CYBERWELLNESS PROFILE REPUBLIC OF COSTA RICA

BACKGROUND

Total Population: 4 794 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 45.96%
(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:
- Penal Code amended by the Costa Rican Cybercrime Offence Law 9048.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:
- Law on Protecting Individual Personal Information
- Law on the Certificates, Digital Signatures and Electronic Documents
- Law on Registration, Seizure and Examination of Private Documents and Intervention in Communications.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Costa Rica has an officially recognized national CIRT known as CSIRT-CR established under the Ministry of Science, Technology and Telecommunications.

1.2.2 STANDARDS

Cost Rica does not have any framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Costa Rica does not have any framework for certification and accreditation of national agencies and public sectors professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

A National Digital Strategy has been adopted by the government. Its primary focus is on defining a vision for the integrated use of technologies by the State, and it does not go much beyond identifying cybersecurity as a priority. There is presently no national cybersecurity strategy or policy guiding the related efforts of national authorities.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national or sector-specific governance roadmap for cybersecurity in Costa Rica.

1.3.3 RESPONSIBLE AGENCY

The following agencies are responsible for cybersecurity in Costa Rica:
- CSIRT-CR
- Digital Government / Digital Secretariat
- The Computer Crimes Section of the Judiciary
- The Computer Crime Section of the Investigative Branch of the Judiciary.
- Directorate for Digital Signatures
- The Superintendency for Telecommunications
- Ministry of Science, Technology and Telecommunications

1.3.4 NATIONAL BENCHMARKING

Costa Rica does not have any national benchmarking and referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no information on any programs for research and development of cybersecurity standards, best practices and guidelines in Costa Rica.

1.4.2 MANPOWER DEVELOPMENT

The Centre for the Formation of ICTs (CENFOTEC) offers a specialization in cyber security; the Latin American Science and Technology University (ULACIT) offers a specialization in information Security. Other institutions in Costa Rica offer cybersecurity and cybercrime relevant courses.

1.4.3 PROFESSIONAL CERTIFICATION

Costa Rica does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Costa Rica does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states Costa Rica has participated in various training programs by the OAS. Personnel of the computer crime section have received training in the United States and Canada.

1.5.2 INTRA-AGENCY COOPERATION

CSIRT-CR is mandated to coordinate among entities of the State and autonomous institutions to identify threats, minimize risks, and improve cooperation and information-sharing on relevant cybersecurity-related matters.

1.5.3 PUBLIC SECTOR PARTNERSHIP

CSIRT-CR is also mandated to coordinate not just among entities of the State and autonomous institutions, but also companies and banks to identify threats, minimize risks, and improve cooperation and information-sharing on relevant cybersecurity-related matters. There is no legal obligation for private sector entities to share information with national authorities in the event of an incident and the links and mechanisms necessary for facilitating such cooperation are limited and informal.

1.5.4 INTERNATIONAL COOPERATION

Costa Rica is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Article 173* of the Criminal Code, amended by the law n. 8590, July 2007
- Article 173bis* of the Criminal Code, added by the law n. 8590, July 2007
- Article 13* of Law n. 7739, Code for Childhood and Adolescence

- Article 174* of the Criminal Code, reformed by the law 7899, August 1999
- Law n. 8934*Protection of Children and Young from Harmful Content on the Internet and other Electronic Media, March 2011.

2.2 UN CONVENTION AND PROTOCOL

Costa Rica has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Costa Rica has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

A National Committee on the commercial sexual exploitation of children was created under the National Plan against Commercial Sexual Exploitation, 2002- Plan Nacional contra la Exploitación Sexual Comercial de Niñas, Niõs y Adolescentes. A National Committee for Online Security was created in December 2010-Comisión Nacional de Seguridad en Línea (Decree n.36274).

2.4 REPORTING MECHANISM

The Patronato Nacional de la Infancia (PANI) provides a space for online reporting on its Website.

More information is available on ITU website at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx
Last updated on 12th February 2015