



Chief of the Cabinet of Ministers

BUENOS AIRES, July 28, 2011

In the view of the Record CUDAP: EXP-JGM: 0005475/2011 of the Registry of the Presidency of the Cabinet of Ministers (Decree nr. 438/92) and the Resolution ex SFP Nr. 81/ 14th of July of 1999, and

CONSIDERING:

That the contemporary world has been reshaped by dramatic changes through the development and distribution of communications and information technologies in the society, and that these technologies are mostly based at the cyberspace.

That the employ of virtual communications depends, as a resource, on digital infrastructure, understood as critical infrastructure, i.e. the indispensable infrastructure for the communications and information systems to work, and thereby to support the function and efficiency of both the National Public and the private sectors functions and efficiency.

That the security of the digital infrastructure is exposed to continual threats, which could cause, in case they materialized, profound damage to the communications and information systems, being essential then to adopt the necessary actions in order to secure the normal functioning of the above-mentioned critical infrastructures.

That opportunely, through the Resolution ex SFP N° 81/99 was created the Office for the Security Emergency Coordination in the Argentinean Public Administration's Networks (in Spanish, ARCERT), in the frame of the former UNDERSECRETARIAT OF INFORMATION TECHNOLOGIES of the former SECRETARIAT OF THE PUBLIC ADMINISTRATION OF THE PRESIDENCY OF THE CABINET OF MINISTERS



Chief of the Cabinet of Ministers

That hence it is appropriate to create the “NATIONAL PROGRAM OF CRITICAL INFRASTRUCTURES OF INFORMATION AND CYBER SECURITY” within the frame of THE NATIONAL OFFICE OF INFORMATION TECHNOLOGIES FROM THE UNDERSECRETARIAT OF TECHNOLOGIES FOR THE ADMINISTRATION from the CABINET SECRETARIAT OF THE PRESIDENCY OF THE CABINET OF MINISTERS, in order to promote the creation and the adoption of a specific regulatory frame oriented towards the required identification and protection of the critical and strategical infrastructures pertaining to the National Public Sector, the interjurisdictional organs, the civil organizations and/or the private sector, as well as the collaboration of the above-mentioned sectors aimed to the development of strategies and structures appropriated for the joint action towards the implementation of the appropriate technologies, among other actions.

That the revocation of the Resolution ex SFP N° 81/99 becomes hence necessary.

That the General Direction of Juridical Affairs of the Cabinet Secretariat of the Presidency Cabinet of Ministers has already taken care of its area of competencies

That the present Law is dictated in the exercise of the faculties conferred by the Art. 103 of the National Constitution, and complying to it.

THE CHIEF OF THE CABINET OF MINISTERS

RESOLVES:

ARTICLE 1. - to set up in the field of the NATIONAL OFFICE FOR INFORMATION TECHNOLOGIES of the SECRETARIAT FOR ADMINISTRATION TECHNOLOGIES of the



Chief of the Cabinet of Ministers

UNDERSECRETARIAT OF ADMINISTRATION TECHNOLOGIES of the CABINET SECRETARIAT of the PRESIDENCY OF THE CABINET OF MINISTERS, “THE NATIONAL PROGRAM OF CRITICAL INFRASTRUCTURES OF INFORMATION AND CYBER SECURITY”

ARTICLE 2. - “THE NATIONAL PROGRAM OF CRITICAL INFRASTRUCTURES OF INFORMATION AND CYBER SECURITY” has the purpose of elaborating a specific regulatory frame that favors the identification and protection of strategic and critical infrastructures of the entities and jurisdictions defined in the 8th article of Law 24.156 and its amends.

Article 3.- “THE NATIONAL PROGRAM OF CRITICAL INFRASTRUCTURES OF INFORMATION AND CYBER SECURITY” will have the following objectives under its scope:

- a) To elaborate and propose norms in order to increase the efforts oriented towards the increase of the security threshold in the resources and systems pertaining to the employ of information technologies of the National Public Sector.
- b) To collaborate with the private sector in order to define joint policies for the digital security, and to maintain them constantly up-to-date, enhancing the relationships between the public and the private sectors, with the emphasis put on the critical infrastructures.
- c) To administrate the existing information about reports on security issues occurred in offices of the National Public Sector which would adhere to the Program, and to prosecute the quest for solutions in an organized and unified manner.



Chief of the Cabinet of Ministers

- d) To determine strategical priorities and plans to face the challenges of cyber security, and to secure the implementation of the last technological advances for the protection of critical infrastructures.
- e) To investigate new technologies and tools in the field of cyber security.
- f) To incorporate cutting-edge technologies in order to minimize the possible vulnerabilities of the digital infrastructure pertaining to the National Public Sector.
- g) To give advice to the public organs about security tools and techniques required to the defense of their information systems.
- h) To alert the organs that will adhere to this Program about cases of detection of attempts to violate critical infrastructures, be they actual or not.
- l) To coordinate the implementation of exercises or response in the event of an attempt to violate the critical infrastructures pertaining to the National Public Sector.
- j) To give technical advise to the organs of the National Public Sector which would have adhered to the Program in the event of security incidents.
- k) To centralize the reports on security incidents occurred in networks pertaining to the National Public Sector which would adhere to the Program, and to facilitate the exchange of information in order to face them.
- l) To act as a repository provided with the whole existing information about security incidents and protection and defense techniques.
- m) To promote the coordination between the administrative unities of the networks pertaining to the National Public Sector, to enhance the prevention, detection, handling, and gathering of information about security incidents.
- n) To elaborate an annual report of the situation in terms of cyber security, to be published



Chief of the Cabinet of Ministers

in an open and transparent manner.

ñ) To monitor the services offered by the National Public Sector through Internet and those identified as Critical Infrastructure for the prevention of possible security failures.

o) To promote the awareness about the risks brought by the employ of digital resources in the National Public Sector and the Organs of Government to the public in general, and to the shared roles of the National Public and the private sectors for the protection of the critical infrastructure.

p) To provide the necessary information useful to increase the security levels in the networks of the National Public Sector.

k) To be able to interact with equipments of similar nature.

Article 4.- "THE NATIONAL PROGRAM OF CRITICAL INFRASTRUCTURES OF INFORMATION AND CYBER SECURITY" will be under the command of the NATIONAL OFFICE FOR INFORMATION TECHNOLOGIES, charged with the following attributions:

a) To dictate the necessary norms for the Program to be implemented

b) To create a web page in order to prosecute the actions which are necessary to achieve the established objectives.

c) To coordinate the activities with the organs and jurisdictions of the National Public Sector, the interjurisdictional organs and the civil and private organs which would adhere to the "THE NATIONAL PROGRAM OF CRITICAL INFRASTRUCTURES OF INFORMATION AND CYBER SECURITY".

ARTICLE 5. - The entities and jurisdictions defined in the 8th article of Law 24.156 and its



Chief of the Cabinet of Ministers

amends, the Inter-jurisdictional organs, and the civil organizations and those of the private sector, are invited to adhere to the “NATIONAL PROGRAM OF CRITICAL INFRASTRUCTURES OF INFORMATION AND CYBERSECURITY”.

Article 6. - “NATIONAL PROGRAM OF CRITICAL INFRASTRUCTURES OF INFORMATION AND CYBERSECURITY” will not intercept nor intervene by any means any private connection or network, complying with the National Law 25326 for the Protection of Personal Information, as well as its Regulatory Decree 1558 of November 29th, 2001.

Article 7. - THE NATIONAL OFFICE FOR INFORMATION TECHNOLOGIES, in its character of application authority, will offer the technical and administrative support required to the “NATIONAL PROGRAM OF CRITICAL INFRASTRUCTURES OF INFORMATION AND CYBERSECURITY”

Article 8. - “THE NATIONAL PROGRAM OF CRITICAL INFRASTRUCTURES OF INFORMATION AND CYBERSECURITY” should present to the Chief of the Cabinet of Ministers the regulative projects elaborated following the terms of the 2nd article of this Resolution.

Article 9. - The Resolution Nr. 81 of the former Secretariat of Public Administration and its amends are hereby derogated.

ARTICLE 10. - Let it be known, published and given to the NATIONAL DIRECTION OF THE



Chief of the Cabinet of Ministers

OFFICIAL REGISTRY.

RESOLUTION Nr. 580

Dr. Aníbal Domingo Fernandez
Chief of the Cabinet of Ministers