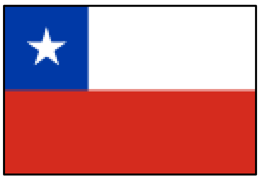

CYBERWELLNESS PROFILE REPUBLIC OF CHILE

BACKGROUND

Total Population: 17 423 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 66.50%
(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:

- Law on Cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Law on Personal Data Protection
- Law on Electronic Documents and Digital Signature.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Chile has an officially recognized national CIRT, CLCERT. CLCERT-CL has existed and functioned within the government but it is not a formal institutional entity so much as an operational capacity and structure maintained by the Ministry of the Interior and Public Safety.

1.2.2 STANDARDS

Chile has officially approved the Supreme Decree No. 1299, Program for the Improvement of Information Security Systems Management as the national framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no information on any framework for certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

While there is no official national cybersecurity strategy or policy document, Chilean authorities have been working for a number of years to develop a strong national capacity for cyber incident response and management. Emphasis has been placed on developing standardized procedures and best practices for incident management and cybersecurity more broadly.

1.3.2 ROADMAP FOR GOVERNANCE

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

1.3.3 RESPONSIBLE AGENCY

The Ministry of the Interior and Public Safety, Cyber Crime Investigation Unit (BRICIB), the General Secretariat of the Presidency and the Sub-Secretariat of Telecommunications all play key roles in cybersecurity.

1.3.4 NATIONAL BENCHMARKING

There is no national benchmarking and referential to measure cybersecurity development in Chile.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Regular risk assessments and trainings for staff are also carried out occasionally as a means of research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in the public sector.

1.4.2 MANPOWER DEVELOPMENT

Personnel from CLCERT -CL receive technical training in aspects of cyber investigations and incident management from experts in the field. Cybersecurity and cybercrime-related bachelors and masters degrees are offered by the University of Chile and other academic institutions. To raise awareness and promote a culture of cybersecurity the Ministry of Education has developed and is implementing, in partnership with several private sector entities, a long-term campaign called Internet Segura. Internet safety is taught in schools as part of the ethics competencies contained in the Technology curriculum.

1.4.3 PROFESSIONAL CERTIFICATION

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

1.4.4 AGENCY CERTIFICATION

Chile 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, CLCERT-CL has actively collaborated with other national CSIRTs around the region in responding to incidents.

1.5.2 INTRA-AGENCY COOPERATION

Chile does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Private companies are able and encouraged by the government to also provide incident management-related services, both to other private enterprises as well as public institutions in Chile.

1.5.4 INTERNATIONAL COOPERATION

To facilitate participation in regional/international cybersecurity platforms and forums:
CLCERT is a member of the FIRST.
CLCERT-CL has participated in initiatives to train personnel in other OAS Member States.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

- Article 366quater and 366quinquies of the Criminal Code, included by Law n. 19.927/2004, January 2004.
- Articles 374 to 374ter of the Criminal Code, included by the Law n.19.617, July 1999, 19.806, May 2002 and 19.927, January 2004.

2.2 UN CONVENTION AND PROTOCOL

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

Chile 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

The website of the Chilean Computer Emergency Response Team CLCERT has general information on cybersecurity and specific information on child online protection.

2.4 REPORTING MECHANISM

Computer incidents can be reported to the National Chile Computer Emergency Response Team CLCERT by the email clcert@clcert.cl. The Integra Foundation provides a helpline.

DISCLAIMER: Please refer to http://www.itu.int/en/Pages/copyright.aspx
More information is available on ITU website at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx
Last updated on 11th February 2015