**URGENCY DECREE**
**No. 007-2020**
**URGENCY DECREE THAT APPROVES THE DIGITAL TRUST FRAMEWORK AND PROVIDES MEASURES FOR ITS STRENGTHENING**

THE PRESIDENT OF THE REPUBLIC

CONSIDERING:

That, in accordance with Article 135 of the Political Constitution of Peru, during the parliamentary interregnum, the Executive Power legislates through emergency decrees of which it reports to the Permanent Commission so that it examines them and raises them to Congress, once it is installed;

That, through Supreme Decree No. 165-2019-PCM, Supreme Decree that dissolves the Congress of the Republic and calls elections for a new Congress, revoked the parliamentary mandate of the congressmen, keeping the Permanent Commission in office;

That, through Legislative Decree No. 1412, Legislative Decree that approves the Digital Government Law, a governance framework of digital government is established for the adequate management of digital identity, digital services, digital architecture, interoperability, digital security and data, as well as the legal regime applicable to the use cross-cutting of digital technologies in the digitization of processes and provision of digital services by Public Administration entities in the three levels of government;

That, article 30 of the aforementioned Legislative Decree defines Digital Security as the state of trust in the digital environment that results from the management and application of a set of proactive and reactive measures against the risks that affect the security of people, economic and social prosperity, national security and the national objectives in that environment. It is based on the articulation with actors from the public sector, private sector and others who support the implementation of controls, actions and measures;

That, likewise, article 33 of the aforementioned Legislative Decree establishes that Information Security focuses on information, independently of its format and support. Digital security deals with the security measures of the information processed, transmitted, stored or contained in the digital environment, trying to generate trust, managing the risks that affect the safety of people and economic and social prosperity in said environment;

That, through Supreme Decree No. 237-2019-EF, the National Competitiveness and Productivity Plan is approved, which presents a set of consensual measures between the public and private sectors with a view to establishing a favorable and competitive environment that allows generating well-being for all Peruvians based on a sustainable economic growth with a territorial approach;

That, from the aforementioned National Plan, it is understood that digital technologies have a strategic value to reduce gaps, promote innovation and support in the growth of the country; Furthermore, it points out that the technological changes that today's world is going through would be much easier to adopt if we made a digital transformation throughout the country;

That, through Supreme Decree No. 086-2015-PCM, the actions, activities and initiatives developed within the framework of the process of Peru's link with the Organization for Economic Cooperation and Development (OECD) and implementation of the Country Program, in this line, the Recommendations for the Management of Digital Security Risks made by the OECD, among which the importance of the establishment of Security Teams is pointed out. Responses to Digital Security Incidents at the State level;

That, in the document Digital Government in Peru "Working with citizens" the OECD indicates as a recommendation that the Peruvian State should "consider establish a National Center for Digital Security "that seeks to articulate actions with the relevant actors to manage digital security incidents and strengthen the confidence;

That, digital trust is a state that emerges as a result of how truthful, predictable, secure and reliable are the digital interactions that are generated between people, companies, public entities or things in the digital environment. Digital trust is a component of Digital Transformation and its scopes are the data protection, transparency, digital security and consumer protection in the digital environment;
That, in view of this as part of our linking process, it is necessary to dictate measures regarding trust and digital security, establishing the mechanisms collaboration and articulation with public and private actors and civil society in the digital environment, through a systemic and comprehensive approach that ensures the strengthening of trust in digital services by people, entities and society in general;
In use of the powers conferred by article 135 of the Political Constitution of Peru;

With the approving vote of the Council of Ministers; Y,

In charge of reporting to the Permanent Commission to examine it and raise it to Congress, once it is installed:

DECREE:

## CHAPTER I

## GENERAL DISPOSITION

**Article 1. Purpose**
The purpose of this Emergency Decree is to establish the measures that are necessary to guarantee the trust of people in their interaction with digital services provided by public entities and private sector organizations in the national territory.

**Article 2. Scope**
The rules and procedures that govern the matter of Digital Trust are applicable to the entities established in article I of the Preliminary Title of the Sole Text Ordered by Law No. 27444, Law of General Administrative Procedure, approved by Supreme Decree No. 004-2019-JUS, and, to the organizations of the civil society, citizens, companies and academia.

**Article 3. Definitions**
For the application of this Emergency Decree, the following definitions are established:

a) Digital Trust.- It is the state that emerges as a result of how truthful, predictable, ethical, proactive, transparent, secure, inclusive and reliable are the digital interactions that are generated between people, companies, public entities or things in the digital environment, with the purpose of promoting the development of the digital economy and digital transformation. It is a component of the digital transformation and its scopes are the protection of personal data, ethics, transparency, digital security and consumer protection in the digital environment.

b) Digital economy.- It is the innovation and transformation of the economy based on the strategic and disruptive use of digital technologies. Develops the ability to increase the efficiency, productivity, transparency, safety and effectiveness of economic and social processes and activities, supported by the intensive use of digital technologies, data or communication networks and digital platforms. It leads to the generation of economic and social benefits, prosperity and well-being for the society.

c) Digital Environment.- It is the domain or field enabled by digital technologies and devices, generally interconnected through networks and data infrastructures or communication, including the Internet, that support the processes, services, platforms that serve as a basis for interaction between people, companies, entities public or devices.

d) Critical activity.- It is the economic and / or social activity whose interruption has serious consequences on the health and safety of citizens, in the operation cash of essential services that maintain the economy, society and government, or affect economic and social prosperity in general.

e) Digital security incident.- Event or series of events that can compromise trust, economic prosperity, and the protection of people and their data personal, information, among other assets of the organization, through digital technologies.

f) Management of digital security incidents.- Formal process that aims to plan, prepare, identify, analyze, contain, investigate security incidents as well as recovery and determination of corrective actions to prevent similar incidents.

g) Digital security risk.- Effect of uncertainty related to the use, development and management of digital technologies and data, in the course of any activity. It results from the combination of threats and vulnerabilities in the digital environment and is dynamic in nature. May undermine achievement of economic goals and social by altering the confidentiality, integrity and availability of the activities or the environment, as well as putting at risk the protection of the private life of the people. It includes aspects related to the physical and digital environments, the critical activities, the people and organizations involved in the activity and the organizational processes that support it.

h) Cybersecurity.- Technological capacity to preserve the proper functioning of networks, assets and computer systems and protect them against threats and vulnerabilities in the digital environment. It includes the technical perspective of Digital Security and is an area of the country's Digital Security Framework.

i) Digital service.- It is that service provided totally or partially through the Internet or other equivalent networks, which is characterized by being partially or totally automated and intensive use of digital technologies and data, allowing at least one of the following benefits: i) Acquire a good, service, information or content, ii) Search, share, use and access data, content or information about products, services or people, iii) Pay for a service or good (tangible or intangible) and, iv) The relationship between people.

j) Digital service provider.- It comprises any public entity or private sector organization, regardless of its geographical location, whichever is responsible for the design, provision and / or access to digital services in the national territory.

## CHAPTER II

## DIGITAL TRUST FRAMEWORK

**Article 4. Digital Trust Framework**
4.1 The Digital Trust Framework is constituted by the set of principles, models, policies, standards, processes, roles, people, companies, public entities, technologies and minimum standards that ensure and maintain trust in the digital environment.

4.2 The Digital Trust Framework has the following areas:

a) Protection of personal data and transparency.- The Ministry of Justice and Human Rights (MINJUSDH), who exercises the national authorities of Transparency, Access to Public Information and Protection of Personal Data, within the framework of its functions and powers, rules, directs, supervises and evaluates the matter of transparency and protection of personal data.

b) Consumer protection.- The National Institute for the Defense of Competition and the Protection of Intellectual Property (INDECOPI), within the framework of its functions and competences, norms, directs, supervises and evaluates the matter of consumer protection.

c) Digital Security.- The Presidency of the Council of Ministers (PCM), through the Secretariat of Digital Government, in its capacity as the governing body of digital security in the country, standard, directs, supervises and evaluates the matter of digital security.

**Article 5. Governing body of the Digital Trust Framework**
The Presidency of the Council of Ministers, through the Secretariat of Digital Government, is the governing body in matters of Digital Trust and responsible for the articulation of each of its areas.

**Article 6. Powers of the governing body**
The Presidency of the Council of Ministers, through the Digital Government Secretariat, in its capacity as the governing body of Digital Trust, has the following functions:

a) Formulate, articulate and direct the Digital Trust strategy at the national level, and supervise its compliance.

b) Issue guidelines, standards, specifications, guides, directives, technical norms and standards regarding Digital Trust, without affecting the balance financial economy of digital projects.

c) Assess the needs of public entities, private organizations and individuals in matters of Digital Trust.

d) Articulate actions and measures for the implementation of the Digital Trust strategy at the national level with actors from the public sector, private sector, civil society, academia and other interested parties, as well as promoting recognition.

e) Keep the President of the Council of Ministers informed about the results and progress of Digital Trust in the country and digital security incidents notified in the National Center for Digital Security when appropriate.

These functions are exercised without affecting the autonomies and powers of each sector within the framework of its powers.

**Article 7. National Center for Digital Security**
7.1 Create the National Center for Digital Security as a digital platform that manages, directs, articulates and supervises the operation, education, promotion, collaboration and cooperation of Digital Security at the national level as an integral component of national security, in order to strengthen digital trust. That's it responsible for identifying, protecting, detecting, responding, recovering and collecting information on digital security incidents at the national level to manage them.
7.2 The National Center for Digital Security is in charge of the Presidency of the Council of Ministers, through the Secretariat of Digital Government, and is the only National contact point in communications and coordination with other national and international organizations, centers or teams of a similar nature.
7.3 The National Center for Digital Security constitutes the mechanism for exchanging information and coordinating actions with those responsible for the areas of the Digital Security Framework of the Peruvian State, in accordance with article 32 of Legislative Decree No. 1412, Legislative Decree that approves the Government Law Digital.
7.4 The National Center for Digital Security incorporates the National Digital Security Incident Response Team responsible for: i) Managing the response and / or recovery from digital security incidents at the national level and, ii) Coordinate and articulate actions with other teams of a similar national nature and international agencies to deal with digital security incidents
7.5 The Digital Government Secretariat establishes the escalation, coordination, exchange and activation protocols for digital security incidents in the country and issues the corresponding guidelines and directives.

## CHAPTER III
## MEASURES TO STRENGTHEN DIGITAL CONFIDENCE

**Article 8. National Registry of Digital Security Incidents**
8.1 Create the National Registry of Digital Security Incidents whose objective is to receive, consolidate and maintain data and information on incidents of digital security reported by digital service providers at the national level that can serve as evidence or input for analysis, investigation and solution.
8.2 The National Registry of Digital Security Incidents and the information contained therein is confidential, it is supported on a digital platform administered by the Digital Government Secretariat, who is responsible for its availability, confidentiality and integrity.
8.3 The National Center for Digital Security provides information on the records of digital security incidents, to those responsible for the areas of the Framework of Digital Security, in accordance with article 32 of Legislative Decree No. 1412, and of the Digital Trust Framework, having to observe the regulations for this purpose in force regarding the protection of personal data.

**Article 9. Obligations of the Digital Service Provider**
9.1 Public administration entities, digital service providers in the financial sector, basic services (electricity, water and gas), health and transportation of people, internet service providers, providers of critical activities and educational services, must:
a) Notify the National Center for Digital Security of all digital security incidents.
b) Implement physical, technical, organizational and legal security measures that allow guaranteeing the confidentiality of the message, content and information that is transmitted through their communications services.
c) Manage digital security risks in your organization in order to establish controls that protect the confidentiality, integrity and availability of the information.
d) Establish mechanisms to verify the identity of the people who access a digital service, according to the level of risk of the same and according to the Current regulations regarding the protection of personal data.
e) Report and collaborate with the personal data protection authority when they verify a digital security incident that involves personal data.
f) Maintain a secure, scalable and interoperable infrastructure.
9.2 Private organizations take as a reference the standards issued by the Secretary of Digital Government as soon as it applies to them and generates value for them and they implement in a compulsory way those that prevent the infringement of the rights of the people.
9.3 Public administration entities must implement an Information Security Management System (ISMS), a Response Team to Digital Security Incidents when applicable and comply with the regulation issued by the Digital Government Secretariat.
9.4 All critical activity must be supported by a secure, available, scalable and interoperable infrastructure.

**Article 10. International articulation**
The Digital Government Secretariat of the Presidency of the Council of Ministers coordinates actions related to politics with the Ministry of Foreign Affairs that contribute to strengthening confidence in the digital environment when appropriate and within the framework of their competencies.

**Article 11. Articulation Regarding Communications**
The Digital Government Secretariat of the Presidency of the Council of Ministers coordinates with the Ministry of Transport and Communications the actions related to the communications matters within the framework of its powers.

## CHAPTER IV
## ETHICAL USE OF TECHNOLOGIES DIGITAL AND DATA

**Article 12. Data as strategic assets**
12.1 Public entities and private sector organizations manage data, especially personal, biometric and spatial data, as assets strategic, ensuring that these are generated, shared, processed, accessed, published, stored, conserved and made available for as long as necessary and when appropriate, considering the needs for information, ethical use, transparency, risks and strict compliance with regulations on the matter protection of personal data, digital government and digital security.
12.2 Public entities and private sector organizations promote and ensure the ethical use of digital technologies, the intensive use of data, such as the Internet of things, artificial intelligence, data science, analytics and big data processing.
12.3 The processing of personal data must comply with the legislation on the matter issued by the National Authority for the Protection of Personal Data.

**Article 13. National Data Center**
13.1 Create the National Data Center as a digital platform that manages, directs, articulates and supervises the operation, education, promotion, collaboration and cooperation of data at the national level, in order to strengthen the trust and well-being of people in the digital environment within the framework of this standard.
13.2 The National Data Center is in charge of the Presidency of the Council of Ministers, through the Secretariat of Digital Government and is the only point of national contact in communications and coordination with other organizations, centers or national and international teams of a similar nature.
13.3 The National Data Center exchanges information and coordinates actions with public entities, academia, civil society and the private sector and with the entities responsible for the areas of the Digital Trust Framework for data governance.
13.4 The Digital Government Secretariat, in its capacity as the governing body in data governance, establishes the protocols and mechanisms in matters of data governance and issues the corresponding guidelines and directives.

**Article 14. Financing**
The implementation of what is established in this Emergency Decree is financed from the institutional budget of the entities involved, without demanding additional resources to the Public Treasury.

**Article 15. Endorsement**
This Emergency Decree is endorsed by the President of the Council of Ministers and the Minister of Justice and Human Rights.

## FINAL SUPPLEMENTARY PROVISIONS

**First. Regulation**
The Executive Power, within ninety (90) business days following the entry into force of this regulation, approves its regulations through Supreme Decree endorsed by the President of the Council of Ministers.

**Second. National Registry of Digital Security Incidents**
Within a period of no more than ninety (90) business days, after the publication of this Emergency Decree, the Presidency of the Council of Ministers implements the National Registry of Digital Security Incidents and dictates norms, guidelines and directives for its correct operation.

**Third. Management and Promotion of the National Network of the Peruvian State (REDNACE) and the National Research and Education Network (RNIE)**
The Presidency of the Council of Ministers, through the Digital Government Secretariat, is in charge of the management and promotion of the National Network of the Peruvian State (REDNACE) and the National Research and Education Network (RNIE) referred to in Law No. 29904 in order to contribute to the achievement of national policies, the strengthening of a digital society and the digital transformation of the State. The contracting of services for REDNACE connectivity is carried out by each Public Administration entity, in accordance with the provisions of article 19 of said Law.

**Quarter. Application of the Standard**
This standard applies to public-private partnership projects, concession contracts, projects incorporated into the investment promotion process. private or other projects and platforms on digital transformation that are designed, initiated or managed from the entry into force of the same.
Given at the Government House, in Lima, on the eighth day of the month of January of the year two thousand and twenty.
MARTÍN ALBERTO VIZCARRA CORNEJO
Republic President
VICENTE ANTONIO ZEBALLOS SALINAS
President of the Council of Ministers
ANA TERESA REVILLA VERGARA
Minister of Justice and Human Rights
**1844001-2**