# OFFICIAL DIARY OF THE UNION

Published: 07/19/2021 | Edition: 134 | Section: 1 | Page: 2

**Body: Acts of the Executive Power**

## DECREE NO. 10. 748, OF JULY 16, 2021

Establishes the Federal Cyber Incident Management Network.

**THE PRESIDENT OF THE REPUBLIC**, in the use of the attribution conferred on him by art. 84, caput, item VI, point "a", of the Constitution,

**DECREES:**

CHAPTER I

THE FEDERAL CYBER INCIDENT MANAGEMENT NETWORK

Art. 1 The Federal Cyber Incident Management Network is hereby established, in accordance with the provisions of item VII of the caput of art. 15 of Decree No. 9,637, of December 26, 2018.

§ 1 The participation of public bodies and entities of the direct, autarchic and foundational federal public administration in the Federal Cyber Incident Management Network will be mandatory.

§ 2 The participation of public companies and federal mixed-economy companies and their subsidiaries in the Federal Cyber Incident Management Network will be voluntary and will take place through adhesion.

§ 3 The Secretariat for Digital Government of the Special Secretariat for Debureaucratization, Management and Digital Government of the Ministry of Economy will participate in the Federal Cyber Incident Management Network as the central body of the System of Administration of Information Technologies Resources - Sisp of the Federal Executive Branch.

Art. 2 The Federal Cyber Incident Management Network aims to improve and maintain coordination between public bodies and entities of the direct, autarchic and foundational federal public administration for the cyber incident prevention, handling and response in order to raise the level of cybersecurity resilience of your information assets.

Art. 3 The following are objectives of the Federal Cyber Incident Management Network:

I - to disseminate measures to prevent, treat and respond to cyber incidents;

II - to share alerts about cyber threats and vulnerabilities;

III - to disseminate information about cyber attacks;

IV - to promote cooperation between Network participants; and

V - to promote speed in responding to cyber incidents.

Art. 4 For the purposes of the provisions of this Decree, it is considered:

I - cyber incident prevention, treatment and response team - group of public agents with the responsibility of providing cybersecurity-related services for the public body or entity of the federal public administration, in compliance with the information security policy and information security risk management processes of the public body or entity;

II - sector coordination team - cyber incident prevention, treatment and response team of regulatory agencies, the Central Bank of Brazil or the National Nuclear Energy Commission or their regulated entities responsible for coordinating cybersecurity activities and to centralize the notifications of incidents from other teams in the regulated sector;

III - main teams - the prevention, treatment and response teams to cyber incidents of entities, public or private, responsible for information assets, in particular those relating to essential services, the interruption or destruction of which, in whole or in part, causes serious social, environmental, economic, political or international impact or a serious impact to the national or to the society security, in accordance with the provisions of item I of the single paragraph of art. 1 of the Annex to Decree No. 9,573 of November 22, 2018;

IV - priority areas - areas defined in the National Critical Infrastructure Security Plan for the application of the National Critical Infrastructure Security Policy, in accordance with the provisions of item I of the **caput** of art. 9 of the Annex to Decree No. 9,573 of 2018;

V - cyber incident - occurrence that compromises, actually or potentially, the availability, integrity, confidentiality or authenticity of the information system or the information processed, stored or transmitted by that system, which may also be characterized by the attempt to exploit information system vulnerability that violates a rule, security policy, security procedure or usage policy;

VI - cyber incident management plan for the federal public administration - plan that guides the teams of the public bodies and entities of the direct, autarchic and foundational federal public administration, except for regulatory agencies, the Central Bank of Brazil and the National Nuclear Energy Commission, on the coordination of activities related to the prevention, treatment and response to cyber incidents; and

VII - sector cyber incident management plans - plans that guide teams in regulatory agencies, the Central Bank of Brazil, the National Nuclear Energy Commission or in their regulated entities on the coordination of activities related to cyber incidents prevention, treatment and response inherent to the specific sector.

CHAPTER II

COMPOSITION

Art. 5 The Federal Cyber Incident Management Network will comprise the Institutional Security Cabinet of the Presidency of the Republic, by the public bodies and entities of the direct, autarchic and foundational federal public administration and, subject to the provisions of § 2 of art. 1, by public companies and mixed-economy companies and by their subsidiaries that join the Network.

§ 1 The Information Security Department of the Institutional Security Cabinet of the Presidency of the Republic will coordinate the Federal Cyber Incident Management Network through the Cyber Incident Prevention, Handling and Response Center of Brazilian Government.

§ 2 The public bodies and entities of the direct, autarchic and foundational federal public administration will act in the Federal Cyber Incident Management Network through their for the cyber incident prevention, treatment and response teams, in accordance with the provisions of items I to III of the **caput** of art. 4.

§ 3 Having observed the state's interest in national cybersecurity, other public or private entities may be invited by the Institutional Security Cabinet of the Presidency of the Republic to join the Federal Cyber Incident Management Network, through official letter, provided that they have been complied with the requirements of art. 7.

Art. 6 Within the scope of the Ministry of Defense and Armed Forces, the articulation with the Cyber Incident Prevention, Handling and Response Center of Brazilian Government will be made primarily through the sector coordination team, operated by the Cyber Defense Command, as the central body of the Military Cyber Defense System.

§ 1 Exceptionally, the cyber incident prevention, treatment and response teams of the Ministry of Defense and Armed Forces will be able to articulate directly with the Cyber Incident Prevention, Handling and Response Center of Brazilian Government, in which case they must inform the Ministry of Defense's sector coordination team.

§ 2 The information shared by the cyber incident prevention, treatment and response teams referred to in § 1 with the Cyber Incident Prevention, Handling and Response Center of Brazilian Government will observe the legal restrictions on data access due to State security needs.

Art. 7 The adhesion of the entities of which § 2 of art. 1 shall be formalized by the act of the highest authority of the direct federal public administration body to which they are bound or subordinated.

§ 1 When preparing the act dealing with the **caput**, the direct federal public administration body will assess whether there is a need to provide additional requirements to the information security regulations established by the Institutional Security Cabinet of the Presidency of the Republic as a result of the activities carried out

by the entities of which § 2 of art. 1, especially when these activities are related to critical infrastructure.

§ 2 The entities referred to in § 2 of art. 1 that apply for access to the Federal Cyber Incident Management Network must comply with the following requirements to be approved by the Institutional Security Cabinet of the Presidency of the Republic:

I - to have a cyber incident prevention, treatment and response team implemented in accordance with the information security regulations established by the Institutional Security Cabinet of the Presidency of the Republic; and

II - to refer to the Institutional Security Cabinet of the Presidency of the Republic, through its cyber incident prevention, treatment and response team or its sector coordination team, a term of adhesion to the Federal Cyber Incident Management Network signed by the highest authority of the organization or its legal representative.

§ 3 The adhesion to the Federal Cyber Incident Management Network will depend on the formal approval by the Institutional Security Cabinet of the Presidency of the Republic, which may reasonably refuse it, even if the requirements established in this article have been met.

§ 4 The provisions of this article shall apply, as it may be, to other legal entities of private law and to legal entities of domestic public law from other Powers and federative entities that are invited by the Institutional Security Cabinet of the Presidency of the Republic to join the Federal Cyber Incident Management Network.

§ 5 The spontaneous collaboration, on a case-by-case basis, of the entities of which § 2 of art. 1 with the Cyber Incident Prevention, Handling and Response Center of Brazilian Government or any of its members will not depend on the adhesion to the Federal Cyber Incident Management Network.

Art. 8 Legal entities that do not belong to the direct, autarchic and foundational federal public administration and that have signed a term of adhesion with the Institutional Security Cabinet of the Presidency of the Republic to integrate the Federal Cyber Incident Management Network must report to the sector coordination team to which they are linked or, in their absence, directly to the Cyber Incident Prevention, Handling and Response Center of Brazilian Government, in the event of:

I - cyber incident that exceeds its ability to remedy it; and

II - vulnerability in information assets that your cyber incident prevention, treatment and response team deems that may cause a cyber incident, both on your computer network and on that of other entities.

Art. 9 The departure of the legal entity referred to in § 4 of art. 7 of the Federal Cyber Incident Management Network will take place:

I - at the request of its highest authority of the organization; or

II - by decision of the Institutional Security Cabinet of the Presidency of the Republic, in the event of:

a) failure to comply with the requirements of art. 7;

b) failure to comply with the provisions of the sector cyber incident management plan; or

c) administrative convenience.

CHAPTER III

THE POWERS

Art. 10. It is the responsibility of the Institutional Security Cabinet of the Presidency of the Republic:

I - to coordinate the Federal Cyber Incident Management Network; and

II - to convene a meeting of the Chamber of Foreign Affairs and National Defense of the Council of Government to deliberate on the occurrence of a major cyber incident or when to identify an high cyber risk, in accordance with the provisions of Decree No. 9819, of June 3, 2019.

Art. 11. It is the responsibility of the Information Security Department of the Institutional Security Cabinet of the Presidency of the Republic, through the Cyber Incident Prevention, Handling and Response Center of Brazilian Government:

I - to coordinate the activities of the cyber incident prevention, treatment and response teams members of the Federal Cyber Incident Management Network related to prevention, treatment and response to cyber incidents;

II - to connect with the cyber incident prevention, treatment and response team referred to in item I using a dedicated computing platform to coordinate them;

III - to create, update and publish the cyber incident management plan for public bodies and entities of the direct, autarchic and foundational federal public administration;

IV - to interact with counterpart organizations from other countries;

V - to seek international cooperation, with an emphasis on sharing information about cyber threats, vulnerability and incidents;

VI - to share alerts, recommendations and statistics related to cyber incidents to members of the Federal Cyber Incident Management Network; and

VII - to keep updated the website of the Cyber Incident Prevention, Handling and Response Center of Brazilian Government with alerts, recommendations and statistics about cyber incident, subject to the provisions of art. 15.

Art. 12. It is responsibility of the public bodies and entities of the direct, autarchic and foundational federal public administration:

I - to institute and implement its cyber incident prevention, treatment and response teams, in accordance with the provisions of item VII of the **caput** of art. 15 of

Decree No. 9,637 of 2018, and information security regulations established by the Institutional Security Cabinet of the Presidency of the Republic;

II - to support the activities of its cyber incident prevention, treatment and response teams and information security actions, in accordance with provisions of art. 15 of Decree No. 9,637 of 2018;

III - to identify the main teams of the priority areas under their responsibility, in accordance with the provisions of items III and IV of the **caput** of art. 4;

IV - to notify immediately the Cyber Incident Prevention, Handling and Response Center of Brazilian Government, through its cyber incident prevention, treatment and response teams about the existence of vulnerabilities or cybersecurity incidents that impact or may impact the services provided or contracted, in accordance with the provisions of art. 17 of the Decree No. 9,637 of 2018;

V - to require directly to the identified main teams, or through the sector coordination team, when established, notifications about cyber incidents of biggest impact;

VI - to notify the Cyber Incident Prevention, Handling and Response Center of Brazilian Government, directly or through the sector coordination team, when established, regarding the cyber incidents of biggest impact, based on information obtained from the cyber incident prevention, treatment and response teams of the entities under their management;

VII - to promote training and professionalization actions of their cyber incidents prevention, treatment and response teams, in accordance with the provisions of art. 15 of Decree No. 9,637 of 2018;

VIII - to keep updated the infrastructure used by its cyber incident prevention and treatment and response teams; and

IX - to remedy urgently cyber vulnerabilities, in particular those identified in the alerts and recommendations issued by the Cyber Incident Prevention, Handling and Response Center of Brazilian Government.

§ 1 The cyber incidents of biggest impact referred to in items V and VI of the **caput** shall be established based on the severity classification contained in the information security risk management process of the public body or entity.

§ 2 The provisions of this article also apply to regulatory agencies, to the Central Bank of Brazil and the National Nuclear Energy Commission.

Art. 13. It is responsibility of the regulatory agencies, the Central Bank of Brazil and the National Nuclear Energy Commission:

I - to establish or to designate a sector coordination team, in accordance with the provisions of item II of the **caput** of art. 4;

II - to support the activities of its cyber incident prevention, treatment and response teams, in accordance with the provisions of Decree No. 9,637 of 2018;

III - to identify the main teams of the priority areas under their regulation, in accordance with the provisions of item III and IV of the **caput** of art. 4;

IV - to require the notifications from the main teams identified, through the sector coordination team, about cyber incidents of biggest impact;

V - to notify the Cyber Incident Prevention, Handling and Response Center of Brazilian Government, through the sector coordination team, regarding cyber incidents of biggest impact, based on information obtained from the cyber incident prevention, treatment and response teams of the entities under their regulation;

VI - to analyze the cyber risks that should be included in the specific sector cyber incident management plan;

VII - to establish their form of coordination with the sector coordination team;

VIII - to identify other entities, public or private, relevant to cybersecurity in your priority area;

IX - to provide information on the cyber incident prevention, treatment and response teams of the entities referred to in item VIII, which shall be included in the sector cyber incident management plan; and

X - to identify the critical infrastructure in their priority areas that require attention in terms of national cybersecurity.

§ 1 The cyber incidents of biggest impact referred to in items IV and V of the **caput** shall be established based on the severity classification contained in the information security risk management process of the public body or entity.

§ 2 The Cyber Incident Prevention, Handling and Response Center of Brazilian Government will publish the basic elements and the frequency of updating the sector cyber incident management plan referred to in items VI and IX of the **caput** on its website.

§ 3 The provisions of this article also applies to other bodies and entities of the direct, autarchic and foundational federal public administration with regulatory competence in a priority area that may be established in the National Critical Infrastructure Security Plan, within a period of up to eighteen months, counted from the date of notification by the Institutional Security Cabinet of the Presidency of the Republic, for the public body or entity to implement the necessary actions.

Art. 14. It is responsibility of the sector coordination teams:

I - to develop the sector cyber incident management plan referred to in item VI of the **caput** of art. 13; and

II - to coordinate activities and centralize incidents notifications received from the other cyber incident prevention, treatment and response teams of the entities under their coordination.

Single paragraph. It is also the responsibility of the sector coordination teams to comply with the provisions of the information security regulations established by the Institutional Security Cabinet of the Presidency of the Republic, that regulate the cyber incidents prevention, treatment and response teams.

CHAPTER IV

FINAL AND TRANSITIONAL PROVISIONS

Art. 15. Specific information on cyber incidents and on the technical configurations and characteristics of information assets of each public body or entity of the direct, autarchic and foundational federal public administration are considered essential for the security of society and the State.

§ 1 The information referred to in the **caput** may only be accessed by professionals authorized by the authorities responsible for the information assets of the public bodies or entities of the direct, autarchic and foundational federal public administration.

§ 2 The Cyber Incident Prevention, Handling and Response Center of Brazilian Government will publish on its website general public interest statistics related to cyber incidents that occurred in the public bodies and entities of the direct, autarchic and foundational federal public administration.

Art. 16. The actions foreseen for the operation of the Federal Cyber Incident Management Network under responsibility of the public bodies and entities referred to in art. 13 that include the institution or the designation of sector coordination teams shall be implemented within a period of eighteen months, counted from the date of publication of this Decree.

Art. 17. The public bodies and entities of the direct, autarchic and foundational federal public administration referred to in § 1 of art. 1 shall implement the actions foreseen for the operation of the Federal Cyber Incident Management Network within a period of one year, counted from the date of publication of this Decree.

Art. 18. This Decree comes into force on the date of its publication.

Brasília, July 16, 2021; 200th of Independence and 133rd of the Republic.

**JAIR MESSIAS BOLSONARO**
*Augusto Heleno Ribeiro Pereira*