CYBERWELLNESS PROFILE DOMINICAN REPUBLIC

BACKGROUND

Total Population: 1 359 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 45.90%
(data source: ITU Statistics, December 2012)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-High Technology Crimes Law No. 53/07

-Electronic Commerce, Documents and Digital Signatures Law.

1.1.2 REGULATION AND COMPLIANCE

Dominican Republic does not have specific legislation and regulation related to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT readiness assessment for Dominican Republic at Santo Domingo, Dominican Republic in April 2012 (23-27th April 2012).

Dominican Republic does not have an officially recognized national CIRT.

1.2.2 STANDARDS

Dominican Republic does not have officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Dominican Republic does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Dominican Republic does not have an officially recognized national cybersecurity strategy or policy.

1.3.2 ROADMAP FOR GOVERNANCE

Dominican Republic does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The Interagency Commission against Crimes and High Tech Crime is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Dominican Republic does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Dominican Republic does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The National Commission for Information Society and Knowledge (CNSIC) has an officially recognized national awareness program that promotes norms, values and social behaviors that contribute to integrity, creativity and innovation in navigating cyberspace.

1.4.3 PROFESSIONAL CERTIFICATION

Dominican Republic does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Dominican Republic 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

Dominican Republic does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Dominican Republic 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

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

1.5.4 INTERNATIONAL COOPERATION

Dominican Republic is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Dominican Republic also cooperated with the Cybercrime Convention Committee (T-CY) of the Council of Europe, Inter-American Committee contra el Terrorismo (CICTE) of the OAS and INTERPOL.
Dominican Republic is among the beneficiary countries of the EU/ITU co-funded project “Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures” (HIPCAR).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific national legislations pertaining to child online protection are enacted through the following legal instrument:
- Law against High Technology Crimes and Offences (Article 24).

2.2 UN CONVENTION AND PROTOCOL

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

Dominican Republic 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 High Technology Investigation Department (Departamento de Investigación de Crímenes de Alta Tecnología) has produced a presentation on online safety for children.

The National Commission for the Information and Knowledge Society (CNSIC*) maintains together with the Dominican Telecommunications Institute (INDOTEL*) a website* dedicated to prevent the risk of using internet for young people. The website also has information for parents and teachers.

2.4 REPORTING MECHANISM

Complaints can be made by the telephone of the Attorney-General 1-809-200-7393, or by filling the form available in the website www.internetsano.do

---