBRUARY 26, 2021

Provides for the cyber security policy and the requirements for contracting services of data processing, data storage and cloud computing to be observed by financial institutions and other institutions licensed by the Central Bank of Brazil.

The Central Bank of Brazil, in the form of art. 9 of Law 4,595 of December 31, 1964, announces that the National Monetary Council, in its meeting held on February 25, 2021 based on art. 4, item VIII of this Law, art. 9 of Law 4,728 of July 14, 1965, art. 7 and art. 23, sub-item "a" of Law 6,099 of September 12, 1974,art. 1, item II of Law 10,194, of February 14, 2001, and art. 1, Paragraph 1, of Complementary Law 130 of April 17, 2009,

R E S O L V E D:

CHAPTER I
ON THE OBJECT AND SCOPE OF APPLICATION

Art. 1. This Resolution provides for the cyber security policy and the requirements for contracting services of data processing, data storage and cloud computing to be observed by financial institutions and other institutions licensed by the Central Bank of Brazil.

Sole paragraph. The provisions established in this Resolution do not apply for payment institutions, that must comply with the regulation published by the Central Bank of Brazil, in the exercise of its legal attributions.

CHAPTER II

ON THE CYBER SECURITY POLICY

Section I
On the Cyber Security Policy Implementation

Art. 2. The institutions mentioned in art. 1 must implement and maintain a cyber security policy formulated according to principles and guidelines that seek to ensure the confidentiality, integrity and availability of data and information systems used.

Paragraph 1. The policy mentioned in the heading must be commensurate with:

I – the institution's size, risk profile and business model;

II – the nature of operations and the complexity of the institution's products, services, activities and processes; and

III – the sensitivity of the data and information under the responsibility of the institution.

Paragraph 2. A single cyber security policy may be adopted by:

I – a prudential conglomerate; and

II – a credit cooperative system.

Paragraph 3. The institutions that decide not to constitute their own cyber security policy because of the discretion on paragraph 2 must formalize the option in a board's meeting or, in case the board is nonexistent, in a senior management's meeting.

Art. 3. The cyber security policy must comprise, at a minimum:

I – the institution's cyber security objectives;

II – the procedures and controls adopted to reduce the institution's vulnerability to incidents and to address other cyber security objectives;

III – the specific controls, including those directed at information traceability, aiming to ensure the security of sensitive information;

IV – the record of incidents relevant to the institution's activities, as well as the analysis of their cause and impact and the control of their effects;

V - the guidelines to:

a) the development of scenarios that reflect incidents considered in business continuity tests;

b) the definition of procedures and controls directed at the prevention and treatment of incidents to be adopted by third party providers that handle sensitive data or information, or that are relevant for the institution's operational activities;

c) the classification of data and information according to their relevance; and

d) the definition of parameters to be used in the assessment of the relevance of incidents;

VI – the mechanisms for dissemination of a cyber security culture within the institution, including:

a) the implementation of programs for training and periodic evaluation of employees;

b) the provision of information to clients and users regarding precautions when using financial products and services; and

c) the commitment of senior management with the continuous improvement of procedures related to cyber security; and

VII – the initiatives for sharing information with other institutions mentioned in art. 1 regarding the relevant incidents mentioned in item IV.

Paragraph 1. When defining the cyber security objectives mentioned in item I, the institution must consider its capacity to prevent, detect and reduce the vulnerability to cyber incidents.

Paragraph 2. The procedures and controls mentioned in item II must comprise, at least, authentication, criptography, prevention and detection of intrusions, prevention of information leaking, performance of periodic tests and scanning to detect vulnerabilities, protection against malicious soft-

wares, implementation of traceability mechanisms, control of access and segmentation of the computer network, as well as maintenance of data and information backups.

Paragraph 3. The procedures and controls mentioned in item II must also be applied to the development of secure information systems and to the adoption of new technologies employed by the institution.

Paragraph 4. The incident recording, analysis of cause and impact and control of effects mentioned in item IV must also comprise information received from third-party providers

Paragraph 5. The guidelines mentioned in item V, sub-item “b”, must comprise procedures and controls with a level of complexity, coverage and precision compatible with those employed by the institution itself.

Section II

On Disclosure of Cyber Security Policy

Art. 4. The cyber security policy must be disclosed to the institution’s employees and to third-party providers, in a clear and accessible language and in a level of detailing compatible with the functions developed and with the sensitivity of the information involved.

Art. 5. The institutions must disclose to the public a summary containing an outline of the cyber security policy.

Section III

On Plan of Action and Response to Incidents

Art. 6. The institutions mentioned in art. 1 must establish a plan of action and response to incidents, aiming at the implementation of the cyber security policy.

Sole paragraph. The plan mentioned in the heading must cover, at least:

I – the actions to be developed by the institution in order to adjust its organizational and operational structures to the principles and guidelines established by the cyber security policy;

II – the routines, the procedures, the controls and the technologies to be employed in the prevention of incidents and response, in conformity with the cyber security policy guidelines; and

III– the area responsible for recording and controlling the effects of relevant incidents.

Art. 7. The institutions mentioned in art. 1 must appoint a director responsible for the cyber security policy and for the execution of the plan of action and response to incidents.

Sole paragraph. The appointed director mentioned in the heading may perform other functions in the institution, except those that may result in a conflict of interest.

Art. 8. The institutions mentioned in art. 1 must prepare an annual report regarding the implementation of the plan of action and response to incidents, mentioned in art. 6, with a reference date of December 31 of each year.

Paragraph 1. The report mentioned in the heading must comprise, at a minimum:

I – the effectiveness of the implementation of the actions mentioned in art. 6, sole paragraph, item I;

II – the summary of results obtained in the implementation of routines, procedures, controls and technologies to be employed in the prevention of and response to incidents mentioned in art. 6, sole paragraph, item II;

III– the relevant cyber security incidents that occurred during the period; and

IV- the results of the business continuity tests, considering scenarios of unavailability caused by incidents

Paragraph 2. The report mentioned in the heading must be:

I – submitted to the risk committee, if existent; and

II – reported to the board or, in case a board is nonexistent, to the senior management by March 31 of the year following the reference date.

Art. 9. The cyber security policy mentioned in art. 2 and the plan of action and response to incidents mentioned on art. 6 must be approved by the board or, in case a board is nonexistent, by the senior management.

Art. 10. The cyber security policy and the plan of action and response to incidents must be documented and revised at least annually.

CHAPTER III

ON THE CONTRACTING OF SERVICES OF DATA PROCESSING, DATA STORAGE AND CLOUD COMPUTING

Art. 11. The institutions mentioned in art. 1 must ensure that their policies, strategies and structures for risk management established in regulation in force, specifically regarding to the criteria for decision on the outsourcing of services, include the contracting of relevant data processing, data storage and cloud computing services, in the country or abroad.

Art. 12. The institutions mentioned in art. 1, previously to the contracting relevant services of data processing, data storage and cloud computing, must adopt procedures that comprise:

I –the adoption of corporate governance and management practices proportional to the relevance of service to be contracted and to the risk they incur; and

II – the verification of the capacity of the third-party provider to ensure:

a) compliance with the laws and regulations in force;

b) the institution’s access to data and information to be processed or stored by the third-party provider;

c) confidentiality, integrity, availability and recovery of data and information processed or stored by the third-party provider;

d) its adherence to certifications required by the institution in order to perform the services to be contracted;

e) the institution's access to reports provided by the specialized independent auditor hired by the third-party provider, related to the procedures and the controls used in the services to be contracted;

f) provision of adequate information and management resources to monitor the services to be contracted;

g) the identification and segregation of data pertaining to the institution's clients through physical or logical controls; and

h) the quality of access controls aimed at protecting the data and information of the institution's clients.

Paragraph 1. In the assessment of the relevance of the service to be contracted, mentioned in item I of the heading, the contracting institution must consider the criticality of the service and the sensitivity of the data and information to be processed, stored and managed by the third-party provider, considering the classification carried out in accordance to art. 3, item V, sub-item "c".

Paragraph 2. The procedures mentioned in the heading must be documented, including the information related to the verification mentioned in item II.

Paragraph 3. In the case of applications run through the internet, referred to in item III of art. 13, the institution must ensure that the potential third-party provider adopts controls that mitigate the effects of possible vulnerabilities in releasing new versions of the application.

Paragraph 4. The institution must have the necessary resources and competencies for the adequate management of the services to be contracted, including the analysis of information and use of resources provided under the terms of sub-item "f", item II.

Art. 13. For the purposes of this Resolution, cloud computing services comprises the availability to a contracting institution, on demand and in a virtual form, of at least one of the following services:

I – data processing, data storage, network infrastructures and other computational resources that enable the contracting institution to deploy or run softwares, which may include operating systems and applications developed or acquired by the institution;

II - deployment or execution of applications developed or acquired by the contracting institution using a third-party provider's computing resources; or

III - execution, through the internet, of applications deployed or developed by a third-party provider using its own computational resources.

Art. 14. The institution contracting the services mentioned in art. 12 is responsible for the reliability, integrity, availability, security and confidentiality of the services contracted, as well as for compliance with the legislation and regulation in force.

Art. 15 The contracting of relevant services of data processing, data storage and cloud computing must be previously communicated to the Central Bank of Brazil by the institutions mentioned

in art. 1.

Paragraph 1. The communication mentioned in the heading must comprise the following information:

I – the name of the third-party provider to be contracted;

II – the relevant services to be contracted; and

III – the designation of the countries and the regions in each country where the services can be provided and the data can be stored, processed and managed, as defined in item III, art. 16, in the case of contracting abroad.

Paragraph 2. The communication mentioned in the heading must be made within ten days after contracting the services.

Paragraph 3. The contractual changes that imply a modification of the information referred to in paragraph 1 must be communicated to the Central Bank of Brazil within ten days after the contractual changes.

Art. 16. The contracting of data processing, data storage and cloud computing relevant services provided abroad must fulfill the following requisites:

I - the existence of an agreement for exchange of information between the Central Bank of Brazil and the supervisory authorities of the countries where the services may be provided;

II – the contracting institution must ensure that the provision of the services mentioned in the heading do not cause damage to its own functioning neither do they deter the action of the Central Bank of Brazil;

III – the contracting institution must define, previously to the contracting, the countries and the regions in each country where the services can be provided and the data can be stored, processed and managed; and

IV – the contracting institution must anticipate alternatives for business continuity either in the case of impossibility of continuation of the contract or in the case of its termination.

Paragraph 1. In the absence of an agreement under the terms of item I of the heading, the contracting institution must request an authorization from the Central Bank of Brazil for:

I – the service contracting, within a minimum period of sixty days before the contracting, observing the terms of art. 15, paragraph 1 of this Resolution; and

II – the contractual changes that imply modifications of the information referred to in art 15, paragraph 1, observing the minimum period of sixty days before the contractual changes.

Paragraph 2. In order to comply with clauses II and III of the heading, the contracting institutions must ensure that the laws and regulations in the countries and regions in each country where the services may be provided do not restrict or prevent either the institution or the Central Bank of Brazil from accessing the data and information.

Paragraph 3. The proof of compliance with the requirements referred to on items I to IV of the heading and the fulfillment of the requirement mentioned in paragraph 2 must be documented.

Art. 17. The contract of relevant services of data processing, data storage and cloud computing must comprise:

I – an indication of the countries and the regions in each country where services may be provided and data may be stored, processed and managed;

II– the adoption of security measures for transmission and storage of the data mentioned in item I from heading;

III – the segregation of data and the access controls to protect the clients' information while the contract is in force;

IV – the obligation of, in the case of contract termination:

a) transfer of the data cited in item 1 to the new third-party provider or the contracting institution; and

b) elimination of the data mentioned in item 1 by the substituted third-party provider, after the data transfer mentioned in item 'a' and the confirmation of the integrity and availability of the received data.

V – the access by the contracting institution's to:

a) information provided by the third-party provider, in order to verify the compliance with items I and III from heading;

b) information related to certifications and reports provided by the specialized independent audit mentioned in art. 12, item II, sub-items "d" and "e"; and

c) proper information and management resources to monitor the services to be provided, mentioned in art. 12, item II, sub-item "f";

VI – the obligation of the third-party provider to notify the contracting institution in case of subcontracting services deemed relevant to the institution;

VII – the permission of access by the Central Bank of Brazil to the contracts and terms related to the rendering of services, the documentation and information related to the services provided, data stored and information about its processing, backup of data and information, as well as access codes to the data and information;

VIII – the adoption of measures by the contracting institution as a result of determinations from the Central Bank of Brazil; and

IX – the obligation of the third-party provider to keep the contracting institution permanently informed about possible limitations that may affect the services provided or compliance with laws and regulations in force.

Sole Paragraph. The contract mentioned in the heading must comprise, in case the contracting institution is submitted to a resolution regime by the Central Bank of Brazil:

I – the obligation of the third-party provider to allow full access by the responsible for the resolution regime to contracts, terms, documentation and information related to the services provided, to the data stored and information about its processing, to the data and information backup, as well as to the access codes mentioned in item VII that are available to the third-party provider; and

II- the obligation to previously inform the responsible for the resolution regime about the intention of the third-party provider to interrupt the rendering of services, at least thirty days before the date of the interruption, observed that:

a) the third-party provider is obliged to accept an occasional request by the responsible for the resolution regime for an additional period of thirty days before the interruption of services; and

b) the previous information also applies to an interruption motivated by a default of the contracting institution.

Art. 18. The provisions of articles 11 to 17 do not apply to contracting of systems operated by clearing and settlement systems operators or trade repositories.

CHAPTER IV

GENERAL PROVISIONS

Art. 19. The institutions mentioned in art. 1 must ensure that their risk management policies implemented in conformity with the regulation in force comprise, relating to business continuity:

I – the treatment of relevant cyber security incidents mentioned in art. 3, item IV;

II– the procedures to be followed in case of an interruption of relevant data processing, data storage and outsource of cloud computing services, containing scenarios that consider a substitution of the third-party provider and the resumption of the normal operation of the institution; and

III – the scenarios of incidents considered in the business continuity tests referred to on art. 3, Item V, sub-item “a”.

Art. 20. The procedures adopted by institutions for risk management in conformity with the regulation in force must comprise, relating to business continuity:

I – the treatment adopted to mitigate the effect of relevant incidents mentioned in item IV, art. 3 and the interruption of relevant data processing, data storage and cloud computing services contracted;

II – the deadline stipulated for resumption or normalization of activities or relevant services interrupted, mentioned in item I; and

III – the timely communication to the Central Bank of Brazil on the occurrence of relevant incidents and the interruption of relevant services, mentioned in item I, that configure a crisis situation to the financial institution, as well as procedures for restart of activities.

Sole paragraph. Institutions must establish and document the criteria that configure a crisis situation referred to on item III from heading.

Art. 21. The institutions mentioned in art. 1 must establish monitoring and controlling mechanisms to ensure the implementation and the effectiveness of the cybersecurity policy, the plan of action and response to incidents, and the requirements for contracting services of data processing, data storage and cloud computing, including:

I – the definition of processes, tests and audit trails;

II– the definition of adequate metrics and indicators; and

III– the identification and correction of occasional deficiencies.

Paragraph 1. The definition of mechanisms mentioned in the heading must consider the notifications received on the subcontracting of relevant services mentioned in art. 17, item VI.

Paragraph 2. The mechanisms mentioned in the heading must be submitted to periodic tests by the internal audit, when applicable, in line with the internal controls of the institution.

Art. 22. While safeguarding the duty of secrecy and free competition, the institutions mentioned in art. 1 must develop initiatives for sharing information on the relevant incidents mentioned in art. 3, item IV.

Paragraph 1. The information sharing mentioned in the heading must comprise information on relevant incidents received from third-party providers.

Paragraph 2. The information shared must be made available to the Central Bank of Brazil.

CHAPTER V

FINAL PROVISIONS

Art. 23. The documents relative to the following topics must be made available to the Central Bank of Brazil for five years:

I – the cyber security policy mentioned in art. 2;

II–the minute of the board's meeting or, in case the board is nonexistent, the minute of the senior management's meeting, in the case the option mentioned in the Art. 2, paragraph 2, is exercised;

III – the plan of action and response to incidents mentioned in art. 6;

IV – the annual report mentioned in art. 8;

V – the procedures mentioned in art. 12, paragraph 2;

VI – the documentation mentioned in art. 16, paragraph 3, in the case of services provided abroad;

VII – the contracts mentioned in art. 17, the lapse mentioned in the heading being counted from the termination of the contract;

VIII – the data, the records and information related to the mechanisms of monitoring and control mentioned in art. 21, the lapse mentioned in the heading being counted from the implementation of such mechanisms; and

IX – the documentation with the criteria that configure a crisis situation referred to on art. 20, sole paragraph.

Art. 24. The Central Bank of Brazil may adopt measures to enforce the provisions in this Resolution, as well as the establishment of:

I – the requirements and procedures related to information sharing, in accordance with art. 22;

II – the requirement of certifications and other technical requisites to be demanded from

third-party providers by the contracting financial institution for rendering the services mentioned in art 12;

III – the maximum deadline, mentioned in art. 20, item II, for resumption or normalization of the financial institution's relevant activities or services interrupted; and

IV – the technical requirements and operational procedures to be observed by institutions in order to comply with the provisions established in this Resolution.

Art. 25. The institutions referred to in art. 1 that, on April 26, 2018, had already contracted the provision of relevant data processing, data storage and cloud computing services must adjust the contract to provide such services:

I – art. 16, items I, II, IV and paragraph 2, in the case of services provided abroad; and

II – art. 15, paragraph 1, and art. 17.

Sole paragraph. The deadline for compliance mentioned in the heading must not exceed December 31, 2021.

Art. 26. The Central Bank of Brazil may reject or impose restrictions, at any time, to the contracting of services for data processing, data storage and cloud computing in case of a failure in compliance with the provisions established in this Resolution, establishing a deadline for adequacy of the services provided by the institution.

Art. 27. These following resolutions are hereby revoked:

I - Resolution 4,658, of April 26, 2018; and

II - Resolution 4,752, of September 26, 2019.

Art. 28. This Resolution enters into force on July 1st, 2021.

Roberto de Oliveira Campos Neto

Governor of the Central Bank of Brazil