INSTITUTIONAL SECURITY CABINET OF THE PRESIDENCY OF THE REPUBLIC

NORMATIVE INSTRUCTION GSI/PR No. 3, OF MAY 28, 2021.

Dispose about the procedures related to the management of information security in the bodies and in entities of federal public administration.

THE STATE MINISTER HEAD OF THE INSTITUTIONAL SECURITY CABINET OF THE PRESIDENCY OF THE REPUBLIC, in the use of the attribution conferred on it by art. 87, single paragraph, item II, of the Constitution, and in view of the disposal in the art. 10, items IV and V, of Law No. 13,844, of July 18, 2019, in the art. 12 of the Decree No. 9,637, of December 26, 2018, and in the Decree No. 9,668, of January 2, 2019, solve:

Art. 1 To approve the procedures related to the management of information security in the bodies and entities of the federal public administration.

CHAPTER I

PRELIMINARY PROVISIONS

Art. 2 The present Normative Instruction deals with the processes related to information security management that must be observed by the bodies and entities of the federal public administration in the planning and implementation of their actions referring to information security.

§ 1 The concepts related to the subject of this Normative Instruction may be consulted in the information security glossary, approved and updated by an ordinance of the Institutional Security Cabinet.

§ 2 The information security management must be maintained and implemented continuously, seeking to maintain alignment with the evolution of technology e its risks, identifying internal and external factors that may impact the achievement of the objectives of the body or the entity.

§ 3 The procedures related to the information security management must be aligned with the internal management controls of the body or entity.

Art. 3 The information security management is going to be formed by the following mandatory realization procedures by the bodies and entities of public federal administration:

I – information assets mapping;

II – information security management;

III – management of continuity of business in information security;

IV – management of changes in information security aspects; and

V – evaluation of compliance of information security.

CHAPTER II

INFORMATION ASSETS MAPPING

Art. 4 The information asset mapping process aims to structure and maintain a record of information asset, dedicated to subsidize the management of risks procedures, the management of continuity and the management of changes in information security related aspects.

Art. 5 The information asset mapping process must consider, preliminarily:

I – the strategical goals of the organization;

II – the internal procedures of the organization;

III – the legal requirements; and

IV – the structures of the body or entity.

Art. 6 The record of information asset resultant of the process of information asset mapping must contain:

I – those responsible – owners and custodians – for each information asset;

II – basic information about the information security requirements of each information asset;

III – the containers of each information asset;

IV – the interfaces of each information asset and its interdependencies in between them;

Art. 7 The information asset record must be approved by the body or the entity holder's act.

Art. 8 It is incumbent upon the information security manager of each body or entity to coordinate the information asset mapping procedure, as well as assign an agent responsible for the information asset management, among the effective employees of the body nor the entity.

Art. 9 It is incumbent upon the agent responsible for the information asset management:

I – to identify and to classify the information assets by criticality level;

II – to identify potential threats to the information assets;

III – to identify vulnerabilities in information assets;

IV – to consolidate resultant information of the information security level analysis of each information asset or of groups of information assets in a report;

V – to authorize the update of the report mentioned in the item IV of the caption; and

VI – to evaluate the risks of the information assets or of groups of information assets;

CHAPTER III

MANAGEMENT OF RISKS OF INFORMATION SECURITY

Art. 10 The information security risk management process aims to direct and control the risk of information security, in order to adequate it to acceptable levels to the body or entity.

Art. 11 The information security risk management process must be aligned with the institutional model for risk management, compatible with the mission and the strategical objectives of the body or the entity, besides considering, preliminarily:

I – the institutional internal processes;

II – the legal requirements;

III – the information security policy of the body or the entity;

IV – the management policy of institutional risks, in case it exists; and

V – the structure of the body or the entity.

Art. 12 The information security risk management process shall provide to the organization the following documents:

I – the information security risk management plan;

II – report of identification, information security risk analysis and evaluation; and

III – information security risk treatment report;

Art. 13 The information security risk management plan must contain, at least:

I – the risks management implementation coverage, setting out its action scope and the information assets that will be object of treatment;

II – the methodology to be used shall include, at least, risk assessment and acceptance criteria;

III – risks types;

IV – the severity level of risks;

V – a template for the information security risk identification, analysis and assessment report with the necessary guidelines for its preparation; and

VI – a template for the information security risk treatment report with the necessary guidelines for its preparation.

§ 1 The information security risk management plan must be regularly reviewed, in order to keep the risks of information security updated.

§ 2 The process of implementing the information security risks management plan shall consider, among other aspects, the recommendations of changes in relation to risk acceptance criteria,

the implementation of the project coverage, the security information action and the predicted activities of risks treatment.

Art. 14. The information security risk identification, analysis and assessment report shall be prepared based on the model established by the information security risk management plan and shall contain at least:

I – the associated risks to each information asset, considering the involved threats, the existing vulnerabilities and the already implemented information security actions;

II – the level of severity of identified risks, considering the values or the levels of risk occurrence probability and the consequences of the risk occurrence (integrity loss, availability, reliability or authenticity in involved assets);

III – the occurred information security events, with security actions description, and possible consequences for the body or the entity;

IV – changes in risk factors, and

V – changes related to evaluation and analysis criteria.

§ 1º The identification, analysis and evaluation report of the information security risks must be updated annually and whenever happen any modifications in some of the risk factors or in some internal or external context, with the obligation of posteriorly sent to the information security manager to approval.

§ 2º It is understood as internal and external context the conjunct of events that could influence the organization's capacity to get their strategic goals.

Art. 15 The treatment of information security risks report must be resultant of the identification, analysis and evaluation information security risks report.

§ 1º The treatment of information security risks report must consider the possibilities of treatment to each identified risk.

§ 2º To each possibility of treatment detected in function of identified risk, must be observed, as far as proper:

I – the information security action efficiency.

II – the technical restraints;

III – the physics structural restraints;

IV – the operational restraints;

V – the organizational restraints;

VI – the legal requirements; and

VII – the cost-benefit relation.

§ 3º The report of treatment of information security risks must be made based on the model established by the risk management plan and must contain, at least:

I – the definition and prioritization of security actions and the activities of risks treatment must be carried out;

II –those responsible for the execution and monitoring of security actions and treatment risks activities;

III – the deadlines for the execution of security actions and risks treatment activities; and

IV - prioritized risk treatment options.

Art. 16 The information security manager of each body or entity is responsible for:

I – coordinating the information security risks management;

II responsible for the information security risks management among the effective employees of the agency;

III – approving the information security risks management plan;

IV – approving the identification, analysis and evaluation report of information security risks and send it to senior management;

V – approving the treatment of information security risks report;

VI – proposing preventive measures to the senior management;

Art. 17 It is incumbent upon the agent responsible for the information security risks management to prepare:

I – the information security risks management plan;

II – the identification, analysis and evaluation report of information security risks; and

III – the information security risks treatment report.

CHAPTER IV

MANAGEMENT OF BUSINESS CONTINUITY IN INFORMATION SECURITY

Art. 18 The implementation of business continuity management in information security aims to minimize the impacts due to failures, disasters or significant unavailability about the activities of the body or entity in this area, besides recovering information assets losses in an acceptable level, through incidents response actions and disaster recovery.

Art. 19 The business continuity management process in information security must be based on continuity strategies for the critical activities, on the risks evaluation collected in the risks management process and on institutional guidelines about the business continuity management.

Art. 20 The institutional guidelines about the subject must be formalized by the body or entity, contemplating, at least, the following aspects:

I – accordance with the mission of the body or entity, considering its structure, business nature and its complexity, so that the policy reflects the institutional culture and environment;

II – clear commitment related to legal and regulatory obligations and to continuous improvement of the business continuity management in information security;

III – definition of the coverage and boundaries of the business continuity management in information security;

IV – identification of any authorities of the body or entity and required delegations, including the ones responsible for the business continuity in the institution;

V – criteria for the type and scale of the incidents to be handled;

VI – references to the standards, regulations or policies which the process should consider or comply with; and

VII – commitment to carry out and maintain the institution's business continuity.

Art. 21 The business continuity management process in information security must be composed by a plan of continuous business in information security, which will observe the provisions of the report on identifying, analyzing and assessing information security risks and the priority of recovering business processes.

Art. 22 The business continuity in information security aims to define how the incident management will be accomplished in case of disasters or other business operations interruptions and how the activities should be recovered within the established deadlines.

Art. 23 The business continuity in information security plan shall contain, at least:

I – the objective;

II – critical activities of business to be contemplated the plan;

III – the requirements for the plan activation, especially, the maximum time in the failure continuity;

IV – the responsible one(s) for the plan activation, with their respective contacts details;

V – the responsible one(s) for applying the defined contingency measures, with each employee having responsibilities formally defined and nominally assigned, including their respective contacts details; and

VI – the definition:

a) of the needed actions for measure operationalization which implementation depends on the purchase of physical and/or human resources;
b) of the decision limits for those responsible agents for the implementation of contingency measures in the face of unexpected situations;
c) of the parameters for ending the plan and returning to normality;

d) of the responsible for those action, including their contacts details;
e) of the way in which this process is monitored;
f) and of a run test simulation script and the form of its application.

Single paragraph. The business continuity plan must be tested regularly, with intent to document their results and might ensure their effectiveness in case of activation need.

Art. 24. The business continuity plan review must be carried out:

I – at least, once a year;

II – depending of the functionality tests results realized, once proven the validation and efficiency loss of the adopted measures faced with new situations;

III – after significant change in the information assets, on the activities or in some of their components.

Art. 25. The information security manager will coordinate the process of business continuity management in information security and their respective bodies or entities, as well as designate an agent responsible for the referred management, among the effectives employed of the body.

Art. 26. The persons responsible for the process or the holders of the units in which critical activities are identified are responsible for the following attributions:

I – proposing the guidelines to be contemplated on the business continuity plan in information security;

II – elaborating the business continuity plan in information security;

III – carrying out the functionality test of this plan;

IV – evaluating and improving this plan from the functionality tests results;

V – managing the contingency when the activities interruption occur, based on this developed plan.

VI – proposing the necessary resource to the implementation and the development of actions related to continuity of the activities, as well as to the realization of the functionality test of this plan.

Art. 27. It is incumbent upon the agent responsible for the business continuity management in information security:

I – to advise those responsible for the process or the holders of the units in which critical activities are identified on the attribution described in the art. 26;

II – to evaluate the business continuity plan in security information and propose changes, when applicable;

III – to supervise the implementation, the functionality tests and the updating of this plan;

IV – to propose improvements in the implementation of new controls referring to the business continuity plan in information security.

V – to participate in the analysis preparation in the business impact; and

VI – propose measures aimed at developing a culture of business continuity management in information security.

CHAPTER V

MANAGEMENT OF CHANGES IN ASPECTS OF INFORMATION SECURITY

Art. 28. The implementation of the change management process in the aspects of information security aims to prepare and adapt the bodied and entities of the federal public administration to the changes arising from the process and information technology development, aiming for the obtainment of effective and efficient changes and the mitigation of any resistances.

§ 1º The process of management of changes in the aspects of information security must be supported by the information collected by the identification, analysis and assessment of information security risks report and by the information security risks treatment report.

§ 2º The process mentioned on the **caption**, in addition to promoting the planned changes control, must consider the critical analysis of the unforeseen changes consequences, acting to mitigate the adverse effects.

Art. 29. For the purposes of this Normative Instruction, the change will be classified as:

I – emergencies: unforeseen changes of high impact that occur, commonly, in function of due to:

a) serious incidents or modification in risk factors with a high impact on the organization's process;
b) normative change for immediate application;
c) need for immediate significant changes on the information assets; and
d) other similar events;

II – routine: changes in which the technical team already has a high degree of knowledge and insight necessary to carry out the activity and which, generally, due to:

a) information technology infrastructure update;
b) information technology services with regular periodicity that imply changes in one or more security aspects; and
c) other similar events;

III – proactive: change that seek to bring greater efficiency to the organization and usually occurs due to:

a) expansion of the computational park;
b) foreseen obsolescence of process and equipment;
c) need to adopt new technologies ; and
d) other similar events.

Art. 30. The management changes in the aspects of information security must be constituted, at least, by the following instruments:

I – change description document; and

II – change assessment and approval document.

Art. 31. The change description document aims to identify the type of change intended, in order to adapt the organization to changes in the internal and external contexts. Single paragraph. The holders of the units requesting the change are responsible for the preparation and approval of the document mentioned in the **caption**, which should be sent to the agent responsible for managing changes in the aspects of information security.

Art. 32. The change description document must contain, at least:

I – plaintiff agent;

II – unit of origin;

III – description of change;

IV – type of change;

V – objective(s) of the change with the factors that led to this need; and

VI – expected benefits.

Art. 33. The change assessment and approval document is intended to:

I – analyze the required changes;

II – recommend which changes should be approve;

III – suggest alternatives for implementing the changes.

Art. 34. The change assessment and approval document must contain, at least:

I – alternatives for implementing the change, with the basic description of the procedures necessary for its execution;

II – recommendations, in a priority order, which alternatives to be adopted;

III – relationship between the intended change and another changes that, eventually occur simultaneously;

IV – analysis of the risks of information assets that will be affected by the change;

V – assessment of the impact of postponing the change;

VI - definition of the alternative to be implemented or rejection of the change proposed by the senior management of the body or entity; and

VII - critical analysis of the consequences of unforeseen changes and proposed actions to mitigate any negative consequences.

Art. 35. It is incumbent upon the information security manager, related to the process of change management in the aspects of information security:

I – to coordinate the change management;

II – to designate the agent responsible for the change management, among the effective employees of the bodies;

III – to analyze and forward the change assessment and approval document for consideration by the body's senior management, which is responsible for the decision to approve or reject the change; and

IV – to provide the constant interaction between the teams of management changes in the aspects of information security, of information security risk management and of business continuity management in information security.

Art. 36. It is incumbent upon the agent responsible for the management changes in the aspects of information security:

I – recommending to senior management the creation of a technical change group, composed of servers from the affected areas and from the information security area, to prepare the change assessment and approval document;

II – prepare, together with the technical change group, the change assessment and approval document and submit it to the manager of information security for analysis;

III – monitor, together with the technical change group, the tests of the change approved by the change assessment and approval document;

IV – monitor, together with the technical change group, the implementation of the solution approved in the change assessment and approval document;

V – ensure, together with the technical change group, the registry audit containing all the relevant information related to the change; and

VI – inform the information security manager about the progress and conclusion of the process.

CHAPTER VI

ASSESSMENT CONFORMITY IN THE ASPESCTS OF INFORMATION SECURITY

Art. 37 The conformity assessment in information security aspects is to provide an adequate level of trust to a given process by meeting requirements defined in applicable policies, procedures, norms or technical regulations.

Art. 38 The conformity assessment process in the aspects of information security must be composed, at least, of the following documents:

I – compliance verification plan; and

II – conformity assessment report.

Art. 39 The compliance verification plan must contain, at least:

I – the units to be covered;

II – the aspects to be observed for compliance verification;

III – the actions and activities to be carried out;

IV – the documents necessary to substantiate the compliance verification; and

V – the responsibilities.

Art. 40 The conformity assessment report must contain, at least:

I - the details of the actions and activities carried out with the identification of the person responsible for the analysis;

II – the compliance report; and

III – the recommendations.

§1 The non-conformities identified in the assessment report must be dealt with in a procedure that allows for the monitoring of the adopted solutions and that is defined by the bodies or entity.

§2 The process mentioned in the §1 may be a constituent part of the information security risks management mentioned in Chapter III of this Normative Instruction, if the identified non-compliances are considered as a risk to the institution.

Art. 41. It is incumbent upon the senior administration of the body or entity:

I – to review and approve the compliance assessment report and forward it to the information security manager; and

II – to promote training actions for the agents responsible for compliance assessment, aiming at improving their knowledge about current legislation on information security.

Art. 42. It is incumbent upon the information security manager, with respect to the conformity assessment in the aspects of information security:

I – to coordinate the compliance assessment in the aspects related to information security;

II – to designate, from among the effective employees of the body, one or more agents responsible for the compliance assessment, according to the aspects related to information security, and these may not be any of the members of the information security management team of the body or entity;

III – to provide, to the agent(s) responsible for the compliance assessment, all of the information necessary for the compliance management process in the aspects of information security;

IV – to analyze the compliance assessment report and submit it for consideration and approval of the senior administration;

V – to adopt the necessary measures to attend the recommendations of the compliance assessment report approved by the senior administration;

Art. 43 It is incumbent upon the agent(s) responsible for the conformity assessment:

I – to prepare the compliance verification plan;

II – to prepare the report of compliance assessment and send it to the senior administration of the body; and

III – to verify the adequacy of information security procedures in accordance with the recommendations described in the compliance assessment report.

CHAPTER VII
GENERAL DISPOSALS

Art. 44 The processes mentioned in this Normative Instruction must comply with the Normative Instruction No01, May 27, 2020, of the Institutional Security Cabinet of the Presidency of the Republic.

Art. 45 The bodies and entities of the federal public administration must adopt the processes described in this present Normative Instruction, as well as contemplating it in its institutional strategical planning the information security management.

Single Paragraph. In order to comply with the provisions of the **caption**, the bodies and entities of the federal public administration must define their own actions plans, with activities, deadlines and those responsible for implementing the processes of information security management, as described in this Normative Instruction.

Art. 46 It is incumbent upon the bodies and entities of the federal public administration:

I – appoint at least one substitute in the positions provided for in this Normative Instruction, so that they can act in case of impediment or absence of the holder; and

II – to allocate budget resources to carry out the Information Security actions provided in this Normative Instruction.

CHAPTER VIII

FINAL AND TRANSITIONAL DISPOSALS

Art. 47 The following normative acts of the Institutional Security Cabinet of the Presidency of the Republic are hereby revoked, as established in art. 7, item I, of the Decree nº 10.139, November 28th 2019:

I – Ordinance nº 62, November 19th 2009;

II – Ordinance nº 7, February 7th 2012;

III – Ordinance nº9, February 7th 2012;

IV – Ordinance nº10, February 7th 2012; and

V – Ordinance nº2, February 15th 2013.

Art. 48 This Normative Instruction enter in force on July 1, 2021.

This text does not replace the one published in the DOU of 05/28/2018