1. Document Information

1.1 Distribution List
Reserved information

1.2 Date of Last Update
Version 1.0 03/09/2015

1.3 Locations where this Document May Be Found
The current version of this document can always be found at http://www.icic.gob.ar

1.4 Authenticating this Document
This document has been signed with the PGP key of ICIC-CERT

2. Contact Information

2.1 Name of the Team
CERT of CIIP and Cybersecurity of ARGENTINA
Short name: “ICIC – CERT”.

2.2 Address
Av. Roque Sáenz Peña 511 Floor 5– CABA – CP 1035 – ARGENTINA

2.3 Time Zone
UTC-GMT-3

2.4 Telephone Number
+54-11 5985-8654/5

2.5 Facsimile Number
No available

2.6 Other Telecommunication
No available

2.7 Electronic Mail Address
cert@icic.gob.ar

2.8 Public Keys and Encryption Information
PGP is used for functional exchanges between ICIC CERT and its Partners (incident reports, alerts, etc.).

ID
0x0977 2CB1

Fingerprint es: 556F FB47 176B A40A B91C 03C3 FD72 8FEF 0977 2CB1

2.9 Members of the Team

Sr. Darío Hidalgo
Sr. Enrique Beláustegui
Sr. Arturo Busleiman
Sra. Claudia Lacanna
Sr. Marcelo Soto
Sra. Magdalena Marcenaro

2.10 More Information

General information about ICIC- CERT, and recommendations can be found at http://www.icic.gob.ar

2.11 Days/Hours of Operation

08:00 to 18:00 Monday to Friday

2.12 Points of Customer Contact for clients

The preferred method to contact ICIC-CERT is to send an e-mail to the address ICIC-CERT (cert@icic.gob.ar) which is monitored by a duty officer during hours of operation

3. Constituency

3.1 Mission

ICIC-CERT's mission under the regulatory framework of the UNDERSECRETARY OF CRITICAL INFRASTRUCTURE INFORMATION PROTECTION AND CYBER SECURITY under the CABINET SECRETARIAT of the CHIEF OF THE CABINET OF MINISTERS is to protect critical information assets of the ARGENTINA NATION of possible attacks I could be objective, actions are played prevention, detection, response and recovery.

Among its specific actions we can mention:

• Understand all aspects of cybersecurity and protection of critical infrastructure, capacity building detection, defense, response and recovery from incidents understanding.
• Manage all information about reports of security incidents in the National Public Sector and prosecute possible solutions in an organized and unified.
• Provide technical security incident in computer systems that agencies report
• Centralize reports of security incidents in telematics networks National Public Sector and facilitate the exchange of information to tackle them.
• To act as a repository of all information on security incidents, tools, techniques of protection and defense.

• Promote coordination between management units of computer network of the National Public Sector, for the prevention, detection, management and collection of information on security incidents.
• To disseminate useful information to increase levels of security for telematics networks in the National Public Sector.
• Interact with equipment of similar nature.

3.2 Constituency

The constituency of ICIC-CERT is composed of all the strategic and critical infrastructures of the National Public Sector of the National State, and the jurisdictional agencies and organizations of the civil and private sectors that require it.

3.3 Sponsorship and/or Affiliation

CHIEF OF THE CABINET OF MINISTERS – PRESIDENCY OF THE NATION.

3.4 Authority

CHIEF OF THE CABINET OF MINISTERS, assuming the coordination of activities for the definition of strategies, rules, procedures and regulations.

4. Policies

4.1 Types of Incidents and Level of Support

The ICIC-CERT Team will gradually roll out its services, starting with Announcements, Alerts and Incident Response Coordination

4.2 Co-operation, Interaction and Disclosure of Information

The information will be handled with complete confidentiality in accordance with policies and procedures for the management of incidents set out to the ICIC-CERT and the cooperation agreements previously established with other teams CSIRTs. Communications are established with National CSIRTs and Internacional CERTs through granting of tickets that are assigned with a unique number for tracking.
ICIC-CERT also communicates with the Law Enforcement Agencies and the Focal points of Cybercrime in the Public Prosecutor MINISTRY.

.

4.3 Communication and Authentication

The public Keys are publishing in the server pgp.mit.edu

5. Services

5.1 Announcements

This service aims at providing information (e.g. on threat landscape, published vulnerabilities, new attack tools or artefacts, security/protection measures, etc.) needed to protect systems and networks.

.

5.2 Alerts and warnings

This service aims at disseminating information on cyber-attacks or disruptions, security vulnerabilities, intrusion alerts, computer viruses, and providing recommendations to tackling the problem to the constituent.

5.3 Incident Response Coordination

This service aims at the coordination of response to information security incidents in the institutions and bodies of the Argentina, in cooperation with the owners and providers of impacted parts of the respective IT infrastructure and international communities of Computer Emergency Response Teams, telecommunication operators, ISPs and other public and private bodies (police, investigators, courts) as appropriate.

6. Incident Reporting Forms

For reporting incidents you may use the following mail address cert@icic.gob.ar or call to: +54-11 5985-8654/5.

7. Disclaimer

The ICIC CERT Argentina Team assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.