PCC.I/REC. 23 (XXVI-15) [1]

CREATION OF NATIONAL COMPUTER INCIDENT RESPONSE TEAMS

The XXVI Meeting of Permanent Consultative Committee I: Telecommunications/Information and Communications Technology (PCC.I),

CONSIDERING:

a) The work being undertaken by the Administrations of CITEL related to the creation of national incident response teams, facing the threat that now a days jeopardize the effective use of the information and communication technologies (ICT´s), attending, thereby, the recommendations made by the International Telecommunications Union (ITU);

b) That the Americas´ Region has the second higher level of broadband penetration as well as populations with high growth in the use of Internet, represents a great number of challenges in cyber security, therefore, it is necessity to implement mechanisms that can be reflected in the detriment of the threats in this matter;

c) That the cyber incidents identified are increasing such as *phishing,* identity theft for financial fraud, the leak of governmental information, defamation and cyber-bulling; issues that can be prevented;

d) That among the benefits of having a national computer incident response team are to respond in a rapid manner, and in a given case restore the damage caused, provide information regarding the possible vulnerabilities of cyber security, advice in the protection of computer areas, among others,

RECOGNIZING:

a) That Member States of CITEL that lack computer incident response teams take the best practices of those Administrations that do have this figure in order to achieve a complete implementation of Computer Incident Response Teams (CIRTs) in the Americas Region recognizing the important role that Inter-American Committee against Terrorism (CICTE) plays in this area;

b) That Resolution 58 (Dubai, 2012) “Encouraging the creation of national computer incident response teams, particularly for developing countries” of the World Telecommunication Standardization Assembly of the International Telecommunications Union, resolves to support the creation of national CIRTs in ITU Member States where CIRTs are needed and are currently absent;

c) That Resolution 69 (Dubai, 2014) “Facilitating creation of national computer incident response teams, particularly for developing countries1, and cooperation between them” of the World Telecommunication Development Conference of the International Telecommunications Union, invites the Member States to create national CIRTs;

d) That the line of action C5 of one of the mandates of the High Level Event of the World Summit on the Information Society + 10 (WSIS+10) relating to the implementation of the outcome of WSIS, invites the Administrations that have CIRTs to offer support for the establishment of national Computer Incident Response Teams (CIRTs) in those countries of the region that do not have them, so as to answer to incidents that impact their information infrastructure,

[1] CCP.I-TIC/doc. 3629/15 rev.2

REMEMBERING:

Resolution AG/RES. 2004 (XXXIV-O/04) "Adoption of a comprehensive inter-american strategy to combat threats to cybersecurity: a multidimensional and multidisciplinary approach to creating a culture of cybersecurity",

TAKING INTO ACCOUNT:

a) That each day, the dependency of the human being over the information and communication technologies increases, and with that, the vulnerabilities of security and protection of those who make use of them;

b) That cybersecurity represents the central element for the creation of confidence on the use of information and communication technologies, thus, security mechanisms need to be necessarily intensified;

c) That it is necessary a cooperation between Member States, in the sense of fully cover the Americas Region regarding computer incident response teams, attending Resolutions and Recommendations of the ITU,

RECOMMENDS:

1. That the Rapporteurship on Cybersecurity, Vulnerability Assessment and Critical Infrastructure makes a list of ongoing regional activities related to cybersecurity cooperation and capacity building that CITEL members may take advantage of;

2. To those Administrations without CIRTs, to revise the Recommendation PCC.I/REC. 12 (XIX-11) on the guidelines for the creation of Computer Security Incident Response Teams (CSIRT) to take it as a basis for the development of future projects regarding the implementation of these teams;

3. That Administrations take into account the list of documents produced by CICTE on Cybersecurity and Critical Infrastructure Protection that is included in the Working Group on Deployment of Technologies and Services (WGDTS)'s Report CCP.I-TIC/doc. 3633/15 rev.2,

INSTRUCTS THE EXECUTIVE SECRETARY OF CITEL:

1. To require the Rapporteurship on Cyber security, vulnerability assessment and critical infrastructure, make a report on the progress obtained relating the Technical Notebook 4 "Cyber Security", since its redaction to date.

2. To prepare in collaboration with the Inter-American Committee against Terrorism (CICTE), a list of organizations, committees and initiatives related with the subject of cybersecurity, with the purpose of serving as reference for those Administrations that have projects of establishment of teams of intervention.