Resolution No. 4,658 of April 26, 2018

This Resolution addresses cybersecurity policy and requirements for the hiring of data processing, storage and cloud computing services to be complied by financial institutions and other institutions authorized to operate by the Brazilian Central Bank.

As per section 9 of Law No. 4,595 dated of December 31, 1964, the Brazilian Central Bank states that the National Monetary Council, in a meeting held on April 26, 2018, based on section 4, item VIII of such Law, section 9 of Law No. 4,728 dated of July 14, 1965, sections 7 and 23, sub item "a" of Law No. 6,099 dated of September 12, 1974, section 1, item II of Law No. 10,194 dated of February 14, 2001, section 1, paragraph 1 of Supplementary Law No. 130 dated of April 17, 2009,

RESOLVED:

CHAPTER I
PURPOSE AND SCOPE

Section 1. This Resolution determines cybersecurity policy and requirements for the hiring of data processing, storage and cloud computing services to be complied by financial institutions and other institutions authorized to operate by the Brazilian Central Bank.

CHAPTER II
CYBERSECURITY POLICY

Segment I
Implementing Cybersecurity Policy

Section 2. The institutions referred to in section 1 shall implement and maintain a cybersecurity policy based on principles and guidelines designed to ensure confidentiality, integrity and availability for data and information systems used.

§ 1 The abovementioned policy must be compatible with:

I - the institution's scale, risk profile and business model;

II - the nature of its operations and the complexity of its products, services, activities and processes; and

III - the sensitivity of data and information under the institution's responsibility.

§ 2 A single cybersecurity policy may be adopted by:

I - prudential conglomerates; and

II - cooperative credit systems.

§ 3 Institutions that do not adopt their own cybersecurity policy, under the terms of § 2, shall formalize this option in a meeting of the board of directors or, in its absence, in a meeting of the executive board of the institution.

Section 3. The cybersecurity policy shall contemplate, as a minimum:

I – the institution's cybersecurity objectives;

II - the internal procedures and controls adopted by the institution to reduce its vulnerability to incidents and address other cybersecurity objectives;

III - the specific controls, including those used to ensure data traceability in order to secure sensitive information;

IV – the logging or recording, analysis of cause and impact, and control of the effects of incidents that are material for the institution's activities;

V – the guidelines for:

a) preparing scenarios for incidents covered by business continuity testing;

b) defining procedures and controls to prevent and treat incidents to be adopted by third party service providers that handle data or information that is sensitive or material for running the institution's operational activities;

c) classifying data and information by its materiality; and

d) defining parameters to be used to assess the materiality of incidents.

VI - the mechanisms for the dissemination of cybersecurity culture in the institution, including:

a) the implementation of personnel training programs and periodic evaluation;

b) the provision of information to customers and users concerning precautions in the use of financial products and services; and

c) the commitment of senior management with the continuous improvement of procedures related to cybersecurity.

VII - the measures to disclose information on material incidents, mentioned in item IV, with other institutions referred to in Section 1.

§ 1 In the definition of the cybersecurity objectives referred to in item I, it should be contemplated the ability of the institution to prevent, detect and reduce the vulnerability to cyber related incidents.

§ 2 The procedures and controls mentioned in item II shall at least cover authentication, encryption, prevention and detection of intrusion, prevention from data leakage, periodic testing and scanning to detect vulnerabilities, protection against malicious software, establishment of traceability mechanisms, controls of access and segmented computer networks and maintenance of backup copies of data and information.

§ 3 The procedures and controls mentioned in item II shall also be applicable in the development of secure information systems and in the adoption of new technologies used for the institution's activities.

§ 4 The registration, analysis of cause and impact, and control of effects of incidents, mentioned in item IV, must also include information received from third party service providers.

§ 5 The guidelines referred to in item V, sub item "b" should include procedures and controls at similar levels of complexity, coverage and accuracy compatible with those used by the institution itself.

Segment II

Disclosure of the Cybersecurity Policy

Section 4. The cybersecurity policy shall be disclosed to the institution's employees and to third party service providers, using a clear and accessible language and with a level of detailing compatible with the functions performed and with the sensitivity of the information.

Section 5. Institutions shall disclose to the public a summary with general lines of the cybersecurity policy.

Segment III
Action Plan and Incident Response

Section 6. The institutions referred to in section 1 should have cybersecurity policy action plans and incident response procedures in place.

Sole paragraph. The abovementioned plan shall establish at least the following:

I - actions to be developed by the institution for its organizational and operational structures to comply with cybersecurity policy principles and guidelines;

II - routines, procedures, controls and technologies to be used for incident prevention and response in accordance with cybersecurity policy guidelines; and

III - the area responsible for the register and control of the effects of material incidents.

Section 7. The institutions referred to in Section 1 shall designate a director or officer in charge of cybersecurity policy and the execution of the action plan and incident response procedure.

Sole paragraph. The abovementioned director or officer may have other duties in the institution provided that there is no conflict of interest.

Section 8. The institutions referred to in Section 1 shall prepare an annual report covering the adoption of the action plans and incident response procedures as mentioned in Section 6, by base date December 31.

§ 1 The abovementioned report shall cover at least the following matters:

I - the efficacy of the adoption of the actions described in Section 6, Sole Paragraph, item I;

II - summary of the results obtained in the implementation of the routines, procedures, controls and technologies to be applicable in case of incident prevention and response, described in Section 6, Sole Paragraph, item II;

III - any material cyber incident that occurred in the period; and

IV - business continuity test results, including unavailability scenarios arising from incidents.

§ 2 The abovementioned report shall be:

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

II – presented to the institution's board of directors or, in its absence, to the executive board of the institution by 31 March of the year following the base date.

Section 9. The cybersecurity policy referred to in Section 2 and action plan and incident response mentioned in Section 6 must be approved by the institution's board of directors, or, in its absence, by the executive board of the institution.

Section 10. The cybersecurity policy and action plan and incident response shall be documented and reviewed, at least, annually.

CHAPTER III
HIRING OF DATA PROCESSING, STORAGE AND CLOUD COMPUTER SERVICES

Section 11. Institutions referred to in Section 1 shall ensure that their policies, strategies and structures for risk management set forth in the regulation currently in force, in particular the criteria for outsourcing services, contemplate the hiring of material data processing, storage and cloud computing services, in Brazil or offshore.

Section 12. Institutions referred to in Section 1, prior to hiring material data processing, storage and cloud computing services, shall adopt procedures that contemplate:

I – the adoption of corporate governance and management practices proportional to the materiality of the service to be hired and their risk exposure; and

II - examination of the potential ability of the potential service provider to ensure:

a) compliance with legislation and regulation in force;

b) access by the financial institution to data and information to be processed or stored by the service provider;

c) the confidentiality, integrity, availability and retrievability of data and information processed or stored by the service provider;

d) compliance with the certifications required by the institution for the provision of the service to

be hired;

e) the institution's access to the reports drafted by independent and specialized audit firm hired by the service provider, related to the procedures and controls used to provide the services to be hired;

f) the provision of information and management resources appropriate to the monitoring of the services to be provided;

g) identification and segregation of financial institution's client data using physical or logical controls; and

h) quality of the access controls to protect financial institution's client data and information.

§ 1 In assessing the materiality of service to be hired, as mentioned in item I above, the financial institution shall consider the criticality of the service and the sensitivity of data and information to be processed, stored and managed by the service provider, including its classification as per Section 3, item V, sub item "c".

§ 2 The procedures addressed above, including the information related to the examination referred to in item II, shall be documented.

§ 3 In the case of running applications over the Internet, mentioned in item III of Section 13, the institution shall ensure that the potential service provider adopts controls to mitigate the effects of any vulnerabilities when new versions of the application are released.

§ 4 The institution shall have the necessary resources and abilities to the appropriate management of the services to be hired, including for the analysis of information and use of resources provided pursuant to item II, sub item "f" of Section 12.

Section 13. For the purposes of this Resolution, cloud computing services shall include on demand and virtual availability for the financial institution of at least one of the following services:

I - data processing, data storage, network infrastructure and other computing resources that enable the financial institution to implement or run software that may include operating systems and applications developed by or acquired by the institution;

II - implementation or execution of applications developed by or acquired by the institution, using the service provider's computing resources; or

III - over the internet, run applications implemented or developed by the service provider, using the services provider's own computing resources.

Section 14. Institutions engaging the services mentioned in Section 12 shall be responsible for the reliability, integrity, availability, security and confidentiality of the services hired and for compliance with current legislation and regulations.

Section 15. The hiring of material data processing, storage and cloud computing services shall be previously communicated to Brazilian Central Bank by the institutions referred to in Section 1.

§ 1 The communication addressed in Section 15 should contain the following information:

I - the corporate name of the service provider;

II - the material services to be hired; and

III - the indication of countries and regions in each country where services can be provided and data may be stored, processed and managed, defined in Section 16, item III, in case of hiring abroad.

§ 2 The communication referred to above must be carried out, at least, sixty days before the hiring of the services.

§ 3 The contractual amendments that result in the modification of the information referred to in § 1 must be communicated to the Brazilian Central Bank, at least, sixty days before the contractual amendment.

Section 16. The hiring of material data processing, storage and cloud computing services provided offshore must comply with the following requirements:

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

II - the financial institution shall ensure that the provision of the services mentioned above does not cause damage to the regular operation of the institution, nor embarrassment to the performance of Brazilian Central Bank;

III - the financial institution shall define, prior to the hiring, the countries and regions in each country where services can be provided and the data may be stored, processed and managed; and

IV - the financial institution shall establish alternatives for the business continuity, in case of impossibility of maintenance or termination of the services agreement.

§ 1 In the case of the non-existence of an agreement under the terms established in item I above, the financial institution shall request authorization from the Brazilian Central Bank for the hiring of services, following the deadline and the information required under Section 15 of this Resolution.

§ 2 In order to comply with items II and III above, the financial institutions shall ensure that legislation and regulation in the countries and regions in each country where services may be provided do not restrict or impede the access of the financial institution and the Brazilian Central Bank to data and information.

§ 3 Proof of compliance with the requirements set forth in item I to IV above and compliance with the demand referred to in § 2 shall be documented.

Section 17. Material data processing, storage and cloud computing services agreements shall stipulate:

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

II - the adoption of security measures for data transfer and storage as mentioned in item I above;

III - maintenance, throughout the contractual term, of data segregation and access controls to protect client information;

IV - the obligation, in case of termination of the service agreement, of:

a) transferring the data mentioned in item I to the new service provider or to the financial institution; and

b) deleting data mentioned in item I by the replaced service provider, after the transferring of data set forth in sub item "a" above and the confirmation of integrity and availability of the received data.

V - the financial institutions access to:

a) information provided by the service provider in order to verify the compliance with the rules

established in item I to III above;

b) information related to certifications and reports of specialized audit firm, mentioned in Section 12, item II, sub items "d" and "e"; and

c) information and appropriate management resources to the monitoring of services to provided, mentioned in section 12, sub item "f" above.

VI - the obligation of the service provider to notify the financial institution regarding the subcontracting of material services for the institution;

VII - the permission to the access of the Brazilian Central Bank to contracts and agreements signed for the provision of services, documentation and information involving the services provided, data stored and respective information concerning data processing, backup copies of data and information, as well as access codes to the data and information;

VIII - the adoption of measures by the financial institution due to the determination of Brazilian Central Bank; and

IX - the obligation of the service provider to keep the financial institution constantly informed of any limitations that may affect the provision of services or compliance with current legislation and regulations.

Sole Paragraph. The agreement with service provider shall stipulate that, in the event that the Brazilian Central Bank orders the liquidation/winding up of the financial institution:

I - the obligation of the service provider to allow full and unrestricted access of the responsible for the liquidation/winding up arrangements to the contracts, agreements, documentation and information related to the provision of services, to data stored and information concerning the respective data processing, to backup copies of data and information, including access codes, mentioned in item VII above, that are being held by service provider; and

II - the obligation of giving advance notice to the person or entity responsible for the liquidation/winding up arrangements as to the contractor's intention to cease the provision of services at least thirty days before the scheduled date for the interruption, provided that:

a) the service provider undertakes to agree to any request made by the responsible for the liquidation/winding up arrangements to postpone termination of services for an additional thirty (30) days; and

b) the advance notification must also occur in the event of termination arising from breach or default by the contracting party.

Section 18. The provisions set forth in Sections 11 to 17 shall not apply to the hiring of systems operated by chambers, by providers of clearing and settlement services or by entities exercising registration or centralized depository activities.

CHAPTER IV
MISCELLANEOUS

Section 19. The institutions referred to in Section 1 shall ensure that the risk management policies provided for in the current regulation stipulate, concerning the business continuity, about:

I – the treatment of material incidents related to cybernetic environment as per item IV of Section 3;

II - procedures to be followed in cases of disruption of material data processing, storage and cloud computing services, covering scenarios that consider the replacement of the service provider and recovery of the institution's normal operations; and

III - the scenarios of business continuity testing incidents referred to in Section 3, item V, sub item "a".

Section 20. In relation to business continuity, the institutions' risk management procedures as stipulated in current regulations must include:

I – the treatment planned to mitigate the effects of material incidents referred to in Section 3, item IV and those arising from disruption of material data processing, storage and cloud computing services;

II – the stipulated term to resume or normalize its disrupted activities or material services as mentioned in item I; and

III - timely communication to the Brazilian Central Bank of any material incidents and disruptions of the material services, mentioned in item I, that constitutes a crisis situation by financial institution, as well as the measures taken to resume its activities.

Section 21. The institutions referred to in section 1 shall adopt monitoring and control mechanisms to ensure the deployment and efficacy of cybersecurity policy, action plan and

incident response, and requirements for hiring data processing, storage and computing services, including:

I - definitions of audit processes, tests and trails;

II - definitions of appropriate metrics and indicators; and

III - identification and correction of eventual deficiencies.

§ 1º The notices received regarding the subcontracting of material services described in Section 17, item VI, shall be considered in the definition of the abovementioned mechanisms.

§ 2º The abovementioned mechanisms must be periodically submitted to testing by the internal audit, when applicable, compatible with the institution's internal controls.

Section 22. Without prejudice to the duty of secrecy and free competition, the institutions mentioned in section 1 shall adopt measures for the disclosure of information regarding material incidents referred to in Section 3, item IV.

§ 1 The abovementioned disclosure must include information regarding material incidents received from third party service providers.

§ 2 The information disclosed must be available to Brazilian Central Bank.

CHAPTER V
FINAL PROVISIONS

Section 23. The following should be retained at the Brazilian Central Bank's disposal for five years:

I - the cybersecurity policy document mentioned in Section 2;

II - minutes of the meeting of the board of directors or, in its absence, meeting of the executive board of the institution, in the event that the option addressed in Section 2, § 2 is formalized;

III - the document related to the action plan and incident response procedure mentioned in Section 6;

IV - the annual report mentioned in Section 8;

V- the documentation on the procedures referred to in Section 12, § 2;

VI - the documentation referred to in Section 16, § 3, in case of services provided offshore;

VII - the agreement mentioned in Section 17, given that such term must be counted as of the termination date of the agreement; and

VIII - the data, logs and information concerning the monitoring and control mechanisms mentioned in section 21, given that such term must be counted as of the implementation of such mechanisms.

Section 24. The Brazilian Central Bank may take measures required to enforce the compliance with the provisions hereof and may determine:

I - the requirements and procedures to the disclosure of information, under the terms of Section 22;

II - certifications and other technical requirements to be required of service providers engaged by a financial institution in its capacity as principal, for the provision of services mentioned in Section 12;

III - the final terms mentioned in Section 20, item II, for resuming or normalizing disrupted material activities or services; and

IV - the technical requirements and operational procedures to be followed by the institutions in order to comply with this Resolution.

Section 25. Institutions referred to in Section 1 that, in the date that this Resolution enters into force, have already hired material data processing, data storage and cloud computing services must submit, to the Brazilian Central Bank, within one hundred and eight days as of the date on which this Resolution enters into force, a schedule for adequacy:

I – to the compliance with the Section 16, items I, II, IV and § 2, in case of services provided offshore; and

II – to the provisions of Sections 15, § 1 and 17.

Sole paragraph. The term provided in the schedule for adequacy mentioned above shall not exceed December 31, 2021.

Section 26. The approval of the cybersecurity policy, referred to in Section 2, and of the action plan and incident response, referred to in Section 6, must be accomplished, under the terms of Section 9, until May 6th, 2019.

Section 27. The Brazilian Central Bank may prohibit or impose restrictions on the hiring of data processing, data storage and cloud computing services if, at any time, it finds that such service does not comply with the terms hereof, as well as limits the action of Brazilian Central Bank, and may set a deadline for the adequacy of the referred service.

Section 28. This Resolution shall enter into force on its publication date.

Ilan Goldfajn
President of the Brazilian Central Bank