OFFICIAL DIARY OF THE UNION

Published: 31/08/2021 | Edition: 165 | Section: 1 | Page: 2

Body: Presidency of the Republic/Institutional Security Cabinet

NORMATIVE INSTRUCTION NO. 5, OF AUGUST 30, 2021

Provides for the minimum information security requirements for the use of cloud computing solutions by bodies and entities of the federal public administration.

THE STATE MINISTRY HEAD OF THE INSTITUTIONAL SECURITY CABINET OF THE PRESIDENCY OF THE REPUBLIC, in the use of the attribution conferred on him by art. 87, single paragraph, items I and II, of the Constitution, and in view of the provisions of art. 12 of Decree No. 9,637, of December 26, 2018, resolves:

Art. 1 Provide for the minimum information security requirements for the use of cloud computing solutions by the agencies and entities of the federal public administration.

CHAPTER I

GENERAL DISPOSALS

Art. 2 For the purposes of this Normative Instruction, will be considered the concepts contained in the Glossary of Information Security, approved and updated by an ordinance of the Institutional Security Cabinet of the Presidency of the Republic.

Art. 3 Cloud computing is composed of the following implementation models:

I - private (or internal) cloud - cloud infrastructure dedicated for the exclusive use of the body and its linked units, or of an entity composed of multiple users, and its property and management may belong to the organization itself, third parties or both;

II - community cloud - dedicated cloud infrastructure for the exclusive use of a community, or a group of users from unrelated bodies or entities, who share the same nature of work and obligations, and may be owned and managed by organizations community, third parties, or both;

III - public (or external) cloud - cloud infrastructure dedicated for open use by any organization, and its property and management can be public, private or both; and

IV - hybrid cloud - cloud infrastructure composed of two or more distinct infrastructures (private, community or public), which remain with their own characteristics, but grouped by standard technology that allows interoperability and portability of data, services and applications.

CHAPTER II

OF THE NORMATIVE ACT ON THE SAFE USE OF CLOUD COMPUTING

Art. 4 All bodies or entities that wish to use cloud computing must compulsorily edit a normative act on the safe use of cloud computing.

Art. 5 The normative act on the safe use of cloud computing must, at least:

I - be prepared based on the information security policy of the body or entity;

II - be approved by senior management and disclosed to all interested parties;

III - list the goals to be achieved and the objectives that govern the cloud computing service;

IV - define the roles and responsibilities of agents assigned to manage cloud computing services; and

V - establish the periodicity for its review, which should not exceed two years.

Single paragraph. The review of the normative act provided for in the caput may occur at any time, when there are significant changes in information security requirements that influence the safe use of cloud computing, in order to ensure its continuity, sustainability, adequacy and effectiveness.

Art. 6 The body or entity must establish a team to prepare and review the normative act on the safe use of cloud computing.

CHAPTER III

OF THE RESPONSIBILITIES

Art. 7 The Information Security Manager is responsible for:

I - establishing and coordinating the team described in art. 6, responsible for drafting and revising the normative act on the safe use of cloud computing;

II - supervising the application of the normative act on the safe use of cloud computing;

III - ensuring the continued effectiveness of communication with the cloud service provider, which provides such services to the body or entity, in order to ensure that the agreed controls and service levels are complied with;

IV - supervising the application of corrective measures by the cloud service provider, in cases of possible deviations;

V - communicating cyber incidents reported by the cloud service provider to the competent bodies for their treatment, according to the relevance of the incidents previously established; and

VI – forwarding the drafts for the preparation and revision of the normative act on the safe use of cloud computing for approval by senior management.

Art. 8 The Information Security Committee or equivalent structure is responsible for:

I - establishing the countries in which data and information under the custody of the federal public administration may be stored in cloud computing solutions;

II - defining the minimum cryptographic requirements for the storage of data and information, under the custody of the federal public administration, in cloud computing solutions; and

III - analyzing, conclusively, the drafts for the preparation and revision of the normative act on the safe use of cloud computing.

Art. 9 The senior management of the body or entity is responsible for approving the drafts for the preparation and revision of the normative act on the safe use of cloud computing and disclosing them to interested parties.

CHAPTER IV

OF THE REQUIREMENTS FOR THE SAFE ADOPTION OF CLOUD COMPUTING

Art. 10. The minimum requirements of this Chapter must be observed for bodies or entities to adopt cloud computing solutions in a secure manner, with the objective of raising the level of protection of information in the use of this technology.

Section I

Of the transfer of services to a cloud service provider

Art. 11. Before transferring services or information to a cloud service provider, bodies or entities must at least:

I - ensure that the following operations are in line with Brazilian legislation and the rights to privacy, protection of personal data and the confidentiality of private communications and records:

a) collection, storage, custody and processing of personal data records; and

b) communications carried out by internet connection and application providers, in which at least one of these acts takes place in national territory;

II - carry out risk management, preceded by analysis and report on the impact of personal data, in accordance with the legislation, of the following items:

a) the type of information to be migrated;

b) the data treatment flow that may be affected by the adoption of the solution;

c) the value of the assets involved; and

d) the benefits of adopting a cloud computing solution in relation to security and privacy risks related to making information and services available to a third party;

III - define the cloud computing service and implementation model that will be adopted;

IV - use, for structuring systems, only the implementation models of private cloud or community cloud, as long as they are restricted to the infrastructure of agencies or entities;

V - evaluate what information will be hosted in the cloud, considering:

a) the information classification process in accordance with legislation;

b) the value of the information asset;

c) physical and logical access controls related to information security; and

d) the cloud computing service and implementation model;

VI - define risk and cost mitigation measures for the implementation of a cloud computing solution and for the possibility of growth of this solution; and

VII - plan information and service migration costs, in the case of entry and exit of the cloud computing service.

Section II

Of the ability of the cloud service provider to implement updates

Art. 12. Due to the ability of the cloud service provider to implement updates related to information security in its products and services, bodies or entities shall, at least:

I - define the criteria and frequency of updates to procedures and computational resources to be observed by the cloud service provider; and

II - periodically review and update its internal information security risk management processes.

Section III

Of the managing identities and records (logs)

Art. 13. In relation to the management of identities and records, bodies or entities shall, at least:

I - adopt a federated identity standard to allow the use of single sign-on technology in the process of authenticating its users to the cloud service provider;

II - deny the cloud service provider permission to use and direct access to the authentication environment of the body or entity;

III - adopt, according to the level of criticality of the information, the use of single sign-on technology, which must go along with:

a) multifactor authentication; or

b) of another alternative that increases the degree of security in the authentication process of its users with the cloud service provider;

IV - require the cloud service provider to:

a) register all cyber accesses, incidents and events, including information about sessions and transactions; and

b) store, for a period of one year, all the records referred to in paragraph a;

V - store records of all cyber accesses, incidents and events, including information on sessions and transactions, for five years, in the cloud service provider's environment or in its own controlled environment, at the discretion of the contracting agency or entity;

VI - keep in a controlled environment, for a period of five years, records of all cyber accesses, incidents and events, including information on sessions and transactions received from the cloud service provider; and

VII - enable the security team to access and use the records generated by the cloud service provider.

Section IV

Of the use of cryptographic resources

Art. 14. In relation to the need to use cryptographic resources, bodies or entities must, at least:

I - check whether the organization's data is being processed and stored in accordance with the law;

II - analyze the need to encrypt data based on legal requirements, risks, criticality level, costs and benefits; and

III - use, whenever possible, hardware-based encryption keys.

Section V

Of the data segregation and logical separation

Art. 15. In relation to data segregation and logical separation in cloud computing environments, bodies or entities, together with the cloud service provider, shall establish at least the following actions:

I - ensure that the contracted environment is protected from external users of the cloud service and unauthorized persons and implement information security controls in order to provide adequate isolation of the resources used by different agencies or entities of the federal public administration and by others cloud service users;

II - ensure that appropriate logical segregation of data from virtualized applications, operating systems, storage and network is applied in order to establish the separation of resources utilized;

III - ensure the separation of all resources used by the Cloud Service Provider from those resources used by the internal administration of the body or entity; and

IV - assess the risks associated with running proprietary software to be installed on the cloud service.

Section VI

Of the cloud management

Art. 16. In relation to cloud management, bodies or entities must, at least:

I - capacitate the team responsible for this management of the technologies used by the cloud service provider;

II - require the cloud service provider to document and to communicate their information security resources, roles and responsibilities for the use of their cloud services;

III - prepare a matrix of responsibilities that includes obligations and responsibilities of its own; and

IV - develop an incident treatment process with the cloud service provider and communicate it to the team responsible for managing the cloud.

Section VII

Of the treatment of information

Art. 17. In relation to the treatment of information in a cloud computing environment, the body or entity, in addition to complying with the guidelines contained in the legislation on personal data protection, must observe the following guidelines:

I - information without access restrictions may be treated in a cloud environment, considering the legislation and information security risks;

II - classified information in the degree of secrecy and preparatory document that may originate classified information cannot be processed in a cloud computing environment; and

III - may be treated in a cloud computing environment, subject to information security risks and current legislation:

a) information with access restriction provided for in the legislation, pursuant to the Annex to this Normative Instruction;

b) material with restricted access regulated by the body itself or by the entity;

c) personal information relating to intimacy, privacy, honor and image; and

d) the preparatory document not provided for in item II of the caput.

Art. 18. The data, metadata, information and knowledge produced or held in custody by the body or entity, transferred to the cloud service provider, must be hosted in Brazilian territory, subject to the following provisions:

I - at least one updated backup copy must be kept in Brazilian territory;

II - the information without access restriction may have up-to-date backup copies outside Brazilian territory, in accordance with applicable legislation;

III - information with access restriction provided for in the legislation and the preparatory document not provided for in item II of the caput art. 17, as well as their updated backup copies, cannot be processed outside Brazilian territory, in accordance with applicable legislation; and

IV - in the case of personal data, the guidelines provided for in Law No. 13,709, of August 14, 2018, General Personal Data Protection Law - GPDPL and other legislation on the subject must be observed.

Section VIII

Of the specific contractual clauses

Art. 19. The contractual instrument to be signed with a cloud service provider for the provision of the cloud computing service must contain devices that address the requirements established in art. 10 to art. 18 in addition to at least the following security procedures:

I - confidentiality term that prevents the cloud service provider from using, transferring and releasing data, systems, processes and information of the body or entity to national, transnational, foreign companies, countries and foreign governments;

II - guarantee of exclusivity of rights, by the agency or entity, on all information processed during the contracted period, including any available copies, such as security backups;

III - prohibition of the use of information of the body or entity by the cloud service provider for advertising, optimization of artificial intelligence mechanisms or any unauthorized secondary use;

IV - compliance of the cloud service provider's information security policy with Brazilian legislation;

V - full return of data, information and systems under the custody of the cloud service provider to the contracting agencies or entities at the end of the contract;

VI - elimination, by the cloud service provider, at the end of the contract, of any data, information or system of the body or entity under its custody, observing the legislation that deals with the mandatory data retention; and

VII - guarantee of the right to be forgotten for personal data, pursuant to art. 16 of Law No. 13,709, of August 14, 2018 - LGPD.

CHAPTER V

CLOUD SERVICE PROVIDER REQUIREMENTS

Art. 20. In order to be able to provide cloud services for the bodies or entities of the federal public administration, the cloud services provider must comply, not minimum, the following requirements:

I – have risk management methodology, prepared in accordance with the best practices and with the legislation, as well as performing the risk management described in item II of art. 11;

II – implement practices to strengthen virtualization mechanisms, which should include, at least the following procedures:

a) disable or remove all unnecessary interfaces, ports, devices or services run by the operating system;

b) securely configure all network interfaces and virtual storage areas;

c) establish limits for the use of virtual machine resources (Virtual Machine – VM);

d) keep all operating systems and application running in the virtual machine on its most current versions;

e) validate the integrity of cryptographic key management operating;

f) have controls that allow authorized users of the public bodies or entities to access the administrative access logs of the virtual machine monitor – Hypervisor;

g) enable full Hypervisor logging; and

h) support the use of trusted virtual machines (Trusted VM) provided by the public body or entity, which are in compliance with the required network strengthening policies and practices to the cloud services provider;

III – in relation to the management of identities and records:

a) have procedures of access control that address the transition between roles, the limits and controls on user privileges and controls on the use of user accounts;

b) impose an authentication mechanism that requires minimum size, complexity, duration and access password history;

c) support single sign-on technology for authentication;

d) support multifactor authentication mechanisms or another alternative that increase the degree of security in the authentication process of users of the public body or entity at the service provider cloud, according to the criticality level of the information;

e) allow the public body or entity to manage its own identities, including creation, update, delete and suspend in the environment provided by the cloud service provider; and

f) meet legal requirements, best security practices and other required criteria by the public body or entity in its authentication, access control, accounting and registration (format , retention and access);

IV – in relation to the security of web applications made available in the cloud environment:

a) use specialized firewalls to protect systems and applications;

b) develop web code in accordance with best development practices insurance and with existing regulations;

c) use best practices in operating system and application security;

d) periodically perform network and application penetration test; and

e) have a vulnerability remediation program;

V – have business continuity management and change management process, in compliance with existing regulations and best practices in these areas;

VI – have a disaster recovery plan that establishes procedures for recovery and restoration of platform, infrastructure, applications and data after loss incidents of data;

VII – establish a secure communication channel using at least Secure Sockets Layer/Transport Layer Security (SSL/TLS);

VIII – use a secure encryption standard, as per the international standard admittedly accepted, that can be implemented with generated encryption keys and stored by the public body or entity;

IX – provide facilities that enable the application of its own cryptographic protection of the public body or entity;

X – in relation to data segregation:

a) isolate, using logical separation, all data and services of the public body or entity of other cloud service customer;

b) segregate management traffic from public body or entity data traffic; and

c) implement security devices between zones;

XI – have procedures in relation to the disposal of information and data assets, which ensure:

a) safely sanitize or destroy existing data on devices discarded by through the use of methods that comply with the standards established for the conduct and best practices;

b) securely destroy an information asset at the end of its life cycle or considered unserviceable, with the provision of a Certificate of Electronic Equipment Destruction – CEED and itemize the assets that have been recycled, as well as the weight and the types of materials obtained as a result of the destruction process; and

c) securely store information assets to be disposed of in an environment with controlled physical access, with registration of all movement in and out of devices;

XII – immediately notify the cyber incident public body or the entity against the services or data in your custody;

XIII – have the necessary procedures for preserving evidence, in accordance with legislation; and

XIV – demonstrate compliance with cloud security standards, through annual audit Service and Organization Controls 2 (SOC 2), conducted by an independent auditor, with the submission of Type I and Type II reports.

CHAPTER VI

THE USE OF CLOUD BROKERS

Art. 21. The cloud broker shall act as an integrator of cloud computing services between the body and entity of the federal public administration and two or more service providers of a cloud.

Art. 22. If the body or entity contracts through the cloud broker management platform multi-cloud to perform environment provisioning and orchestration procedures, it is necessary that the tool has at least:

I – regarding multi-cloud provisioning and orchestration functionalities:

a) a single integrated end-user provisioning portal;

b) use of provisioning models;

c) secure automation of simultaneous provisioning and use, where appropriate, tools open source and interoperable;

d) event-based orchestration workflows; and

e) integrated secure infrastructure creation solutions by code – IaaC

II – in relation to the multi-cloud monitoring and analysis functionalities:

a) cloud resources performance monitoring reports;

b) collection and monitoring of records ; and

c) alert monitoring procedures;

III – in relation to the multi-cloud inventory and classification functionalities:

a) inventory of cloud resources;

b) security procedures for setting up resources on the management platform multi-cloud; and

c) detection of untagged resources; and

IV – in relation to security, compliance and identity management functionalities:

a) single sign-on and multifactor authentication mechanisms for cloud platform;

b) secure management of users and user group;

c) resource security management ;

d) notifications of multichannel alert events;

e) identity and access management – IAM; and

f) cloud platform activity logs.

Single paragraph. The cloud broker may use a Software as a Service (SaaS) tool common in the market, as long as there is no risk of technological dependence to make this platform.

Art. 23. The cloud broker is responsible for ensuring that the cloud service providers that it represents:

I – comply with all the requirements set forth in this Normative Instruction and in Brazilian legislation; and

II – operate in accordance with the best security practices.

Single paragraph. The body or entity must provide in the contractual instrument that the cloud broker may be held liable, civilly, and administratively, for any non-compliance in the providers it represents.

CHAPTER VII

GENERAL PROVISIONS

Art. 24. To ensure the security referred to in this Normative Instruction, the public bodies and entities adopt other complementary guidelines, as long as they do not confront the options of the legislation.

Art. 25. The presentation of type I and type II reports of the SOC 2 audit, proven to compliance with cloud security standards is an essential condition, both to enable the participation in a bidding process, such as to renew the contract for the provision of cloud services with bodies or entities of the federal public administration.

Single paragraph. In the event of using a cloud broker, this will be responsible for submit the SOC 2 audit Type I and Type II reports of all cloud service providers that he represents.

Art. 26. The bodies or entities of the federal public administration that are already using cloud service provider services will have a term of twelve months after entry into force of this Normative Instruction, for the adequacy of its contracts.

CHAPTER VIII

FINAL AND TRANSITIONAL PROVISIONS

Art. 27. The following normative acts are hereby revoked:

I - GSI/PR Ordinance No. 11, of February 7, 2012; and

II - GSI/PR Ordinance No. 9, of March 15, 2018.

Art. 28. This Normative Instruction enters into force on the date of its publication.

AUGUSTO HELENO RIBEIRO PEREIRA

ANNEX

EXEMPLIFICATION TABLE OF DESCRIPTIVE TYPES OF INFORMATION.

<table>
<tr><td>Type</td><td colspan="2">Description</td></tr>
<tr><td rowspan="2">1.OSTENSIVE</td><td colspan="2">Active Transparency</td></tr>
<tr><td colspan="2">Passive Transparency</td></tr>
<tr><td rowspan="3">2. SECRETCLASSIFIED IN DEGREE OF CONFIDENTIALITY</td><td colspan="2">2.1 Reserved – Maximum access restriction of 5 years</td></tr>
<tr><td colspan="2">2.2 Secret - Maximum access restriction of 15 years</td></tr>
<tr><td colspan="2">2.3 Ultra-secret- 25 years access restriction period, extendable only once, and for a period not exceeding 25 years, limited to a maximum of 50 years for the total term of the classification.</td></tr>
<tr><td rowspan="8">3. CONFIDENTIALITY PROTECTED BY SPECIFIC LEGISLATION (the legal hypotheses for restricting access to information listed in this item are not exhaustive)</td><td colspan="2">3.1 Confidentiality Arising from Personality Rights</td></tr>
<tr><td rowspan="5"></td><td>3.1.1 Fiscal Secrecy</td></tr>
<tr><td>3.1.2 Bank Secrecy</td></tr>
<tr><td>3.1.3 Commercial Secrecy</td></tr>
<tr><td>3.1.4 Business Secrecy</td></tr>
<tr><td>3.1.5 Accounting Secrecy</td></tr>
<tr><td colspan="2">3.2 Confidentiality of Processes and Procedures</td></tr>
<tr><td></td><td>3.2.1 Confidentiality of the Disciplinary Administrative Procedures in Progress</td></tr>
</table>

		3.2.2 Confidentiality of the Police Inquiry
		3.2.3 Secrecy of Justice in Civil Proceedings
		3.2.4 Secrecy of Justice in Criminal Proceedings
	3.3 Heritage Information	
		3.3.1 Trade Secret
		3.3.2 Copyright
		3.3.3 Computer Program Intellectual Property
		3.3.3 Industrial Property
4. Personal	4.1 Personal – Maximum period of access restriction 100 years, regardless of confidentiality classification and when referring to the intimacy, private life, honor and image of people.	