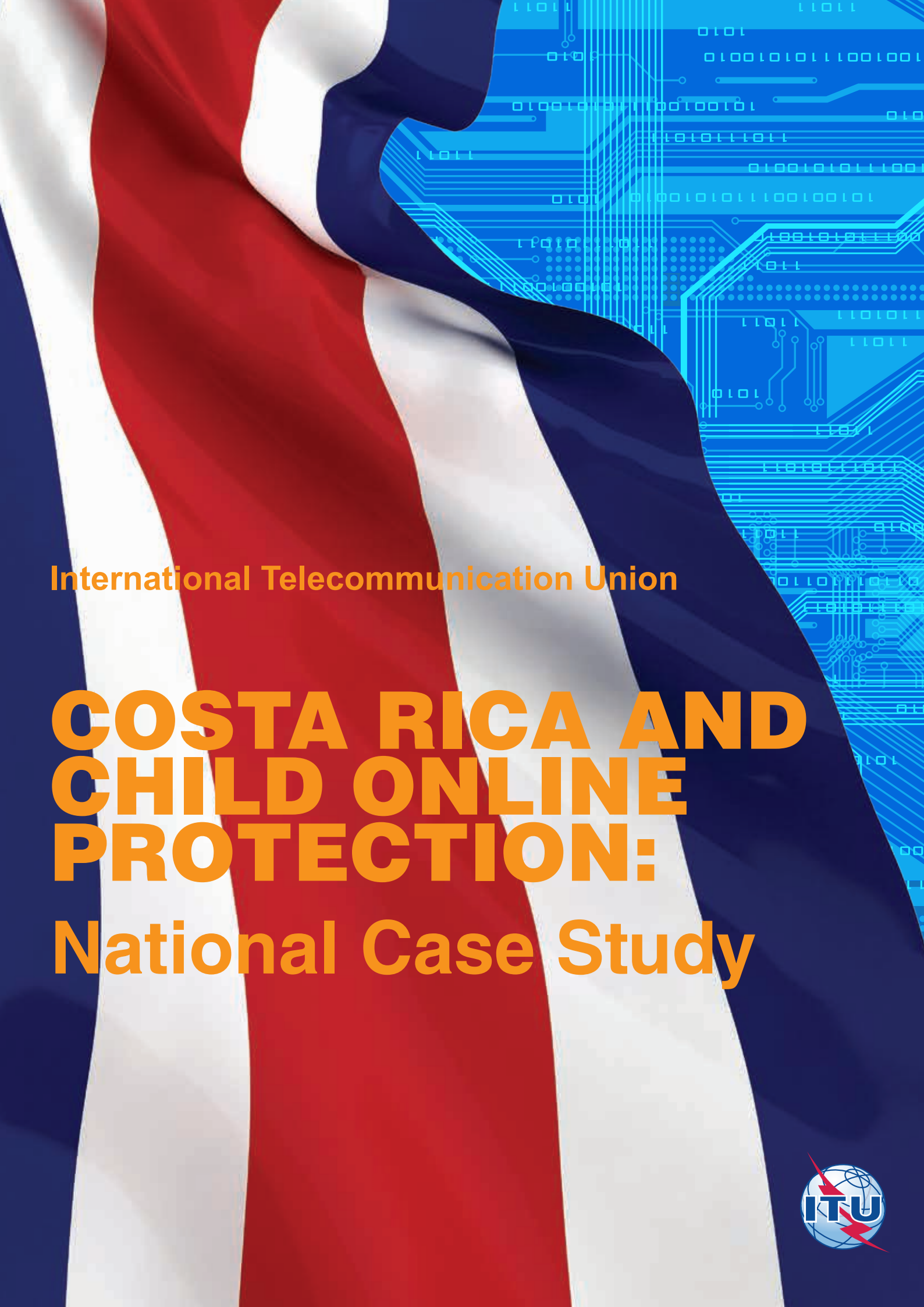


International Telecommunication Union

COSTA RICA AND CHILD ONLINE PROTECTION:

National Case Study

COSTA RICA AND CHILD ONLINE PROTECTION

National Case Study

FOREWORD

The outcomes of the Geneva and Tunis phases of the World Summit on the Information Society included strong commitments to the protection of children in cyberspace. The Geneva Declaration of Principles stated "We are also committed to ensuring that the development of ICT applications and operation of services respects the rights of children as well as their protection and well-being." The Tunis Agenda declared "We will strengthen action to protect children from abuse and defend their rights in the context of ICTs. In that context, we emphasize that the best interests of the child are a primary consideration."

The ITU Child Online Protection (COP) Initiative is a response to those and similar commitments. It is an international collaborative effort led by ITU within the framework of its Global Cybersecurity Agenda (GCA). The COP initiative was launched in 2008 and endorsed by the UN Secretary-General, Heads of State, Ministers and heads of international organizations from around the world. It aims to promote global awareness on the importance of child safety in the online world, develop practical tools to assist governments, industry and educators and share their experiences in working to ensure a safe and secure online experience for children everywhere. In 2009, a multistakeholder group of Child Online Protection members developed global guidelines for children, parents, governments and industry.

In November 2010, under the patronage of the President of Costa Rica, H.E. Laura Chinchilla, I have launched the COP Global Initiative with the aim to implement the COP Guidelines at the global level and develop a new strategy for taking action to protect children online.

The aim of the National Case Study of Costa Rica is to provide an example of best practice and showcase how a comprehensive and holistic strategy at the national level can leverage the awareness of children on how to behave safely online. The National Case Study also collects information in various related areas including Costa Rica's economy and political system, the ICT habits of young people, the level of fixed line Internet penetration and data on the availability of mobile Internet access and usage.

I trust that the political commitment of Costa Rica and the invaluable work developed at the national level will inspire many other leaders, experts, private companies, civil society, to continue to fulfill the dream of making cyberspace a safe, healthy and productive environment – especially for our children and youth.

Dr Hamadoun I. Touré
ITU Secretary-General

TABLE OF CONTENTS

1. Introduction: Purpose of the Case Study 7

1.1 Overview 8

2. Country background 9

2.1 Overview 9
2.2 Internet access 12
2.3 Internet users 19

3. National bodies/Agencies dealing with cybersecurity 21

3.1 Government 21
3.2 Public institutions 29
3.3 Regulators 30

4. National framework on child online protection 37

4.1 Legislation 37
4.2 Organisational structure 39
4.3 Capacity building and awareness-raising strategies (civil society and public institutions) 40
4.4 International cooperation 43
4.5 Recent development under the ITU Child Online Protection Global Initiative 43

5. Best practices 45

5.1 Creating a culture of child online protection 45
5.2 Transparency 45
5.3 Cooperation 46
5.4 Continuity, stability and flexibility 46

6. Recommendations 47

7. Conclusion 49

Annex A — Abbreviations and acronyms 48
Annex B — Organizations interviewed 50

Bibliography 53

Boxes

Box 1 — Public policies in the field of ICT
Box 2 — Key tasks of the CSIRT-CR
Box 3 — Structure of the CSIRT-CR and composition of the Council of Directors
Box 4 — Key components of the CSIRT-CR workplan
Box 5 — Articulation of national strategies
Box 6 — Digital safety in the national plan of science, technology and innovation
Box 7 — What is DNSSEC?
Box 8 — Key legislation governing Costa Rica´s telecommunication sector
Box 9 — Key landmarks in the process of market opening
Box 10 — SUTEL´s organizational chart
Box 11 — Child Online Protection — 2011 PRONIE MEP-FOD workplan

Figures

Figure 1 — Human development indicators (2011)
Figure 2 — Type of technology used for fixed (wired) Internet
Figure 3 — Households with fixed broadband by speed, end of 2011
Figure 4 — Computer ownership, by age range
Figure 5 — Computer ownership, by school years
Figure 6 — Percentage of households with at least one cellular phone, by region
Figure 7 — School and student beneficiaries of PRONIE MEP-FOD by grade, 30 March 2012 (projection)
Figure 8 — Student beneficiaries of PRONIE MEP-FOD by types of programme and grade, 30 March 2012 (projection)
Figure 9 — Distribution of CECI, by provinces. October 2011
Figure 10 — Distribution of training activities, by provinces, October 2011
Figure 11 — Uses of fixed-Internet nationwide, late 2011
Figure 12 — Main Internet applications and services used, fixed Internet, nationwide, late 2011
Figure 13 — Victimisation on the Internet (early 2010)

Maps

Map 1 — Map of Costa Rica and main cities
Map 2 — CSIRTs in North and South America
Map 3 — Map of CSIRTs around the world

Map 1 — Map of Costa Rica and main cities

Source: www.worldofmaps.net/uploads/pics/karte-regionen-costa-rica.png

1. INTRODUCTION: PURPOSE OF THE CASE STUDY

A fundamental role of the International Telecommunication Union (hereinafter referred to as ITU), following the World Summit on the Information Society (WSIS) and the 2006 ITU Plenipotentiary Conference, is to build confidence and security in the use of Information and Communication Technologies (ICTs).

In 2008 ITU launched the Global Cybersecurity Agenda (GCA), a framework for international cooperation whose main aim is to enhance confidence and security in the information society. Under the umbrella of the GCA, the Child Online Protection (COP) Initiative has been established as an international collaborative network to promote the protection of children online by providing guidance on safe online behaviour, in conjunction with other UN agencies and partners.

In 2010, the President of Costa Rica, H.E. Laura Chinchilla, became the new patron of COP. Together with Costa Rica, the ITU Secretary-General launched the COP Global Initiative with high-level deliverables. This Global Initiative was designed to implement the four sets of COP Guidelines[1].

Following requests from a growing number of countries to provide examples of best practices, guidelines and recommendations regarding child online protection at a national level, ITU has decided to gather a series of case studies from different countries.

For instance, this first case study[2] shows how Costa Rica is addressing the online child safety agenda at the national level through the implementation of several programmes and projects. Moreover, the study provides important contextual information about Costa Rica's economy and political system, the ICT habits of young people, the level of fixed line Internet penetration and data on the availability of mobile Internet access and usage.

The aim of this exercise is to provide an example to other countries that wish to promote a responsible and safe use of the Internet among young people. Not all of Costa Rica's experiences will be applicable or relevant to other jurisdictions or environments. However, while reading the document, ideas may come to mind on how to improve or adapt the initiatives of Costa Rica to suit other countries.

H.E. Laura Chinchilla Miranda, President of Costa Rica and patron of the ITU-COP initiative, Ms Clotilde Fonseca, then Minister of Science and Technology and Hamadoun I. Touré, Secretary-General of the International Telecommunication Union at Omar Dengo Foundation facilities. Costa Rica, November 2010. Picture courtesy of the Presidential House.

---

1 ITU has worked with COP partners to develop the first set of guidelines (available in the six UN languages) for different stakeholders: Guidelines for Children on Child Online Protection, Guidelines for Educators on Child Online Protection, Guidelines for Industry on Child Online Protection and Guidelines for Policy-Makers on Child Online Protection. With these guidelines, the COP initiative calls upon all stakeholders to promote the adoption of policies and strategies that will protect children in cyberspace. www.itu.int/cop

2 This case study has been developed during 2012. However, the collection of data and related references refer to 2011 and 2012.

1.1 Overview

During the welcome session of ICANN's 43rd public meeting in March 2012, San José, President Chinchilla emphasised that the country wants to provide broadband access to 100 per cent of the national educational institutions and make ICTs widely available to all people. The President also stated that "the Internet is the hope of an integrated world without frontiers, a common world without controlling owners, a world of opportunities and equality"; Costa Rica has therefore started to set out a series of public policies.

These are further illustrated in the diagram below.

Box 1 — Public policies in the field of ICT

The political will to shift towards an inclusive digital society based on innovation and knowledge is reflected in the implementation of several specific strategies and actions[3] that will be covered in this case study.

One common principle emphasised is that all citizens, especially the most vulnerable, such as children and teenagers, should benefit from any actions taken and not be put at risk by them.

At this stage, it is worth highlighting that exposure to risks does not equal real harm if children are well trained and informed about online risks. As research shows, children and teenagers (11-16 year olds) who carry out risky online activities are often the children who use the Internet in different places, for longer and for more activities; if the child is well trained and aware of online risks, the possibilities of becoming a victim will be much lower. For this reason, in Costa Rica national authorities, the private sector and civil society have initiated, among other things, awareness-raising activities focused on a safe (as an individual) and responsible (as a citizen of the world) use of the Internet.

[3] As explained later in the study, the Costa Rican administration is gradually implementing several specific actions such as the opening of the telecommunications market, the One Laptop per Child educational programme in rural primary schools and secondary schools, the adoption of specific legislation meant to protect underage clients of Internet cafés from inappropriate content, the strengthening of a network of local public telecentres nationwide, the creation of a national Computer Security Incident Response Team and the creation of a Superintendency for Telecommunications.

2. COUNTRY BACKGROUND

2.1 Overview

2.1.1 Geography and demography

Costa Rica is a small country located in the Central American isthmus, and as such, its land portion occupies only 51,100 km². It shares a border with Nicaragua to the North and with Panama to the South. Costa Rica extends from the Pacific Coast to the Caribbean Coast and accumulates a total of 1228 km of coastline. The country has several mountain ranges and its highest point is Cerro Chirripó, at 3820 metres above sea level. The country has more than 100 volcanoes, some still active. It has a tropical (dry and wet) as well as subtropical climate. Its rainy season starts in April and usually lasts until December, while the dry season lasts from January to March in most parts of the country. The temperature is always cooler in the highland areas, comprising mostly of rain and cloud forests.

Picture courtesy of the Omar Dengo Foundation.

Costa Rica is known for its proactive stand regarding the protection of the environment. It has 26 national parks administered by the National System of Conservation Areas and 160 protected areas that represent all together 25 per cent of its territory. It has a vast and diverse wildlife as well as a wide variety of plants. As a result, the country concentrates 5 per cent of the Earth' s biodiversity.

According to the 2011 census, the population of Costa Rica is 4,301,712 — 49 per cent men and 51 per cent women — and there are 1,360,046 households registered[4]. Between 2000 and 2011, the country´s population increased by 491,533. The population density is 84 inhabitants/km², although the Greater Metropolitan Area (GAM), which includes San José, Cartago, Heredia and Alajuela, and its surroundings, concentrates more than half of the population (57 per cent). Costa Rica's territorial division includes seven provinces; the province of San José is by far the most populated of the seven, concentrating 32.6 per cent of the total population of the country.

[4] The National Institute for Statistics and Census (INEC) www.inec.go.cr/Web/Home/pagPrincipal.aspx [Accessed: March 27, 2012].

2.1.2 History and political environment

Costa Rica's first settlements were established in 1522 and it was a remote province. Spain then administered the region of Central America for nearly three centuries from the so-called Captaincy General of Guatemala, where there was a military governor.

However, in 1821 representatives from the church, public powers, civilians and the military gathered in the palace of the Captaincy to sign a joint Declaration of Independence from Spain and to form the Central American Federation. Nevertheless, discord arose amongst the members and following armed conflicts, the Federation ceased to exist. Costa Rica formally withdrew and declared itself sovereign in 1838.

In the aftermath of 1838 a period of gradual reform began, against a backdrop of political unrest. This included the famous battle of Santa Rosa (1856), where the North American mercenary, William Walker, who wanted to annex Central America to the southern US states, was successfully defeated. The "progressive authoritarian" regime of General Tomas Guardía (1870-1882) was also established at this time. Historians consider that the 1899 elections were the first free elections, and except for two major incidents in the first half of the 20th Century, Costa Rica has enjoyed a peaceful democracy ever since.

Between 1948 and 1949, a provisional government set in motion key reforms that would shape modern Costa Rica. Among other things, it adopted a basic welfare system, allowed women, as well as illiterate citizens, to vote, nationalized banks, guaranteed public education for all and gave citizenship to the children of black immigrants. Furthermore, the new constitution approved in November 1949 guaranteed universal suffrage in free elections and the abolition of the army.

Since 1953 Costa Rica has held 15 presidential elections, the latest in 2010. On 8 May 2010 Laura Chinchilla, of the National Liberation Party (PLN), was sworn in as President of the Republic of Costa Rica. Her predecessor (the Nobel Prize winner Oscar Arias) was also affiliated with the same political party.

Costa Rica is a democratic republic. The structure of the government is divided into three branches: executive, legislative and judicial. The executive branch is led by a President who is the Chief of State and Head of Government, and is elected for a four-year term. There are two Vice-Presidents and a cabinet of ministers. The legislative branch is a unicameral Legislative Assembly whose 57 deputies serve four-year terms. The Judicial power is exercised by the Supreme Court of Justice and in 1989 a Constitutional Chamber of the Supreme Court was created to review the constitutionality of legislation.

2.1.3 Economy

According to World Bank standards, Costa Rica is an upper-middle income country.

In 2009, the Costa Rican economy declined by 0.7 per cent, but in 2010 it resumed growth at more than 3 per cent and production grew 4.2 per cent. However, in 2010 the inflation rate reached 5.8 per cent[5] and the government fiscal deficit rose from 3.4 per cent of GDP in 2009 to 5.4 per cent.

Costa Rica is the world leader in per capita exports to the USA, exporting traditional agricultural products such as pineapples, bananas, cassava and melon. These products, together with coffee, sugar and beef are still the backbone of commodity export trade. Nevertheless, a variety of industrial and specialised agricultural products have broadened export trade in recent years. High value-added goods and services, such as microchips and medical equipment, have further boosted exports. The 2011 World Bank's World Development Indicators placed Costa Rica as the first high-tech exporter in Latin America, as well as the fourth largest technology-exporting country in the world; high-tech exports represented 41 per cent of its total manufactured exports in 2009. Tourism is also a foreign exchange earner: according to statistics, two million tourists visited the country in 2011.

Thanks to political stability, relatively high education levels and fiscal incentives offered in free-trade zones, Costa Rica attracts the highest levels of foreign direct investment (FDI) per capita in Latin America. The country has been ranked first in Latin America in FDI and technology-transfer components of the Global Competitiveness Index (GCI) 2011–2012. In 2011, 36 per cent of the total foreign direct investment in the first half of the year was in the manufacturing sector, while the service sector accounted for 33 per cent. Investment in free-trade zones brought in 29 per cent, according to the Ministry of Foreign Trade.

---

[5] XII Report *Estado de la Nación*, 2011. San José, Costa Rica. www.estadonacion.or.cr/images/stories/informes/017/cap_1_sinopsis.pdf

In October 2007, together with El Salvador, Guatemala, Honduras, Nicaragua and Panama, Costa Rica began negotiating a regional Agreement of Association with the European Union. Furthermore, the US-Central American-Dominican Republic Free Trade Agreement (CAFTA-DR) entered into force in January 2009. In April 2010, the country also signed a free trade agreement with China and Singapore, as at 2012 it was pending entry into force.

The National Households Survey showed that in 2010 the Costa Rican labour force amounted to 2,051,696 people, with 59.1 per cent of its population aged 15 and older, the official unemployment rate was registered at 7.3 per cent and public sector employees represented 15.2 per cent of the Costa Rican workforce[6].

2.1.4 Human development

The latest data from the National Institute for Statistics and Census (INEC) shows that, in 2010, the percentage of households living below the poverty line was 21.3 per cent (representing approximately 1,103,522 people[7]) and 6 per cent of households were living in conditions of extreme poverty (31,131 individuals[8]). These numbers are the highest of the decade, according to the latest figures. And yet, Costa Rica´s Human Development Index is 0.744, which places the country above the regional average (0.731Latin America and the Caribbean), and ranks it 69th out of 187 countries.

The chart below displays some of the most illustrative human development indicators:

Expenditure on health, public (percentage of GDP)	**5.9**
Life expectancy at birth (years)	**79.3**
Under-five mortality rate (per 1 000 live births)	**11.0**
Adult literacy rate, both sexes (percentage aged 15 and above)	**96.1**
Combined gross enrolment in education (both sexes) (percentage)	**73.0**
GNI per capita in PPP terms (constant 2005 international $)	**10 497.0**
Adolescent fertility rate (births per 1000 women aged 15-19)	**65.6**
Forest area (percentage of total land area)	**50.1**
Population, urban (percentage of population)	**64.9**

Figure 1 — Human development indicators (2011)

Source: http://hdrstats.undp.org/en/countries/profiles/CRI.html

Health

Costa Rica has had a solid universal healthcare system since the first half of the 20th century. In the 1940s, fundamental rights and social guarantees, including the Labour Code (1943), were granted and several key social institutions were created such as the University of Costa Rica (1940) and the Costa Rican Social Security Fund Institute – *Caja Costarricense de Seguro Social* (CCSS).

The CCSS is responsible for providing healthcare services to 89.7 per cent of the population. Its network includes more than 30 hospitals (national, specialised, regional and peripheral) and 250 local health clinics scattered nationwide[9]. This health system not only includes medical treatment (illness and maternity) but also retirement (disability pension, old-age security pension and death pension).

Mandatory contributions of the State, employers and employees financed the CCSS. Nevertheless, with a 2010 deficit reaching 7.2 per cent of its total spending and a questionable management system, concerns were raised and placed on the public agenda in 2010-2011[10].

6 For additional data from the National Institute for Statistics and Census (INEC), please see www.inec.go.cr/

7 24.2 per cent of the total population.

8 6.8 per cent of the total population.

9 Data from Villalobos, Vilma and Monge-González Ricardo, Costa Rica´s Effort Toward an Innovation-Driven Economy: The Role of the ICT Sector, pp. 119-126, in The Global Technology Report 2010-2011, World Economic Forum.

10 XVII Report *Estado de la Nación*, op.cit

Education

In 1869, the political constitution stated that primary education was mandatory and free. Investment in education continued during the 20th century and the country achieved universal primary education during the 1950s[11]. Unfortunately, policy decisions taken in the 1980s, such as the reduction of the education budget, led to a "full-scale collapse of educational indicators"[12]. However, in the 1990s a constitutional reform guaranteed that public expenditure on education should be at a minimum of 6 per cent of GDP and, in 2011, it actually reached 7 per cent[13].

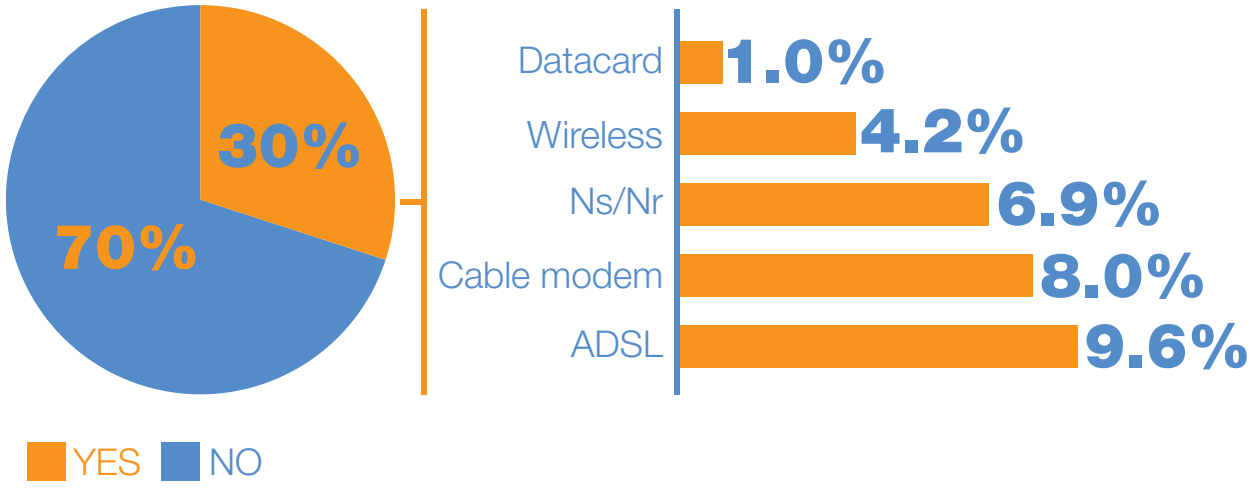
Nowadays, as pointed out in the 2011 report on the State of Education[14], a lot of progress, such as the increase of teachers´ salaries and the improvement of hiring strategies, has been made. However, several problems mainly regarding infrastructure and secondary school coverage still need to be resolved.

2.2 Internet access[15]

According to the latest survey conducted at the end of 2011 by the Ministry of Environment, Energy and Telecommunications (MINAET), 30 per cent of Costa Rican households have fixed (wired)-Internet. In rural areas 21 per cent of households have fixed-subscriptions, this percentage increasing to 35 per cent for households located in urban areas.

The figure below displays the type of technology used to access fixed Internet. Additional data reveals that there are no major differences between the types of technology used to access the Internet from one region to another.

Figure 2 — Type of technology used for fixed (wired) Internet



11 XVII Report *Estado de la Nación*, op.cit

12 Ibíd.

13 Speech by H.E. Laura Chinchilla, 1 May 2012, in Parliament.

14 Report *El Estado de la Education*, 2011, San José, Costa Rica. www.estadonacion.or.cr/index.php/biblioteca-virtual/costa-rica/english

15 Unless expressed otherwise, the data and statistics displayed in section 2.2 and all its subsections have been taken and translated from the national survey *Access, Use and Quality of Telecommunications Services* conducted in October and November 2011 by the Ministry of Environment, Energy and Telecommunications (MINAET) with the support of Demoscopía S.A. Data available since March 2012. www.telecom.go.cr/index.php/publicaciones2/publicaciones

2.2.1 Broadband connections

The National Plan for the Development of Telecommunications 2009-2014 has set the minimum speed for broadband at 512 kbit/s and in fact 47 per cent of households with fixed-Internet (30 per cent) have reached or exceeded this speed.

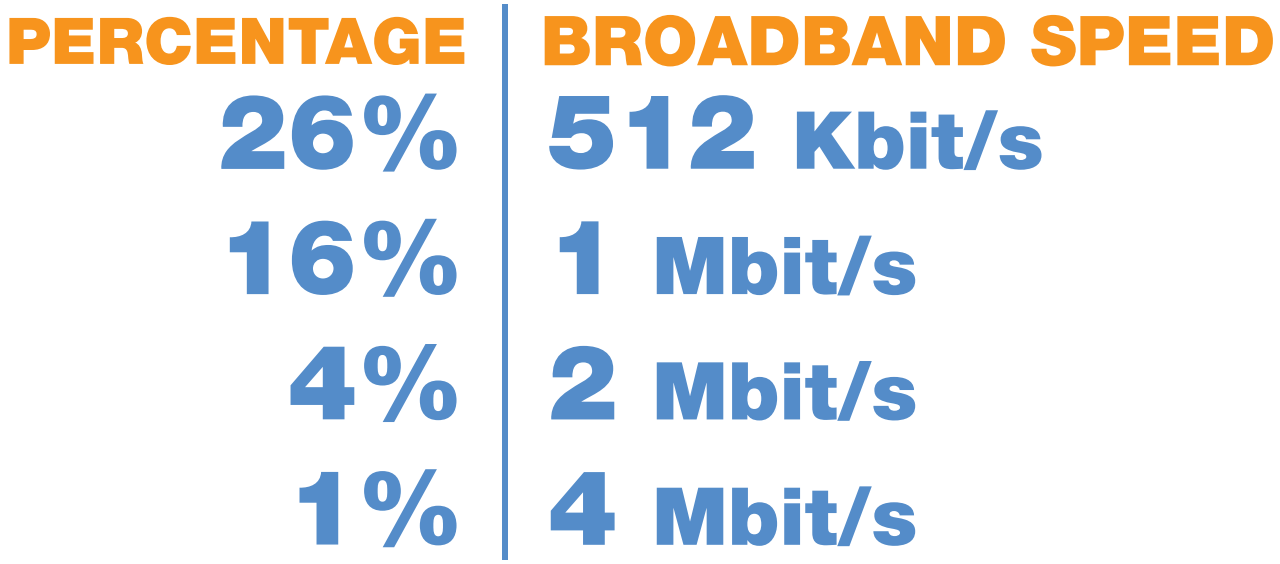


Figure 3 — Households with fixed broadband by speed, end of 2011

The Costa Rican Institute of Electricity (ICE), public operator, is the provider of 58.33 per cent of homes with fixed (wired)-Internet. This corresponds to the historical context that in 2008 the General Telecommunication Act officially opened the telecommunications market to competition. Prior to this, the State-owned ICE and its subsidiaries were the sole providers.

At the end of March 2012 the MINAET launched the National Strategy for Broadband and used data gathered on the use of broadband in the country to serve as a baseline. It is interesting to note that in 2010 the average penetration of fixed-broadband subscriptions per 100 inhabitants was 6.2.

The statistics for broadband use varies according to the region. The central region where the capital of San José is located concentrated the highest rate, with 20.5 per cent of its households with broadband, while the rest of the country registers numbers that range from 5 per cent to 10 per cent.

While in 118 administrative districts there are more than three broadband providers offering services, in 177 administrative districts the ICE is the sole provider offering broadband connection and in 88 districts no broadband services are available at all[16]. Notably, in 2010 the average penetration of fixed-broadband subscriptions[17] per 100 inhabitants was just 6.2[18] and its 43 per cent growth rate was much lower than in other South American countries.

[16] There are 473 districts in Costa Rica.

[17] With a 256 Kbits/s broadband speed.

[18] When considering fixed-broadband subscriptions and mobile-broadband subscriptions, the penetration rate reaches 13 per cent.

2.2.2 Computer ownership

In 2011, 46 per cent of Costa Rican households — whether they had Internet connection or not — reported having one computer (89 per cent had a desktop computer and 11 per cent owned one or more laptops). This showed an increase of 4.7 per cent in computer ownership[19]. It is important to point out that 50 per cent of households with one computer are located in urban areas, while 39 per cent are in rural areas.

Figures 4 and 5 below show the percentage of Internet users in households with fixed Internet and a computer, according to their age range and level of studies.

Figure 4 — Computer ownership, by age range

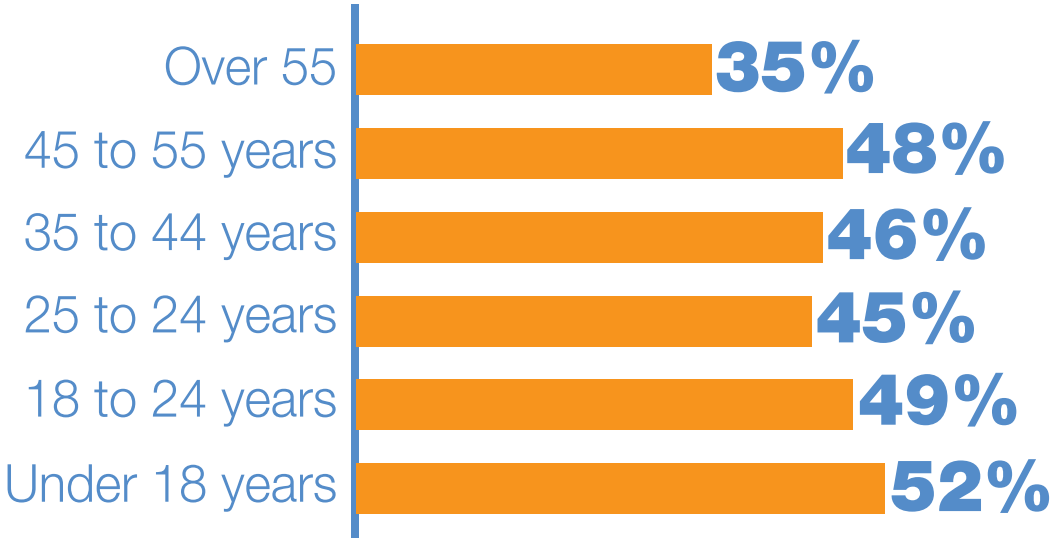
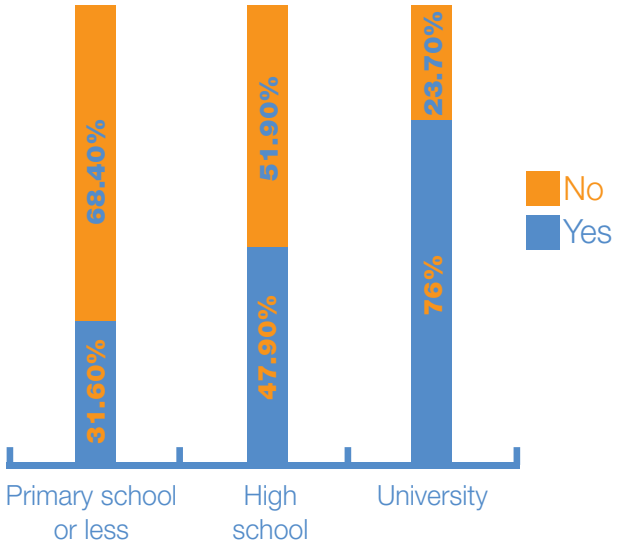


Figure 5 — Computer ownership, by schooling levels



The data above corroborates international findings regarding the link between years of studies and computer ownership.

[19] National Households Survey (ENAHO) from the National Institute for Statistics and Census (INEC), 2010 <www.inec.go.cr/Web/Home/GeneradorPagina.aspx> [Accessed: March 30, 2012)

2.2.3 Mobile-Internet subscriptions

Towards the end of 2011, 82 per cent of the Costa Rican population owned a mobile telephone; of this total, 33 per cent included a mobile-Internet subscription, 71.9 per cent of which comprising pre-paid services. Moreover, according to the National Households survey, 94 per cent of the people surveyed indicated that there was at least one mobile phone in their household, against 73.6 per cent in 2010, and 49.8 per cent in 2005.

Ownership of at least one mobile phone per household is now above 90 per cent in all Costa Rican regions, as detailed in the next box.

Figure 6 — Percentage of households with at least one cellular phone, by region

In terms of operators, ICE continues to dominate 97 per cent of the market, Tuyo 1.4 per cent and Full Móvil 0.5 per cent. However Movistar and Claro were not contenders in the market when the survey showing these results was conducted in October-November 2011.

REGION	PERCENTAGE
Central	94.8
Chorotega	94.5
Central Pacific	93.2
Brunca	90.5
Atlantic Huetar	94.2
North Huetar	97.9

2.2.4 Access at public schools

In 1987, the Omar Dengo Foundation (ODF) established a partnership with the Ministry of Public Education (MEP) to form the National Programme of Educational Informatics (PRONIE MEP-FOD). It started by targeting primary school students, but in other countries it also included secondary school students.

The objectives of the NPEI included improving the quality of teaching, familiarizing the population with informatics, reducing the technology gap between Costa Rica and other countries, and stimulating creativity and logical thinking through the use of computer devices[20]. Most of the curricular content is studied in computer labs or classrooms under the One Computer per Child Programme.

[20] The Global Information Technology Report 2010-2011, World Economic Forum, p. 122.

Displayed in the table below are the projections for 2012 regarding the number of students and institutions enrolled in the PRONIE MEP-FOD and the percentage of students registered in the public educational system.

Figure 7 — School and student beneficiaries of PRONIE MEP-FOD, by grade, 30 March 2012 (projection)[21]

TYPE OF PROGRAMMES	NUMBER OF INSTITUTIONS	NUMBER OF STUDENTS	COVERAGE (%)
Total	1156	475,889	63.7
(secondary)*	223	128,487	
(pre-scholl and primary)	953	347,402	

* It includes 958 students from 7th to 9th grades enrolled in 12 rural secondary schools with the One Computer per Student programme implemented by the ODF.

Figure 8 — Student beneficiaries of PRONIE MEP-FOD, by types of programmes and grades, 30 March 2012 (projection)[22]

GRADE	STUDENTS BENEFICIARIES
Total of students enroled	475,889
Pre-school	43,494
Primary (I-II cycle EGB 1)	295,900
Secondary (III cycle 2)	124,505
Special education (primary)*	2862
Special education (secondary)	3024
Open classroom*	4544
Children from welfare centres	602
Secondary rural schools (1:1)	958

* Special education attends students with disabilities.
* The Ministry of Public Education´s Open Classroom project enrolls primary and secondary school children and adolescents who have not completed the primary school cycle.

In October 2010, Quirós Tanzi established an alliance with the Ministry of Public Education with the aim of working specifically in public primary schools. The schools are located in four areas: Santa Teresita de Turrialba, Rio Claro de Grecia, San Isidro de Alajuela and Curridabat. Excluding Curridabat, all other areas are situated outside the Central Valley in rural parts of the country and the largest school population is 300 students.

The foundation is currently in its initial phase and is working with the 120 teachers, 15 directors and the parents of students enrolled in the participating schools, as well as key members of the communities where the schools

[21] Data provided by the Omar Dengo Foundation, 10 May 2012.
[22] Data provided by the Omar Dengo Foundation, 10 May 2012.

are located. Since the beginning of the school year in February 2012, they have delivered 1600 XO laptops to the student body of 15 primary schools. These students had no previous experience in using computers in the school environment. A computer is donated to each student[23], who uses it in the classroom and is then able to take the computer home. Plans for the 2013 school year include substantially expanding the programme and distributing another 8000 XO computers to students[24].

2.2.5 Access through free Wi-Fi hotspots

Since 9 February 2012 the Costa Rica Wireless Initiative has been implemented by the Ministry of Science and Technology (MICIT). A free Wi-Fi hotspot with a connection speed of 512 kbit/s has been installed on a boulevard [25] adjacent to the Ministry, which starts near the Parliament buildings and ends near the Supreme and judicial courts. According to the MICIT, 80 per cent of the people using this hotspot stay connected 10 to 15 minutes and 20 per cent stay connected one hour. A network technician from the MICIT regularly monitors traffic, mainly for security reasons.

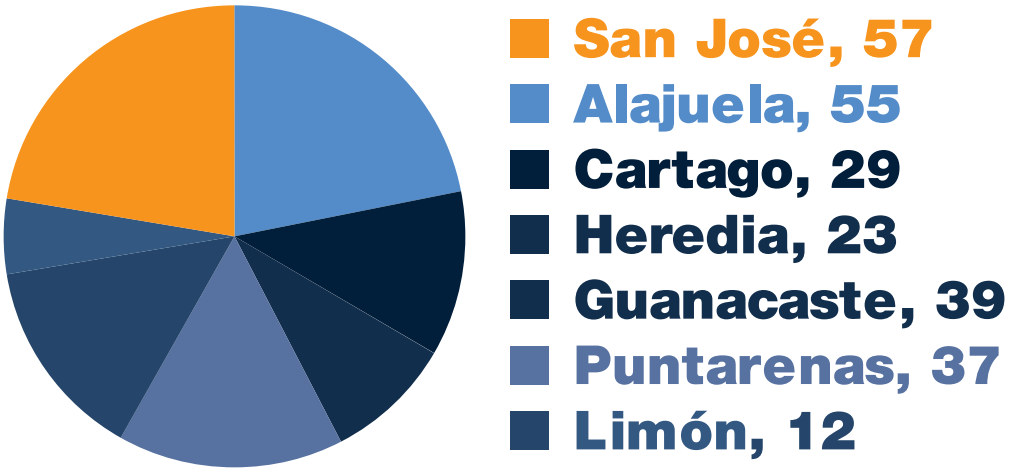
There are ongoing plans to replicate the experience in other strategic parts of the capital and in other cities[26]. For example, the Municipality of San José has plans to install free Wi-Fi hotspots on the central avenue.

2.2.6 Access through State-owned telecentres[27]

In 2006, the Ministry of Science and Technology initiated a programme called *Centros Comunitarios Inteligentes* (CECI), elsewhere known as telecentres. In 2007, an executive decree declared this programme to be of public interest[28]. The programme was conceived as a tool and a strategy to reduce the digital divide and promote a digital and productive culture.

Between August 2006 and November 2011, 279 telecentres were opened all over the country and in November 2011, 253 centres were still active. The current management of the MICIT noticed that the locations chosen for the telecentres didn't always correspond to objective criteria. This is reflected in the chart below:

Figure 9 — Distribution of CECI, by provinces, October 2011



So far, a predicted 400,000 to 450,000 people — approximately 10 per cent of the population — have used the CECI, according to a survey that the MICIT is currently conducting.

---

23 Known as One Laptop per Child or 1:1 model.

24 Carolyn Gourzong, pedagogical adviser, Juan Cubillo, technical coordinator and Sara de la Parra, pedagogical advisor from Quirós Tanzi, interviewed on 30 April 2012.

25 Known as the Oreamuno Boulevard.

26 Santiago Nuñez, op.cit.

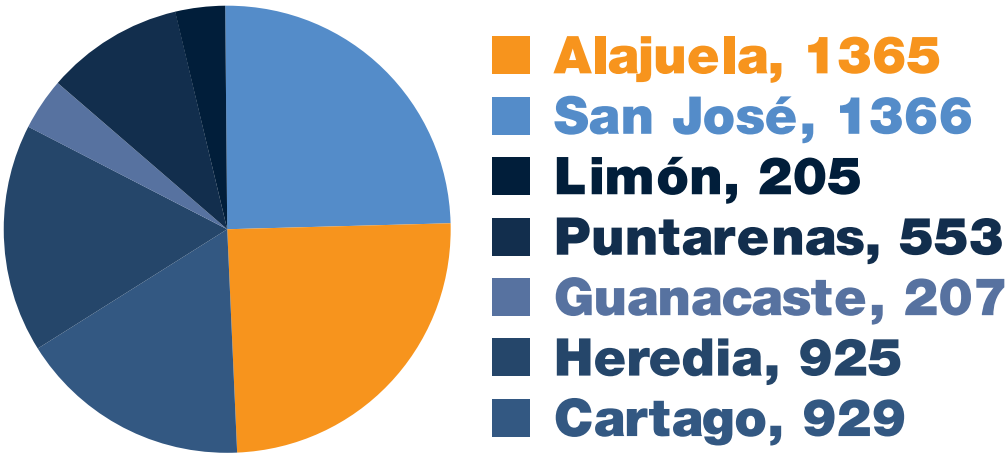
27 The information displayed in this section was obtained from two separate interviews respectively with Santiago Nuñez, Director of Digital Technologies and Oscar Quesada, Coordinator of CECIS (Ministry of Science and Technology), and from the report entitled *Proyecto CECI 2.0* (Ministry of Science and Technology) November 2011, San José, Costa Rica, unpublished.

28 Executive Decree N°33629, 20 February 2007. http://historico.gaceta.go.cr/pub/2007/03/21/COMP_21_03_2007.html

The existing CECI have six to 10 computers and provide free Internet access. The community provides the Internet connection, the staff and the facilities — usually an area of 20m² or more in a public library, university, school or municipality, etc. In return, the MICIT provides the computers, devices and maintenance. In some of the centres, the Linux operating system has been installed in order to reduce costs.

During the first phase (2006-2010), the telecentres were used by citizens as places where they could access the Internet for free. In some cases they received some basic training, mostly to strengthen their ICT skills. An estimated 5500 training activities have since been set up as shown in the chart below.

Figure 10 — Distribution of training activities, by provinces, October 2011



In May 2010, the project entered a second phase called CECI 2.0. which aims to reach 500 active CECI nationwide by 2014, to reactivate the existing ones when needed and to provide a better range of thematic contents for training purposes. The goals of this new phase are:

- to stimulate the entrepreneurship skills of the users;
- to provide online training opportunities to strengthen key personal and professional competencies, with 24 hours of training in total, six hours per week. The 'specificity' of each community's training needs will be taken into consideration (since 2012, 12 training modules have been offered to CECI users. One of the new modules currently being designed is about online safety); and
- to foster the habit of accessing public and private services online.

CECI 2.0 as a strategy contributed to the achievement of some of the objectives mentioned in the 2008 LGT[29] that opened the telecommunications market to competition. This law ensured that universality and solidarity would be the underlying principles guiding access to telecommunications and that citizens would have better opportunities to improve their quality of life. Furthermore, the LGT recognises the importance of 'inclusiveness' by providing access to broadband to rural areas, to lesser developed urban areas, to children's foster homes, to senior citizen homes, to indigenous people and to people with disabilities.

The costs of this new phase (estimated at 20 million USD) will be covered by the National Fund of Telecommunications (FONATEL), since it has been labelled a key project and was included in the Digital Social Agreement. FONATEL is a development fund that has been created specifically to administer the resources set out by LGT and the National Development Plan of Telecommunications. The General Telecommunication Act and the Strengthening and Modernisation of Public Entities in the Telecommunications Sector Act[30], that came into force in August 2008, outline the modalities. The goal is to have the first project financed through FONATEL up and running by the end of 2012[31].

---

29 Known as the "*Ley General de Telecomunicaciones*" (LGT), Law N° 8642 published in the Official Gazette N° 125, 30 June 2008. http://historico.gaceta.go.cr/pub/2008/06/30/COMP_30_06_2008.pdf

30 Law N° 8660 "*Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones*" (LMFT) published in the Official Gazette N° 156, 13 August 2008. http://historico.gaceta.go.cr/pub/2008/08/13/COMP_13_08_2008.html#_Toc206304472

31 Maryleana Méndez, member of the Council of Directors, Superintendency of Telecommunications. Interviewed on 27 June 2012.

The financial resources of this fund are derived from a special para-fiscal charge that operators of public telecommunication networks and telecommunications service providers are obliged to pay. This is in addition to concessions, fines and interest paid for delay and donations, among others. The exact percentage of the annual gross income that the operators will have to transfer to this fund is determined annually, and by law, and oscillate between 1.5 per cent and 3 per cent.

2.3 Internet users

The use of fixed Internet in households nationwide is primarily recreational and email is the main service used, as detailed in Boxes 11 and 12.

Figure 11 — Uses of fixed Internet nationwide, late 2011

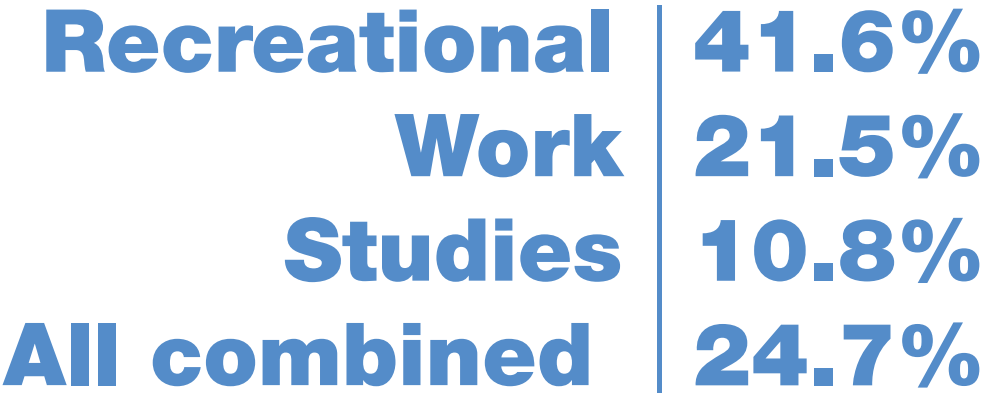
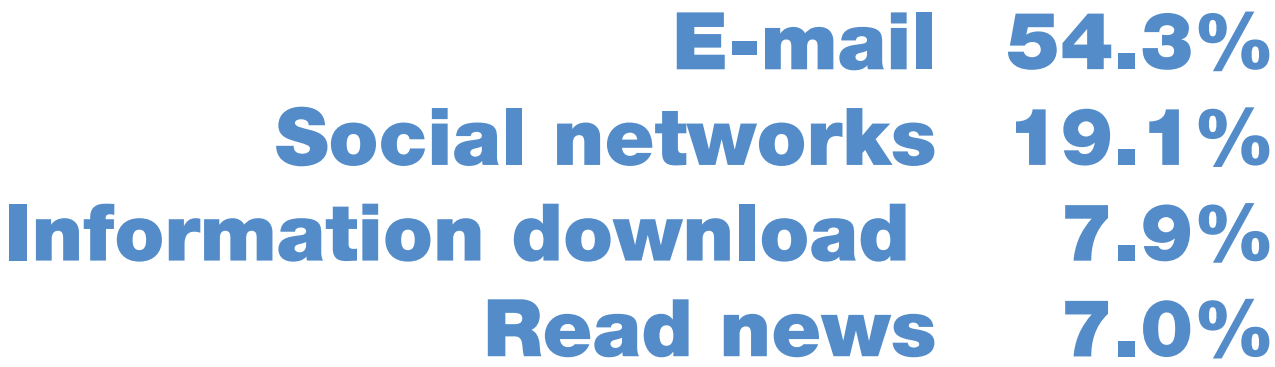


Figure 12- Main Internet applications and services used, fixed Internet, nationwide, late 2011



A survey in 2010[32] conducted with a group of secondary school students (private and public) in the metropolitan area revealed that 37.4 per cent were connected three to five hours weekly while another 21 per cent admitted to being online more than 20 hours a week— an average of almost three hours daily. Nationwide in 2011, the amount of time spent on the Internet was less than two hours a day for 50.24 per cent of households with fixed Internet but was above five hours for 15 per cent of them.

[32] *Conocimientos, Actitudes y Prácticas Asociados al Uso de Internet en Adolescentes, Informe sobre Estudio CAP en los Colegios de la Región Metropolitana*. Paniamor Foundation, with the support of Save the Children Sweden and Racsa S.A., May 2010. Available at http://paniamor.org/interactivo/centrodoc/uit.html (accessed: 2 May 2012)

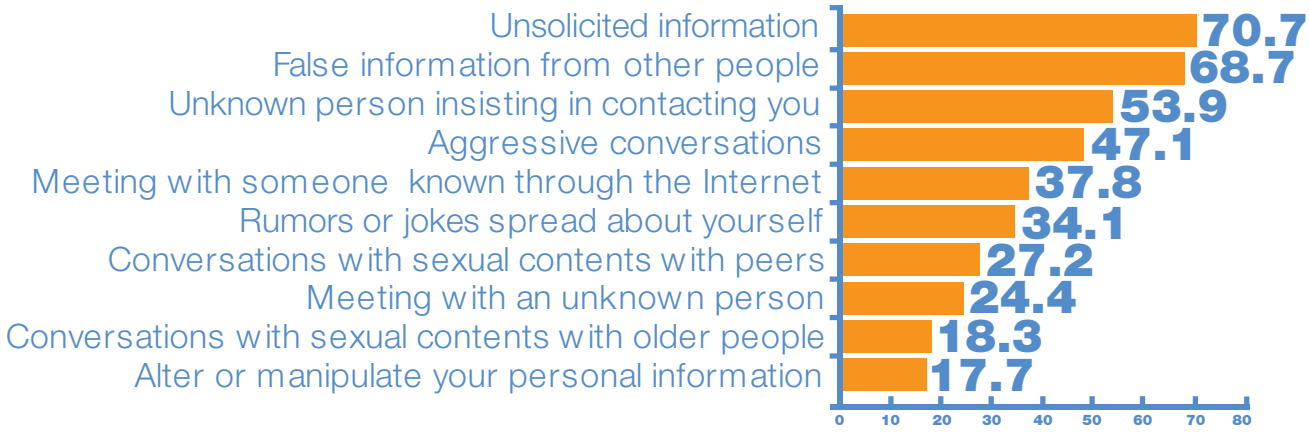
With regard to social networks[33], in 2011 45 per cent of people aged between 12 to 75 residing in the rural and urban metropolitan areas (GAM)[34] had a profile on a social network. As we usually see in other countries, the proportion of minors using social networks is higher than adults. Six out of 19 minors had a profile, while only one in four adults had one.

Facebook is the predominant social network, concentrating 97 per cent of the sample. In fact, 60 per cent of 12- to 17- year olds in the gran metropolitan area (GAM) had a Facebook profile — compared with 46 per cent of Europeans aged 13 to 16[35]. GAM youth spent an average of 150 minutes a day connected to the social network of their preference.

In terms of mobile Internet connections 50 per cent are used for recreational purposes, compared with 18.9 per cent for work purposes. Among the applications and services accessed via mobile Internet, the most popular are emails and social networks (combined accounting for 45 per cent) and music downloads (accounting for 17 per cent).

Finally, almost 50 per cent of the teenagers surveyed admitted having received or accessed pornography while surfing randomnly, while 30 per cent of them admitted having actively searched this kind of content. The figure below illustrates different types of risks faced by teenagers online.

Figure 13 — Victimisation on the Internet (early 2010)[36]



[33] Survey conducted by Unimer on the use of the Internet and social networks for the national newspaper El Financiero between 18 and 30 March 2011. Available at www.elfinancierocr.com/ef_archivo/2011/julio/31/enportada2850796.html [Accessed: April 2, 2012].

[34] GAM includes major cities of the central valley, such as the capital, San José as well as Heredia, Cartago and Alajuela, and surroundings. The sample of 800 contacts is representative of a population of 1,816,000 residing in the GAM. As a reference, in 2011 the total population of Costa Rica was 4,301,712.

[35] Livingston, Sonia et al., op.cit, p.18.

[36] Taken and translated from the Paniamor survey, op.cit.

3. NATIONAL BODIES/AGENCIES DEALING WITH CYBERSECURITY

3.1 Government

The main governmental agency in the field of cybersecurity is the Computer Security Incident Response Team Costa Rica (CSIRT-CR) formally created on 13 April 2012, following the publication of a presidential executive order in the Official Gazette[37].

A Computer Security Incident Response Team (CSIRT) "is a service organization that is responsible for receiving, reviewing and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporation, governmental or educational organization; a region or country; a research network; or a paid client. A CSIRT can be a formalized team or an ad hoc team. A formalized team performs incident response work as its major job function. An ad hoc team is called together during an ongoing computer security incident or to respond to an incident when the need arises"[38]. Each centre will define what exactly constitutes a computer incident threat.

The idea of such a structure was first conceived in the Ministry of Science and Technology in early 2000, and was revisited during the administration of the former President Oscar Arias (2006-2010).The authorities involved at the time made initial contacts with the Organisation of American States. Towards the end of 2009, the Ministry of Science and Technology (under the leadership of minister Alejandro Cruz) gave its final endorsement to the recently established CSIRT-CR. The Ministry of Science and Technology is responsible for CSIRT-CR's daily operations. Its budget for 2012 is approximately USD 59,000[39] and, in addition to the two MCIT personnel already assigned to the daily operations, six full-time employees will be appointed over the next few months[40]. It is important to note that the CSIRT-CR has been declared a project of public interest[41], which has implications, specifically in relation to getting financial support from other public institutions.

Picture courtesy of the Quirós Tanzi Foundation and taken by Once Fotografía

37 The Official Gazette N° 37052, 13 April 2012. http://historico.gaceta.go.cr pub/2012/04/13/COMP_13_04_2012.html#_Toc321989832

38 From www.cert.org/csirts/csirt_faq.html [Accessed: 5 July 2012].

39 In domestic currency: 30 millions CRC. As of 19 April 2012: 1 USD = 508,91 CRC.

40 Newspaper La Nación, 18 April 2012, www.nacion.com/2012-04-18/Portada/Nace-centro-tico-para-prevenir-y--atender-ataques-informaticos.aspx [Accessed: 19 April 2012]

41 The President has the power to declare "of public interest" any project identified as key for the country, according to article 140 of the Constitution.

The CSIRT-CR is a national governmental entity, therefore its main objective is to mitigate risks and cyberthreats that could affect the interests of the central government of Costa Rica and autonomous entities[42], even if its mandate also includes strategies that enhance ICT security for citizens.

According to the terms of the decree, the objectives of the CSIRT-CR are[43]:

- to act as a consultative agency to the Presidency regarding legislation in the field of ICT security;
- to support judicial authorities and law enforcement in the investigation and prosecution of cybercrime cases;
- to sponsor the adoption of public policies aimed at fostering the efficiency of computer resources within the public sector;
- to promote and supervise contingency planning in ICT security within the public sector;
- to propose guidelines for the evaluation of the inter-institutional programmes in ICT security;
- to promote research and training projects in ICT security;
- to coordinate with the Inter-American Committee against Terrorism (CICTE) and other national and international entities with a view to developing strategies, guidelines and policies for the acquisition of ICT security goods and services for the public sector, in light of existing international standards;
- to orient public and private initiatives conducive to improved development of ICT security and better protection for citizens;
- to propel the development and execution of national policies and strategies in ICT security among private and public entities;
- to promote a culture of cybersecurity at national level; and
- to coordinate national actions towards a general enhancement of ICT safety.

In order to achieve the objectives mentioned above, the CSIRT-CR has defined key tasks it will have to perform, as illustrated in the diagram below.

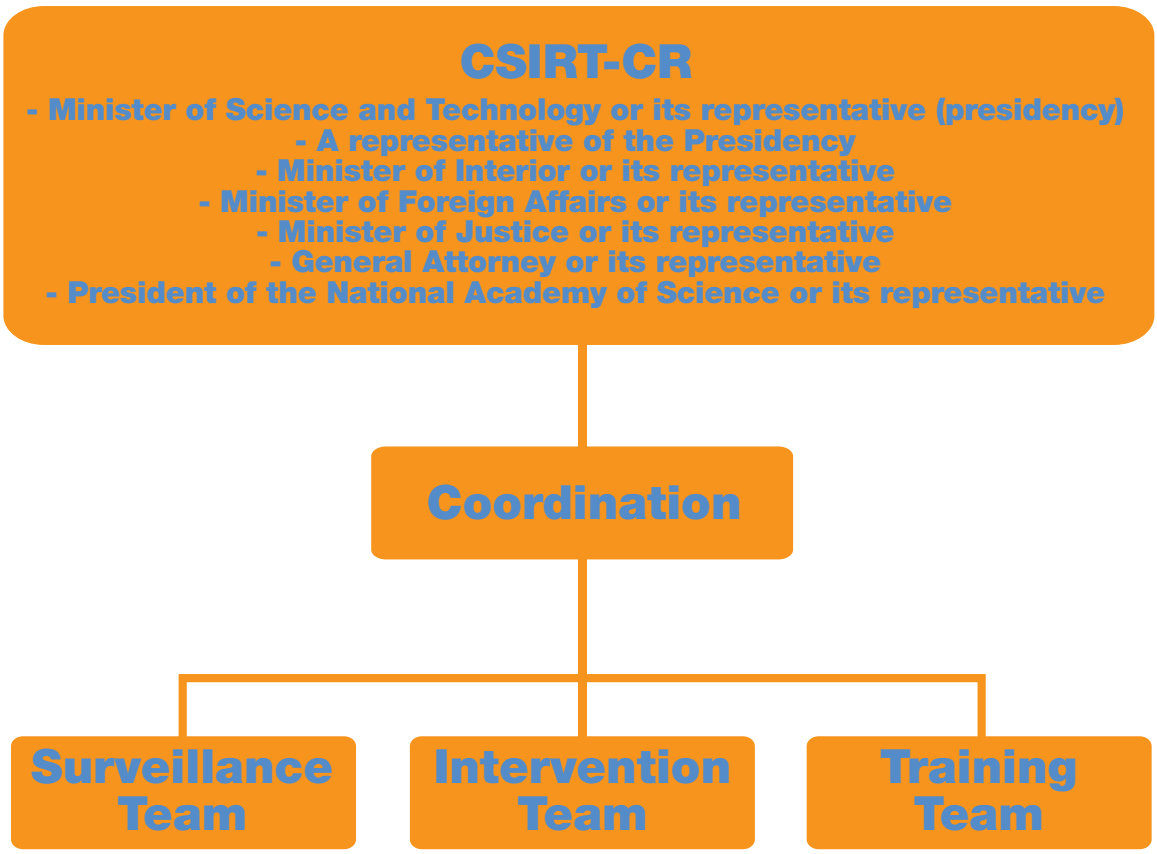
Box 2 — Key tasks of the CSIRT-CR

[42] Santiago Nuñez, Director of Digital Technologies, Ministry of Science and Technology. Interviewed on 10 April 2012.

[43] Extracted and translated from the Executive Decree N° 37052, op.cit.

Regarding its structure, the decree specifies that there will be a Council of Directors that will include a representative from each key public institution, as detailed below.

Box 3 — Structure of the CSIRT-CR and composition of the Council of Directors



Source: Extracted, adapted and translated from a presentation elaborated in its original version in Spanish by Eduardo Jiménez González of the Ministry of Science and Technology, San José, Costa Rica, 2012.

The first formal meeting of the Council of Directors was expected to be held in May-June 2012. A workplan was to be submitted for approval before December 2012. In April 2012, during the preparatory discussions, the components shown in Box 4 were identified as key for the future workplan.

Box 4 — Key components of the CSIRT-CR workplan

Source: Extracted and translated from a presentation elaborated in its original version in Spanish by Santiago Nuñez from the Ministry of Science and Technology, San José, Costa Rica, 2012.

In order to attend to specific issues, specialized commissions attached to the CSIRT-CR will be created. It is anticipated that one of these commissions will attend to security issues relating to the banking sector, which has been perceived by representatives of the Organism of Judicial Investigation and NIC-Costa Rica as positive news[44]. There is also the possibility of transforming the existing National Commission on Online Safety, which has been operating since November 2010, into a specialised commission dedicated to the online safety of children[45].

According to Mr Nuñez, Director of Digital Technologies of the Ministry of Science and Technology, one of the first task of the new Council of Directors should be to address the issue of protection of key public institutions such as the Presidential House, the Central Bank of Costa Rica and the Ministry of Treasury.

The newly created CSIRT-Costa Rica integrates a network of 16 Computer Incidents Teams based in North and South America, as illustrated in Box 3, and a wider network of centres scattered around the world.

[44] Interviews with Luis Diego Espinoza, NIC-Costa Rica and Erick Lewis, Computer Crimes Section, respectively 24 April 2012 and 3 May 2012.

[45] Santiago Nuñez, op. cit.

Map 2 — CSIRTs in North and South America

CSIRTs - 2012

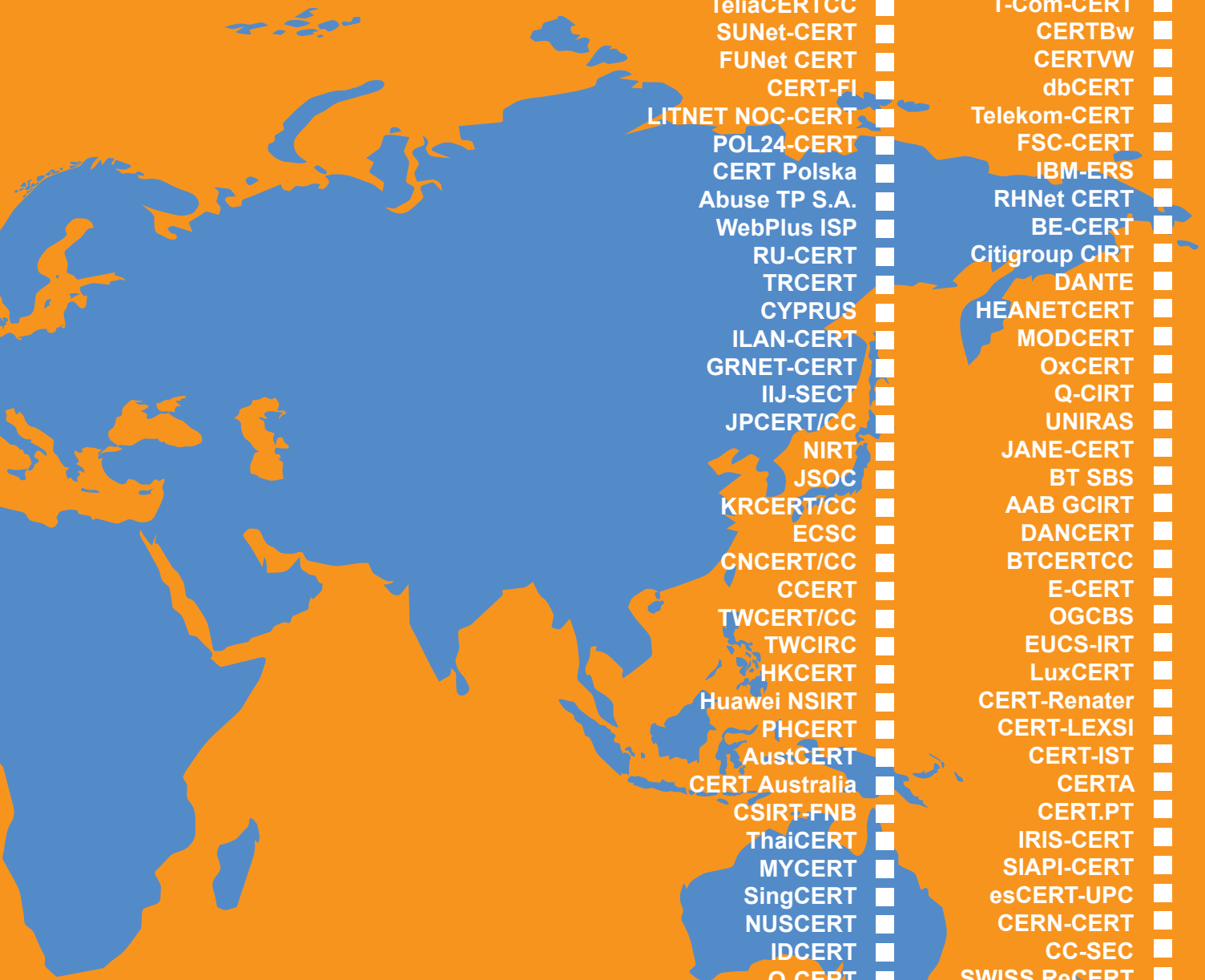
In process

Source: Copied, adapted and translated from an original presentation made in Spanish by Belisario Contreras, CICTE-OAS. San José, Costa Rica, March 2012.

Map 3 — Map of CSIRTs around the world

- PSU
- Cornell University
- UCERT
- Guardent
- RADIANZ
- Goldman Sachs
- IBM MSS
- VISA-CIRT
- MLCIRT
- AT&T
- PruCERT
- JPMC CIRT
- UB-FIRST
- FRS-CERT
- MIT Network Security
- NASIRC
- NIHIRT
- Rutgers CIRT
- ACIRT
- SBACERT
- NIST IT
- FCC CIRT
- ACERT
- IRS CIRT
- FedCIRC
- N-CIRT
- HOUSECIRT
- US Coast Guard CIRT
- ARCcert
- DoD-CERT
- USPS
- GI REACT
- NAVCIRT
- SPRINT
- MARCERT
- K-State SIRT
- NARIS
- CSE
- EWA-Canada
- RBCFG CSIRT
- DND CIRT
- CGI CIRT
- BMO ISIRT
- Cdn CIRCC
- CERT/AQ
- AboveSecCERT
- OSU-IRT
- PCERT
- IU-CERT
- Uchicago Network Security
- DIRT
- BadgIRT
- NCSA-IRST
- NU-CERT
- CERT/CC
- US-CERT
- CSIRT Panama
- TESIRT
- Brasil Telecom CTR/DPD
- CAIS/RNP CSIRT Unicamp
- CSIRT ABN AMRO REAL
- CSIRT Santander Banespa
- CSIRT USP NBSO/Brazillian CERT
- GSR/INPE
- CEO/RedeRio EMBRATEL Star One
- CLCERT
- ArCERT
- CERT-RS
- WFCSIRT
- MCIRT
- MSCERT
- BCERT
- Apple
- GIST
- CIAC
- Siebel
- SUN
- Cisco Systems
- SymCERT
- Foundston
- ORACERT
- PCH
- NAI
- Cisco-PSIRT
- SGI
- HP SSRT
- CAT
- Motorola
- Veridian
- AFCERT
- eForensics
- EDS
- MCIWorldCom
- UNAM-CERT
- MOREnet
- UGaCIRT
- ELN-FIRST
- ISS
- GT.CERT
- State of Florida CSIRTs:
  - Executive Office of the Governor
  - State Technology Office
  - Business and Professional Regulation
  - Children and Families
  - Corrections
  - Environmental Protection
  - Financial Services
  - Health
  - Healthcare Administration
  - Highway Safety and Motor Vehicles
  - Lottery
  - Management Services
  - Military Affairs National Guard
  - Revenue
  - Transportation
  - Veteran's Affairs
  - Workforce Innovation
  - FDLE CIRT

Source: www.cert.org/csirts/



UNINETT CERT
KMD IAC
GovCERT.DK
DK-CERT
CSIRT.DK
NORDUnet
SITIC
UU-IRT
TeliaCERTCC
SUNet-CERT
FUNet CERT
CERT-FI
LITNET NOC-CERT
POL24-CERT
CERT Polska
Abuse TP S.A.
WebPlus ISP
RU-CERT
TRCERT
CYPRUS
ILAN-CERT
GRNET-CERT
IIJ-SECT
JPCERT/CC
NIRT
JSOC
KRCERT/CC
ECSC
CNCERT/CC
CCERT
TWCERT/CC
TWCIRC
HKCERT
Huawei NSIRT
PHCERT
AustCERT
CERT Australia
CSIRT-FNB
ThaiCERT
MYCERT
SingCERT
NUSCERT
IDCERT
Q-CERT
PAKCERT
CERT-IN
CERT-BUND
AMC-CERT
CERT-KUN
SURFnet-CERT
NCSC-NL
CERT-UU
CERT-RUG
KPN-CERT
UvA-CERT

Micro-BIT
DFN-CERT
Siemens-CERT
S-CERT
PRECERT
ComCERT
RUS-CERT
dCERT
T-Com-CERT
CERTBw
CERTVW
dbCERT
Telekom-CERT
FSC-CERT
IBM-ERS
RHNet CERT
BE-CERT
Citigroup CIRT
DANTE
HEANETCERT
MODCERT
OxCERT
Q-CIRT
UNIRAS
JANE-CERT
BT SBS
AAB GCIRT
DANCERT
BTCERTCC
E-CERT
OGCBS
EUCS-IRT
LuxCERT
CERT-Renater
CERT-LEXSI
CERT-IST
CERTA
CERT.PT
IRIS-CERT
SIAPI-CERT
esCERT-UPC
CERN-CERT
CC-SEC
SWISS ReCERT
SWITCH-CERT
IP+CERT
OS-CIRT
SI-CERT
ACOnet-CERT
CERT-IT
GARR-CERT
CARNet-CERT
HUNGARNet-CERT
Hun-CERT
KCSIRT

Regarding international cooperation, the Ministry of Science and Technology is currently receiving support from the Inter-American Committee Against Terrorism of the Organization of American States.

Examples of possible activities in cooperation with the CICTE-OAS are:

- to receive support for the development of a national cybersecurity strategy;
- to organise meetings with key actors in the field[46];
- to attend specialised courses;
- to organise visits to other CSIRTs;
- to receive visits from partners of other national CSIRTs from Latin America in order to foster:
  - the exchange of good practices
  - the sectorial promotion of the CSIRT
- pending request to the CICTE-OAS to become a national contact point[47].

Other potential activities in cooperation with REMJA-OAS[48] are:

- to conduct analysis of crime activity against computer and data in State Members; and
- to conduct a study on legislation, policies and national practices regarding cybercrime[49].

The creation of the CSIRT-CR is one of three projects by the Ministry of Science and Technology intended to create and promote a culture of digital safety. The other two are the telecentres (CECIS 2.0) and the Costa Rica Wireless projects, both mentioned in detail in the previous section.

Box 5 — Articulation of national strategies

Action Line 3.2 of the National Plan of Science, Technology and Innovation 2011-2014, which includes the topic of digital safety, is detailed below.

---

46 Such as the Regional Workshop on Cybercrime and Cybersecurity Policies and Legislation in Central America, co-organized by MICIT/OAS-CICTE/CoE, which took place from 7 to 9 March 2012, San José, Costa Rica, prior to the ICANN43 meeting. www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_phase3_2571/2571_costarica_ws/2571_CR_regional per cent20ws per cent20_agenda_V10_15Feb12.pdf

47 Extracted, adapted and translated from a presentation elaborated in its original version in Spanish by Eduardo Jiménez González of the Ministry of Science and Technology, San José, Costa Rica, 2012 prior to the ICANN43 meeting.

48 The REMJA process is the premier policy and technical forum at regional level on matters related to the strengthening of and access to justice and international legal cooperation in areas related to mutual legal assistance in criminal matters, extradition, penitentiary and prison policies, cybercrime and forensic sciences, among others.

49 Eduardo Jiménez González, op.cit.

Box 6 — Digital safety in the national plan of science, technology and innovation

Strategy 3: Social appropriation of science and promotion of scientific technological vocations as well as entrepreneurship spirit.

Objective
To develop actions to enhance the dissemination, perception, appropriation, social recognition and use of science, technology and innovation.

ACTION LINE	2011-2014 GOALS	RESOURCES REQUIRED	ACTORS INVOLVED
3.2. To promote the acceleration and spread of access, use and appropriation of digital technologies among all sectors of the population nationwide.	3.2.1. To implement the Costa Rica Wireless Programme. 3.2.2. To strengthen and improve local public access points to digital technologies in local communities nationwide (CECI´s 2.0). 3.2.3. To enhance the Digital Signature Programme. 3.2.4. To contribute to other initiatives related to the Social Digital Agreement, such as: network connectivity in schools, digital government, cybersecurity programmes.	CR Wireless: 15 million USD Telecentres (CECIs): 10 million USD	MICIT Digital Government Programme Presidential House Parliament SUTEL MIDEPLAN OAS- POETA UTN Omar Dengo Foundation ITU

Source: Data extracted, translated and adapted from the National Plan of Science, Technology and Innovation 2011-2014.

3.2 Public institutions

NIC-COSTA RICA is a unit that manages the country code top-level domain and provides services for 14,000 domain names registered in the country. It belongs to the National Academy of Science, a public institution which is part of the national system of science and technology.

TECHNICAL AND PROCEDURAL MEASURES:

During the last ICANN43 meeting that took place in Costa Rica on 11-16 March 2012, NIC-Costa Rica announced that, after four years of research and testing, it had finally deployed the DNSSEC protocol. DNSSEC is a tool that prevents a specific type of attack called man-in-the-middle while attacking DNS servers.
Thus, NIC-Costa Rica joined a group of four Latin American countries that have deployed the protocol[50].

Box 7 — What is DNSSEC?

"DNSSEC is a protocol that is currently being deployed to secure the Domain Name System (DNS), the Internet's global phone book. [...] DNS matches each name to a numeric address so that data transfers to the right device. DNSSEC abbreviates "DNS Security Extensions." DNSSEC adds security to the DNS by incorporating public key cryptography into the DNS hierarchy, resulting in a single, open, global Public Key Infrastructure (PKI) for domain names. It is the result of over a decade of community based, open standards development"*.

*** http://dnssec-deployment.icann.org/dnsseccard.pdf [Accessed: April 25, 2012]**

3.3 Regulators

The Costa Rican telecommunications market was State-controlled since its creation on 8 April 1949[51] until the process of market opening that started with the adoption of the DR-CAFTA treaty, in 2007. Several laws reforming the sector were enacted and eventually, towards the end of 2011, the first private operators were allowed to compete alongside the public structure.

Box 8 — Key legislation governing Costa Rica´s telecommunication sector

The DR-CAFTA 2007 "Dominican Republic-Central America Free Trade Agreement (TLC) came into force in 2007. It set the general conditions for the opening of the telecommunications services sector in Costa Rica.

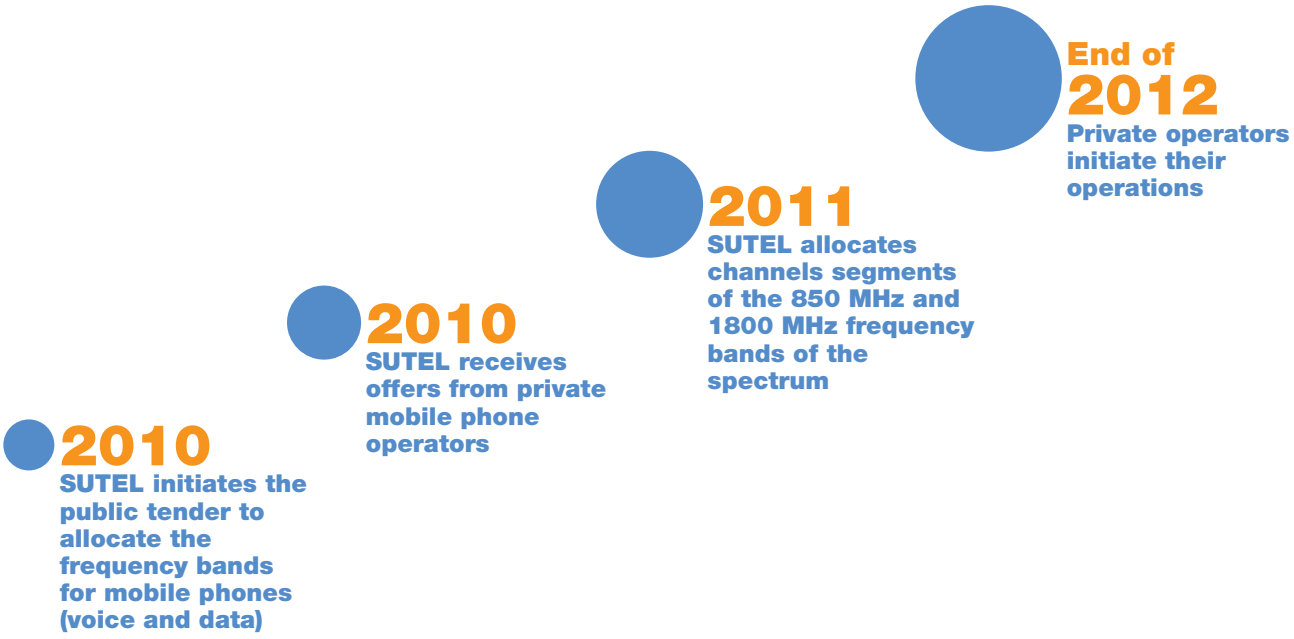
The Telecommunications Act* (LGT) came into force in July 2008. It defined the legal framework of telecommunications, including the rights of end users to privacy; the responsibilities of network operators and telecommunication services providers; the conditions for the use of public radio spectrum, among others, and created FONATEL.

The Strengthening and Modernisation of Public Entities in the Telecommunications Sector Act* came into force in August 2008. It created an independent regulatory authority called SUTEL and established the Ministry of Environment, Energy and Telecommunications as the State authority in the field. SUTEL was attached to the Regulatory Authority of Public Services (ARESEP), which deals with all other sectors except telecommunications.

*** Know as the "*Ley General de Telecomunicaciones*" (LGT), Law N° 8642, op. cit.**
*** Law N° 8660 "*Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones*" (LMFT), op.cit.**

[50] Luis Diego Espinoza, Director of Digital Technologies, NIC-Costa Rica. Interviewed on 25 April 2012.
[51] Decree-law creating the ICE N° 449. www.aresep.go.cr/docs/Ley per cent20449_CREACION per cent20DEL per cent20ICE.pdf

Box 9 — Key landmarks in the process of market opening



Source: Information obtained and translated from a presentation made by Freddy Artavia of SUTEL during the Regional Workshop on Cybercrime and Cybersecurity Policies and Legislation in Central America. 7-9 March 2012, San José, Costa Rica.

On 30 April 2012, the Costa Rican Parliament approved by a large majority the transfer of the Vice-Ministry of Telecommunications from the Ministry of Environment, Energy and Telecommunications to the Ministry of Science, Technology and Innovation. According to the Minister of Science and Technology, the expected outcome of the reform was its final approval in the shortest possible time. Afterwards, the Executive Branch authorities would have six months to implement the transfer[52]. Since 2008 the Ministry of Environment, Energy and Telecommunications, known as MINAET, has led the telecommunications sector through its Vice-ministry of Telecommunications and, among other things, is in charge of:

- Defining policies for the use and development of telecommunications;
- Elaborating the National Telecommunications Plan and its subsequent executive regulations;
- Coordinating the National Plan of Telecommunications Development;
- Supervising the implementation of policies in telecommunications by the public and private sector;
- Coordinating telecommunication policies with other public policies related to the promotion of an information society;
- Assessing the technical criteria of SUTEL regarding concessions and permits to use radio-frequency spectrum; and
- Formulating public interest for the expropriation or forced easement of assets needed for the operation of public telecommunications networks.

[52] Interview of the Minister of Science and Technology to the national newspaper El Diario Extra, published on 4 May 2012. www.diarioextra.com/2012/mayo/04/nacionales.php

Box 10 — SUTEL´s organizational chart

SUTEL's mission is to "guarantee the rights of the citizens to access telecommunications services, while promoting effective competition as a mechanism to increase the availability of services, applying the principles of transparency, universality and solidarity, ensuring the efficiency, continuity, parity, coverage and information at affordable rates" [53].

Its main functions are:

- to oblige operators to give free access to networks and services;
- to stimulate investment in the sector;
- to deliver authorizations and technical opinions to the Executive branch in order to allocate, extend, cease or extinguish permits or concessions;
- to manage and control the efficient use of the spectrum;
- to resolve conflicts between operators and telecommunication services providers;
- to endorse contracts between operators and end users;
- to elaborate technical norms; and
- to determine telecommunication tariffs according to the law.

In line with its legal mandate, SUTEL has developed and implemented several specific strategies that will now be detailed below.

Internet cafés and child protection

According to law, all Internet cafés should be registered with SUTEL. Not all Internet cafés register as required, but the official number of registered Internet cafés is 452.

On 8 September 2011, the Law on the Protection of Children and Teenagers against Internet Harmful Content and Other Electronic Means came into force. This law obliges all establishments offering Internet access to the public to install filters in computers used by minors. Such filters aim to block access to harmful content such as websites promoting racism, war, bad language, the use of drugs, physical, sexual and emotional violence, and websites displaying adult and child pornography.

These establishments were also required to display a visible sign warning minors of the dangers of revealing on social networks, chatrooms and forums private information that could have an impact on their moral and physical integrity. It will be up to each business owner to interpret this legal obligation and implement it.

Early April 2012, SUTEL issued a Council Agreement informing Internet cafés of their new obligations, detailing the documents that must be presented to prove they had installed the appropriate licensed software and the sign, required by law (effective 8 September 2012). Once the owners fulfill the requirements, SUTEL will issue a certification stating that the establishment complies with regulations that require the installation of filters to block online pornography and harmful content.

In addition to issuing certifications, SUTEL is legally obliged to send inspectors to visit Internet cafés to verify whether they comply with the terms of the Law on the Protection of Children and Teenagers against Internet Harmful Content and Other Electronic Means.

Copyrights legislation for service providers

In October 2011[54], the Ministry of Foreign Trade set up a framework for the rights and obligations of service providers in case of breach of legal copyrights when providing services such as hosting, caching and mere conduit. It specified the collaborative measures between service providers and copyright owners that the former can implement in order to deter unauthorized storage and transmission of copyright materials. It also stipulated limitations and exemptions of the liability of service providers in cases where protected contents were not under their control and did not originate from or were not directed by them.

---

53 www.sutel.go.cr/Ver/Contenido/vision-y-mision/38 [Accessed: 14 April 2012]

54 Known as *the Reglamento sobre la Limitación a la Responsabilidad de los Proveedores de Servicios por Infracciones a Derechos de Autor y Conexos con el Artículo 15.11.27 del Tratado de Libre Comercio República Dominicana-Centroamérica-Estados Unidos*. N° 36880-COMEX-JP, published in the Official Gazette N°242, 16 December 2011. http://historico.gaceta.go.cr/pub/2011/12/16/COMP_16_12_2011.pdf

According to this law, service providers should include in the contract signed by their subscribers specific provisions detailing the grounds for blocking a user account or for stopping a contract in case of repeated infringement of copyright law. Compliance with this regulation is not mandatory. Nevertheless, once service providers agree to abide by it, the company is normally required to modify provisions of the contract, as was the case of RACSA S.A.[55] One of SUTEL´s functions is to ratify contracts between operators and subscribers, therefore concerned service providers have to submit for approval the changes made to their contracts.

End-user privacy and data protection

The 2008 Telecommunications Act (LGT)[56] states in article 42 that operators of public networks and telecommunication service providers should guarantee the secrecy of telecommunications, the right to privacy and the protection of the personal data of subscribers and end users through the implementation of technical and administrative measures. In April 2009, MINAET made the ruling compulsory for all operators and telecommunication services providers[57].

According to paragraph 2, operators should inform SUTEL of any recognizable risk threatening network security. Paragraph 3 goes on to stipulate that the operators and providers should guarantee that communications and any associated trafficking data should not be listened to, taped, stored, intercepted or monitored by third parties without consent, except when there is a judicial order.

Another key piece of legislation came into force in July 2011[58] to regulate the use of personal data of individuals. Based on the mandate of SUTEL to protect the interests and the rights of end users, the superintendency has worked with operators to make sure that the contracts signed by the clients clearly indicated whether the client consented or not to the sharing of his or her data.

Ongoing collaboration with the judicial authorities

The Computer Crimes Section of the OIJ first contacted SUTEL in 2009 to discuss the need for a protocol that would clarify the legal rules and obligations of all telecommunication operators when approached by judicial powers. In 2011, a committee of legal and technical representatives was established to draft such a document. The final version was to be issued in May 2012 and SUTEL intends to make it a compulsory ruling.

One of the key aspects regulated by the documents would be related to the periods of response that the operators should respect to provide judicial and police authorities with the required information extracted from their systems. This ruling is perceived as key by judicial powers, since operators have often delayed in providing such data.

Agreement with GSMA[59]

An agreement signed by SUTEL with GSMA and the five operators — Movistar, Claro, ICE, Tuyo Móvil and Fullmóvil — obliges each company to create a reporting mechanism for their clients, should their phones be stolen. This information will then be passed on to an international database operating in 219 countries, receiving information from 189 operators and updated every 24 hours. As of April 27, an average of 850 stolen mobile phones were reported by each company.

A testing period for the newly created reporting mechanism was agreed upon with the operators, running from 5 April until 5 May 2012, when the official launch took place.

The agreement was the result of consensus among existing mobile phone companies. However, the new procedures will make it compulsory for each new company interested in operating in the country to join the initiative.

---

55 RACSA S.A. is a public company and provides Internet services since 1994. Ana Catalina Arias, legal counsel, RACSA S.A. was interviewed on 27 April 2012.

56 Law N° 8642, op.cit.

57 *Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones*. N° 35205-MINAET, 16 April 2009. http://historico.gaceta.go.cr/pub/2009/05/18/COMP_18_05_2009.html#_Toc230147025

58 Known as the P*rotección de la persona frente al tratamiento de sus datos personales,* Law N° 8968, 7 July 2011. http://historico.gaceta.go.cr/pub/2011/09/05/COMP_05_09_2011.html#_Toc302738759

59 GSMA represents the interests of mobile operators located in more than 220 countries. It brings together nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem.

Additionally, before activation, every mobile device should be delivered an official endorsement after verifying that the technical specifications described to the client actually matched the ones of the device purchased. This procedure would allow for the official registration of most mobile phones used in the country.

TECHNICAL AND PROCEDURAL MEASURES

Costa Rica is the first country in Latin America to have signed an agreement with GSMA in order to report the EMEI number of stolen mobile phones, regardless of the operator, to a central international blacklist.

Agreement with national operators regarding the data registry of users of pre-paid phones

In Costa Rica, 59 per cent of mobile phone users use pre-paid services[60]. SUTEL compels Costa Rican operators to keep an updated temporary record of clients who purchase pre-paid phones, although this obligation is not always respected. SUTEL has looked at samples and confirmed that, in some cases, clients give fake information. CLARO Costa Rica argues that these records are useless and are commercially counterproductive[61]. Instead, the company suggests that collecting records of real traffic (voice and data) would be more useful. Mobile phone companies do keep a record of all calls through a Call Detail Record[62] (CRD). Details such as origin of call, called party, call type and duration are documented. However, it is considered to be private data that can only be seized with a judicial order.

Law enforcement

The Computer Crimes Section of the Costa Rican Organization of Judicial Investigation (OIJ) was created in 1996-1997. It is one of the country's oldest specialized sections in the field. It currently has 14 full-time permanent civil servants and eight temporary staff (expected to become permanent in January 2013), which makes it the largest department of this kind in Central America. Microsoft Costa Rica has financially supported training activities for OIJ agents in the field of cybercrime, delivered through the Washington-based International Centre for Missing and Exploited Children (ICMEC)[63].

The OIJ is in charge of investigating generic computer crimes and crimes involving the use of electronic devices aided by computer forensics, when petitioned to do so. However, these investigations still face a number of obstacles despite growing awareness of security issues. For example, many companies do not keep track of log files and computer logging subsystems, or do not do it systematically. These files are key to proving crime, since they allow the retrieval of information such as IP addresses and date and time of access.

Moreover, procedural law mechanisms such as letters rogatory and judicial cooperation channels are complicated and slow, especially when data needs to be obtained from servers outside the country. In many pharming and phishing cases, the IPs identified are from other Latin American countries. The local offices of INTERPOL are sometimes used as alternative channels, however these issues still need to be addressed. On the contrary, cooperation with Spain in cases of online child pornography and fraud has, generally speaking, been quick and efficient.

---

60 National survey *Acceso, Uso y Calidad de los Servicios de Telecomunicaciones*, op.cit.

61 Victor García, Manager of Regulation and Interconnection, CLARO Costa Rica, interviewed on 2 May 2012.

62 Also known as Call Data Record.

63 Vilma Villalobos, Government Affairs Microsoft, information sent via email on 12 April 2012.

Private Sector

The Chamber of Information and Communication Technologies comprises almost 200 companies from the ICT sector. Telecommunications operators such as Amnet and Racsa S.A. are affiliated. They are committed to "a responsible use of the Internet" that, according to them, includes respect for intellectual property rights, a topic they have been actively promoting through several organized activities, one of which in cooperation with the World Intellectual Property Organization. In April 2012, CAMTIC organized two conferences on network security (malware and Internet, penetration tests and network vulnerability analysis). Nevertheless, according to its director, cybercrime-related issues are still relatively new in the country and most people are unaware of them [64].

CLARO Costa Rica is one of the new telecommunications operators in the market. As of 2 May 2012, it had approximately 300 000 clients in Costa Rica and a coverage of 60 per cent of the total population, but none in the GAM. As a telecommunications operator, the company is fully aware that they are bound to respect the legal obligations in force in the country. Nevertheless, when approached by judicial authorities especially for the purpose of intercepting and seizing voice and/or data traffic, they expressed confusion as to the extent of their legal obligations and the procedural steps to follow[65].

[64] Otto Rivera, Director, CAMTIC. Interviewed on 30 May 2012.

[65] Victor García, Manager of Regulation and Interconnection, Claro Costa Rica. Interviewed on 2 May 2012.

4. NATIONAL FRAMEWORK ON CHILD ONLINE PROTECTION

4.1 Legislation

In terms of international legal obligations, Costa Rica is party to the Convention on the Rights of the Child (1989), signed and ratified in 1990. It is also party to its Optional Protocol on the sale of children, child prostitution and child pornography (2002), which entered into force in April 2002.

The International Labour Organization Convention 182 on the Worst Forms of Child Labour, adopted in June 1999, was ratified by Costa Rica in 2001. It stipulated in article 3 that the worst forms of child labour include the use and offer of children for prostitution and the production of child pornography.

The Costa Rican criminal legislation presently mentions the offences of production of child pornography (article 173, introduced in 1999 and reformed in 2007) of possession of child pornography (article 173bis, created in 2007) and of distribution of such materials (article 174, introduced in 1999 and modified in 2001). The legislation covers offences committed through a computer system or not.

In December 2009, a new bill on computer crimes[66] was introduced in Parliament to regulate offences such as data interference, computer-related fraud, extortion, espionage, etc. The bill is specifically related to the protection of children and teenagers; cases where social networks or electronic means are used to look for underage victims constitute an aggravating circumstance and increase the penalties. This is also the case, for violation of computer-stored personal data and of identity theft. On 22 May 2012, Parliament adopted the bill during the first round of debate.

In July 2009, a law against organized crime was passed[67]. Article 14 of this law created a Judicial Centre for the Interception of Telecommunications (CJIC), meant to operate 24 hours a day, seven days a week. Judges can issue orders to intercept communications for specific serious crimes are under investigation, such as cases of sexual exploitation, production of adult and child pornography, bank subtractions using telematic means, trafficking of minors and of human organs, terrorism, drug trafficking, kidnapping, international crimes, money laundering, etc.

Laura Chinchilla Miranda, President of Costa Rica, Hamadoun I. Touré, Secretary-General of the International Telecommunication Union and a group of students from the Technical Secondary School (CTP) of Los Chiles who are the 2009 winners of a video contest about online safety. Mr Touré attended the ceremony of the signature of the decree creating the National Commission on Online Safety, held on 17 November 2010 at the Omar Dengo Foundation in Costa Rica. Picture courtesy of the Presidential House.

66 *Reforma de varios artículos y modificación de la sección VIII, denominada "Delitos informáticos y conexos", y al título VII del Código Penal*. Expediente N° 17.613, 23 April 2011.

67 Law N°8754 published in the Official Gazette Alcance 29, N°143, 24 July 2009. www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=65903&nValor3=87003&strTipM=TC

Article 17 states that any private or public company providing telecommunication services in the country will have to make necessary arrangements to contribute to the efficient running of the CJIC, according to the petition issued. These companies will have to provide conditions that allow the judicial order to be executed without delay or hindrance. In cases where operators do not cooperate as required, SUTEL has the power to sanction the company by withdrawing its concession or permit to carry out its telecommunications activities.

These cases constitute a legal exception to the provision of the LGT, according to which third parties should not listen, store, intercept, tape or monitor communications or voice and data traffic.

In 2011, two important actions were initiated by the national authorities. For instance, in July 2011, article 7 of the criminal code was reformed to stipulate[68] that all sexual exploitation offences perpetrated outside the national territory, whether online or not, against children and teenagers can be judged in Costa Rica if the suspect is apprehended on its territory. Both the nationality of the offender and the legislation in force in the country where the crime was committed (dual criminality) are irrelevant. Moreover, the prosecution can start an investigation even if a complaint has not been filed by the victim in Costa Rica (article 8).

In August 2011, a fairly comprehensive bill was introduced on the initiative of the non-governmental Paniamor Foundation for consideration by Parliament. The bill, called "Special law for the protection of the rights of children and adolescents in instances of violence and ICT-related crimes" includes a wide range of offences that do not exist in the criminal code, such as grooming, cyberharassment among children and teenagers, online identity theft, pseudo child pornography (morphed, digitally drawn child pornography, hentai), the production and dissemination through computer systems of materials depicting scenes of torture and death involving minors, as well as possession of such materials, and violation of the personal data of minors. In addition, the bill proposed to reform articles 173, 173bis and 174 mentioned above. The Parliament´s Commission of Youth, Childhood and Teenagers sought PANI's official views regarding the content of the bill. It is currently being analysed by PANI's legal department.

On 24 April 2012, the Council of Europe's Convention on Cybercrime (2000) (the Budapest Convention) was officially translated into Spanish for signature by the Costa Rican Minister of Foreign Affairs and the President of Costa Rica, then sent to Parliament for approval. Becoming party to the Convention on Cybercrime implies that adjustments will have to be made to national substantive and procedural criminal law. The Budapest Convention regulates international requests for mutual assistance — an area that concerns the Computer Crimes Section of the Organism of Judicial Investigation.

[68] Law N°8961. Published in the Official Gazette N°139, 19 July 2011. www.pgr.go.cr/Scij/scripts/TextoCompleto.dll?Texto&nNorma=70707&nVersion=0&nTamanoLetra=10&strWebNormativa=http://www.pgr.go.cr/scij/&strODBC=DSN=SCIJ_NRM;UID=sa;PWD=scij;DATABASE=SCIJ_NRM;&strServidor=\\pgr04&strUnidad=D:&strJavaScript=NO

4.2 Organisational structure

As a result of the implementation of the COP Global Initiative, the National Commission on Online safety was created by an executive decree published on 9 December 2010[69].

The role of the Commission is to devise policies on the safe use of the Internet and ICTs and to design and develop the National Plan of Online Safety. Specifically, the commission:

- Creates awareness-raising projects for children and teenagers and their families about the appropriate use of the Internet and digital technologies;
- Proposes actions to prevent access to inappropriate contents by minors;
- Promotes safe access to the Internet and digital technologies;
- Develops strategies to avoid the inappropriate use of the Internet or digital technologies in public and private institutions;
- Analyses or proposes legislation to strengthen the rights of individuals, communities and institutions regarding access to the Internet; and
- Proposes coordinating mechanisms with the public administration to prevent the inappropriate use of the Internet and digital technologies.

The National Commission is a multidisplinary and intersectorial structure, and comprises representatives of public and private institutions. If deemed necessary, it has the power to create sub-commission and working groups. Meetings are convened once a month by the Ministry of Science and Technology, which is in charge of the commission.

When the idea of the National Commission on Online Safety was first suggested, the then Minister of Science and Technology, Clotilde Fonseca, invited three institutions to discuss their interest in joining the soon-to-be created commission. These were the National Child Welfare Institute (known as PANI), the Paniamor Foundation and the Omar Dengo Foundation. Each institution nominated a representative and, under the leadership of the MCIT, shared ideas on how to work together, defined the modalities for the mission's guiding principles and discussed how issues of online protection were being tackled. In the meantime, the Executive Decree was published and the commission was officially constituted. At the beginning of 2011, the three original members became official members of the commission and started outlining a workplan. They agreed to invite institutions to join the commission once a clear set of goals had been established. These institutions included the Ministry of Public Education, the Ministry of Culture, Youth and Sports (MCJD), the Superintendency of Telecommunications (SUTEL), judicial authorities and the National Chamber of ICTs.

[69] Decree N° 36.274, published in the Official Gazette N°239, 9 December 2010. http://historico.gaceta.go.cr/pub/2010/12/09/ COMP_09_12_2010.html#_Toc279571975

4.3 Capacity building and awareness-raising strategies (civil society and public institutions)

The Patronato Nacional de la Infancia (PANI), created in 1930, was formally incorporated in the 1949 constitution. Originally, it was called National Welfare Institute attending to children at risk. However, in 1997 its mandate was redefined to protect the rights of all underage citizens by defining, regulating and monitoring relative policies. Since 2007, the institution has incorporated in its capacity building and awareness-raising activities the topic of online protection, focusing on children´s and teenagers´ rights[70].

In 2007, PANI opened a training academy at its San José cultural centre. Protecting the rights of children online has been among the key topics of the training modules since the beginning. These modules are delivered to employees of PANI as part of their professional development activities. The totality of the local staff in community-based offices has been trained on the responsible and safe use of the Internet.

The cultural centre also trains parents, whether referred to the centre by judicial instances or volunteers. Since 2010, five training activities organized in Aguirre, la Unión, Pococí and Pavas were attended by a total of 150 parents. The topic of child online protection was included in all the training delivered.

In 2010, with the support of the Ricky Martin Foundation and the Costa Rican non-governmental organization called *Allianza por Tus Derechos*, PANI launched a national television and radio campaign aimed at raising awareness about the use of children in pornography and the dangers of new technologies. It was replicated in 2011. Since 2011, four adverts on the safe and responsible use of the Internet have been running on national television and radio, as well as on some youth radio stations.

On 15 March 2012, PANI co-organized with the National Commission for the Improvement of the Justice Administration (CONAMAJ) and the legal services of the Commision a one-day activity on child online protection. According to the Director of CONAMAJ, most lawyers showed strong interest and felt they needed to be better equipped to deal with incoming reports related to the protection of children´s rights online. They thought it necessary to elaborate a protocol to clarify procedural and non-procedural steps to be taken in these cases. They also felt that the need for better articulation between the Ministry of Public Education and judicial instances[71].

Several initiatives on the topic of online protection were undertaken in 2012 in collaboration with local offices of other public institutions that will be developed in 60 of the 81 cantons of the countrys. Furthermore, PANI nationwide has received special funding to design, print and distribute materials about the safe and responsible use of the Internet.

PANI has activated phone lines and created two Facebook profiles — one for the general public and the other for minors — that have reached more than 15000 fans. They expect to receive reports from adults or minors regarding any situation affecting the rights of young people and to provide advice or counselling when sought. In addition, the Facebook profiles are used to publish positive messages about key issues and especially the safe and responsible use of the Internet.

The idea of opening an institutional Facebook profile came from the Presidency of PANI. It was orriganallys run by a regular staff member as an additional responsibility. However, the page grew so popular that, in order to properly attend to the growing number of requests for advice and the reports of abuse, the institution decided in mid-2011 to hire a full-time community manager.

CONAMAJ, created in 1985, is another public structure active in the field of child online protection. They are not experts on these issues but rather act as facilitators to raise consciousness. The commission works to strengthen the administration of justice and is committed to defending human rights and promoting social change within the justice sector.

In October 2010, CONAMAJ introduced the topic of responsible use of the Internet when it co-organized a seminar with the Argentinean Institute of Research for Justice, with support from the Canadian International Cooperation. The following year, they issued and distributed an institutional calendar on the safe use of the Internet in forums such as youth groups, religious groups and judicial staff, as promotional material to raise awareness on child online protection.

In early 2012 CONAMAJ, with the support of the Paniamor Foundation, organized a conference for family judges to discuss child online protection from a judicial point of view. However, due to poor attendance at the conference

[70] Ingrid Quesada, lawyer, cabinet of the President of the PANI. Interviewed on 3 April 2012.

[71] Sara Castillo, Director, CONAMAJ. Interviewed on 25 April 2012.

CONAMAJ decided to switch to an online training strategy, which has been more successful. The online module started on 1st May, and lasted one month. It included two stages: the first two weeks were designed to raise awareness through readings, videos, and synchronous online conversations. The other two weeks were dedicated to encourage participants to think about practical steps that would be helpful when dealing with actual cases[72].

The Paniamor Foundation[73] is a leading and well-known non-governmental organization that promotes children´s rights. Between 2009 and 2010 it focused mainly on conducting research on the protection of children and teenagers in cyberspace. In 2009, with the support of Save the Children Sweden, Paniamor conducted their first research activity, but findings were inadequate and thus more research was needed. Their final report was cutting edge in terms of existing national and international literature. A national study followed that revealed three key aspects:

- a lack of parental guidance;
- existing legal loopholes;
- a lack of social control when abuses were committed.

In 2010, Paniamor organized a successful campaign called *Suave un toque.com*[74], encouraging teenagers to work with them on Internet safety (please refer to section 5.1). Besides; in 2009-11 Paniamor organized two editions of a regional video contest called *Tecnología Sí.*[75] Teenagers interested in participating were asked to produce and submit a three-minute video on issues related to the safe use of the Internet. The winners of the 2009 edition were students from a technical secondary school (CTP) in Los Chiles.

In 2011, Paniamor focused on strengthening inter-institutional initiatives, becoming an active and committed member of the National Commission on Online Safety and preparing a legal bill that was submitted to Parliament in August 2011. The main objective of the bill, as detailed in the previous section, was to eliminate legal loopholes. Paniamor also became the coordinating entity of a Latin American network of NGOs (called redNATIC) committed to the promotion of the rights of young people and to safety in ICTs.

As part of its educational strategies, Paniamor developed a series of three guides for secondary school teachers and students on Internet safety. These guides have been officially delivered to the Ministry of Public Education and the Omar Dengo Foundation to be used in classrooms

The Omar Dengo Foundation (ODF) established a partnership with the Ministry of Public Education (MEP) in 1987 to create the National Programme of Educational Informatics (NPEI MEP-ODF). Since 2010, the foundation has systematically and gradually introduced the issue of safe and responsible use of the Internet in the strategies developed with its students, teachers and educational advisors.

In November 2010, several training sessions were organized for the Foundation´s educational advisors to raise their awareness about child online protection. They in turn trained more than 1000 IT teachers (primary and secondary) in the weeks that followed, in schools nationwide.

Next is a summary of the different actions that were implemented in 2011 by the Omar Dengo Foundation[76].

---

72 Sara Castillo, op.cit.

73 Walter Esquivel, Section of Technological Initiatives, Paniamor Foundation. Interviewed on 16 April 2012.

74 For additional information please visit http://paniamor.org/prevencion/suaveuntoque.html

75 Literally translated, “Technology yes”.

76 Information extracted and translated from the files of the National Commission on Online Safety located in the MICIT.

Box 11- Child Online Protection — 2011 PRONIE MEP-FOD workplan

Video contest: *Alerta2*

Production of a video on the safe and responsible use of the Internet by high school students of NPEI. The winner of the contest, Tamara Sánchez of the Alejandro Quesada Ramírez Secondary School, was invited by ITU to participate in the 2011 IGF.

Summer school camps nationwide*

Twenty camps in primary and secondary schools on the safe and responsible use of the Internet.

Each camp was a week-long, 40-hour course

Number of participants: 374 students.

Survey/Mapping of online uses and risks

A survey was designed and applied to 374 students from 25 schools. The data is currently being processed.

Pedagogical contents to be delivered (teacher training and written materials)

Conference on online protection inserted on the agendas of national pre-programmed events:

– Two seminars with special education teachers (total of 500 participants

– Gathering of headmasters

– Seminar for teachers of one-classroom schools. The ITU guide for parents and teachers was used during these activities.

Labour@ camps: one conference about online risks was delivered to 189 students and 14 mediators.

1:1 Project – rural secondary schools REM@

A conference on online child protection aimed at all teachers and parents of the 11 secondary schools of the programme (865 students and 70 teachers participated)

Second phase of training: 99 students and six teachers attended

Special activities on online protection during the 2011 December festival

Awareness-raising materials

1500 copies of the 2011 institutional calendar designed, published and distributed, with tips for teachers.

A game with flash code related to the safe and responsible use of the Internet was designed and used with students during a Tech Fair 360@ organized by the Ministry of Public Education on 16 and 17 May 2011.

Technological solutions

Improved version of the current filter installed in all computer labs.

* Summer camps are delivered in around 180 schools nationwide during summer holidays, mid-July each year.

To conclude, between 2010 and 2012 thousands of students, teachers and parents benefited one way or another from activities related to child online protection organized by the Omar Dengo Foundation. From 16 to 21 April 2012, (attended by a camp with training activities about cyberbullying, sexting and online risks was attended by 334 students from one-teacher schools. Moreover, 52 of their parents participated in training activities about online risks. Finally, 1247 young people and adults involved in a project of the foundation called "*Adultos al día con la tecnología*[77]" also received training on online risks[78].

4.4 International cooperation

With the support of ITU, during IGF 2010 a delegation from Costa Rica established initial contacts with the International Association of Internet Hotlines (INHOPE). The possibilities of joining the association and installing an INHOPE platform in the country were explored. Subsequently, in 2011 the topic was discussed on several occasions in sessions of the Commission on Online Safety.

Similarly, contacts with representatives of the International Centre for Missing and Exploited Children were made to explore the possibilities of implementing the Financial Coalition Against Online Child Pornography (FCACP) in Costa Rica. Members of the National Commission on Online Safety showed strong interest in going ahead with this project.

ITU financially supported the participation of a two-member Costa Rican delegation (one representing the NGO sector and the other, the governement) to the 2010 IGF in Lithuania. Additionally, in 2011 ITU awarded a fellowship to a Costa Rican student (and two accompanying adults), who won the Omar Dengo Foundation video contest and was invited to participate in a COP session at the 2011 IGF in Kenya.

4.5 Recent development under the ITU Child Online Protection Global Initiative

In 2011 and 2012 there was no significant development of the ITU Child Online Protection Global Initiative, due mainly to two circumstances. On the one hand, in the second half of 2011 there was a period of staff rotation within the Ministry of Science and Technology. On the other hand, a decision was taken to focus on the establishment of the CSIRT-CR, formally created early in 2012, and then to reactivate the National Commission on Online Safety as a specialized commission of the CSIRT. Even though the National Commission on Online Safety has been temporarily inactive, its founding members, namely the PANI, the Paniamor Foundation and the Omar Dengo Foundation continue to actively promote online protection.

At the end of May 2012[79], the Ministry of Science and Technology invited the founding members of the National Commission to reconvene. Two sessions were held that focused on re-examining the draft 2011 workplan and to exchange updated information about the work done by each institution in the intervening period. Finally, the decision was taken to invite the institutions mentioned in the constitutive decree to join the Commission[80].

---

77 Literally "Adults staying up-to-date with technology".

78 Written information provided by the Omar Dengo Foundation, 10 May 2012.

79 Information provided by Micaela Mazzei, Ministry of Science and Technology, Costa Rica.

80 Please see p.54 for a complete list.

5. BEST PRACTICES

5.1 Creating a culture of child online protection

Filing complaints

Since 2010, as part of its mandate, PANI has filed 24 reports to the Attorney´s office; 14 of them related to misuse of Facebook profiles. Two of these cases, in particular, were filed because they showed secondary school students (male and female) in sexually suggestive pictures. The profiles were taken down after being reported to the judicial authorities.

Picture courtesy of the Omar Dengo Foundation.

Awareness-raising activities for the general public

In collaboration with an advertising company called Garnier, PANI invited the general public through its Facebook page to send in a picture with their contact information if they wanted to be famous for one day. It was a fake competition organized to ascertain the readiness of minors to disclose their photo and personal data. Approximately 1000 people, both adults and minors, submitted the information. At the celebration of Safer Internet Day (SID), 9 February 2010, PANI organized a street exhibition and displayed blurred images of the pictures received with messages warning citizens about the dangers of disclosing personal information online.

Empowering

The Paniamor Foundation designed and implemented a successful initiative called *Suave un toque.com*[81] that targeted teenagers and worked with focus groups on aspects related to graphics, language used and issues tackled. The campaign used two platforms: a blog where staff from Paniamor posted a story once a week and a Facebook profile for five fictional characters. The content of the stories and comments posted were related to problems and risks teenagers face caused by their use, misuse and misperception of ICTs. Issues such as grooming, cyberbullying, identity theft and the excessive use of the Internet were tackled.

5.2 Transparency

Public access to key information

Promoting transparency implies, among other things, public access to key information; this encourages an environment of increased accountability for all actors involved and the decisions taken. In view of its responsibilities vis-à-vis its stakeholders, the superintendency of telecommunications SUTEL uploads to its website all the information that is allowed to be published.

[81] For additional information, please visit http://paniamor.org/prevencion/suaveuntoque.html

5.3 Cooperation

Celebrating the 2011 Internet Safer Day (SID) together

For the first time, the members of the National Commission on Child Protection — PANI, Paniamor, MICIT and ODF — co-organized the Internet Safer Day on 9 February 2011, in a community centre of Pavas, San José (Costa Rica).

Parents and children learning together

The One Laptop per Child programme of the Quirós Tanzi Foundation allows students to take their computers home. One student from a rural school, who received an XO laptop in early 2012, whose father works as a supervisor of private guards and had never used a computer before, taught his father how to use the laptop and he is now able to use a word processor to produce documents for his job.

A public entity allied with a financial institution

NIC-Costa Rica validated the signature of the security protocol DNSSEC with the National Bank (BN). It is the only country in Latin America that has tested the DNSSEC with a client.

5.4 Continuity, stability and flexibility

Investigate and analyse the problems to be addressed, identify loopholes, design proper educational and awareness-raising strategies and adapt to problems encountered.

This has been the approach adopted by the Paniamor Foundation since it started working on Child Online Protection in 2009.

Learning from experience

After an excellent start late 2010/early 2011, the work done by the National Commission on Online Safety has been temporarily suspended, to be resumed at the end of May 2012, as described above in section 5.

6. RECOMMENDATIONS

Based on the information gathered and displayed in this case study, the main recommendations are:

Picture courtesy of the Omar Dengo Foundation.

National Commission on Online Safety:

- To perform sustainable work in the long term, now that the Commission has been reactivated;
- To strengthen the National Commission on Online Safety as a common space where the numerous ongoing actions conducted in the field of child protection can be articulated;
- To strengthen the National Commission on Online Safety as the unique voice of a group of stakeholders interested in coordinating a national strategy on child online protection;
- To make sure the other key representatives, who are not the founding members, are involved closely;
- To invite other institutions to be observers;
- To reactivate the initial contacts made by the Commission with potential national and international partners and to re-examine the possibility of reaching key agreements in the field of child online protection.

Fostering a culture of online child protection/ cybersecurity:

- To take practical steps in order to ensure the durability of the newly created CSIRT-CR;
- To oblige all Internet cafés to register with SUTEL;
- To initiate the operations of the Judicial Centre for the Interception of Telecommunications (CJIC), created in 2009;
- To raise awareness among network administrators about security issues and specifically about existing protocols and tools that register network traffic;
- To target key policy-makers and persuade them of the importance of security issues;
- To introduce, in a systematic and sustained manner, the responsible and productive use of the Internet into the official curriculum of the Ministry of Public Education;
- To develop specific educational strategies with primary school students who have not yet been targeted by education and awareness-raising strategies;
- To pursue awareness-raising activities with secondary-school students;
- To proceed with the design and development of specific training strategies for educators;

- To focus educational and awareness-raising strategies on parents who have difficulty dealing with important issues due to a digital or generation divide.
- To establish an Internet hotline dedicated to receiving reports on crimes against children online, inspired by the Inhope model, which is economically sustainable;
- To ensure that the topic of responsible and safe use of the Internet is comprised in the training received by the users of community telecentres;
- To train the professionals in charge of the telecentres on existing online risks to children and a safe and responsible use of the Internet.

Private sector

- To involve relevant stakeholders, mobile operators, Internet service provider companies and broadcasters in the development of a code of conduct and tools to enhance child online protection;
- To encourage the financial sector to commit to implementing the Financial Coalition Against Child Pornography, promoted by the International Centre for Missing and Exploited Children (FCACP).

Legal and judicial issues

- To adjust national legislation, once accession to the Council of Europe Convention on Cybercrime has been achieved;
- To adopt the bill, proposed by the Paniamor Foundation, introducing a series of ICT-related offences against children and teenagers;
- To adopt more efficient mechanisms of international cooperation to shorten response delay in cases where the required data is stored in devices located outside the national territory;
- To issue as soon as possible SUTEL´s ruling on the legal obligations and procedures steps for telecommunication operators in cases where judicial authorities require their collaboration, with or without a judicial order.

Public policy issues

- To achieve a proper transfer of the Vice-ministry of Telecommunications, until recently attached to the Ministry of Environment, Energy and Telecommunications, to the Ministry of Science and Technology.

7. CONCLUSION

Costa Rica has taken a strong stand in favour of beginning the irreversible process towards an information society. However, the topic of child online protection in the country only emerged in 2009-2010, as a consequence of concerns raised by several public and private organizations. Among the general public and in key sectors, many adults are still unaware of the importance of child online protection. They are 'digital migrants' dealing with an unknown world, which they are bound to see as a danger instead of an opportunity. Meanwhile children and students, as 'digital natives', long to be almost constantly connected. This is why the National Commission on Online Safety needs to send a clear message that, in order to create a culture of child online protection, we need to empower and build key skills in children and teenagers. In this context, one of the concerns of the National Commission on Online Safety should be to persuade all concerned actors — parents, teachers, telecommunications operators, judicial authorities, etc. — that it is in everybody's interest to cooperate and contribute different perspectives to the creation of a national culture of child online protection. Once this process is set in motion, the country should be able to adopt a comprehensive set of political, educational, technical, judicial and legal strategies that, together, will enhance the protection of Costa Rican children and teenagers online.

Picture courtesy of the Omar Dengo Foundation.

Annex A — Abbreviations and acronyms

ICANN	Internet Corporation for Assigned Names and Numbers
CAMTIC	*Cámara de Tecnologías de Información y Comunicación* / Chamber of Information and Communication Technologies
CCTLD	Country Code Top-Level Domain
CECI	*Centros Comunitarios Inteligentes* / Telecentres
CICTE-OAS	*Comité Interamericano contra el Terrorismo* / Inter-American Committee Against Terrorism
CSIRT-CR	*Centro de Respuesta de Incidentes de Seguridad Informática Costa Rica* / Computer Security Incident Response Team Costa Rica
CONAMAJ	*Comisión Nacional para el Mejoramiento de la Administración de Justicia* / National Commission for the Improvement of Justice Administration
CoE	Council of Europe
DNS	Domain Name System
DNSSEC	DNS Security Extensions
FONATEL	*Fondo Nacional de Telecomunicaciones* / National Development Fund for Telecommunications
FOD	F*undación Omar Dengo* / Omar Dengo Foundation
GDP	Gross Domestic Product
GSMA	Groupe Spéciale Mobile Association
HDI	*Indice de Desarrollo Humano* / Human Development Index
ICE	*Instituto Costarricense de Electricidad* / Costa Rican Institute of Electricity
ICTs	Information and Communication Technologies
INEC	*Instituto Costarricense de Estadística y Censos* / National Institute of Statistics and Census of Costa Rica
INHOPE	International Association of Internet Hotlines
ISP	Internet Service Provider
ITU	International Telecommunication Union
LGT	*Ley General de Telecommunications* /Telecommunications Act
MEP	*Ministerio de Educación* / Ministry of Education
MICIT	*Ministerio de Ciencia y Tecnología* / Ministry of Science and Technology

MIDEPLAN	*Ministerio de Planificación* / Ministry of Planning
MINAET	*Ministerio del Ambiente, Energía y Telecomunicaciones* / Ministry of Environment, Energy and Telecommunications
PRONIE MEP-FOD NPEI MEP-ODF	*Programmea Nacional de Informática Educativa MEP-FOD* / National Programme of Educational Informatics MEP-FOD
OAS	*Organización de los Estados Americanos* / Organization of American States
ODF	*Fundación Omar Dengo* / Omar Dengo Foundation
OIJ	*Organismo de Investigación Judicia*l / Judicial Investigation Organization
PANI	*Patronato Nacional de la Infancia*
RACSA	*Radiográfica Costarricense, S.A*.
REMJA	*Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas* / Meetings of Ministers of Justice or Other Ministers or Attorney Generals of the Americas
SUTEL	*Superintendencia de Telecomunicaciones* / Superintendency for Telecommunications
UTN	*Universidad Técnica Nacional* / National Technical University

Annex B — Organizations interviewed[82]

Ministry of Science and Technology

- Mr Santiago Núñez, Director of Digital Technologies
- Mr Oscar Quesada, Coordinator of Telecentres

National Welfare for Children Institution (Patronato Nacional de la Infancia)

- Ms Ingrid Quesada, Lawyer, Cabinet of the President of the PANI

Non-governmental organizations

Paniamor Foundation

- Mr Walter Esquivel,

Quirós Tanzi Foundation

- Ms Carolyn Gourzong, Pedagogical Adviser
- Mr Juan Cubillo, Technical Coordinator
- Ms Sara de la Parra, Pedagogical Adviser

Telecommunications operators

RACSA

- Ms Ana Catalina Arias Gómez, Legal Division
- Ms Maricruz Delgado, Operational Division
- Mr Richard Elizondo, Operational Division

CLARO

- Mr Victor García, Manager of Regulation and Interconnection

Superintendency of Telecommunications (SUTEL)

- Ms Maryleana Méndez, member of the Council of Directors

National Academy of Science — DNS

NIC — COSTA RICA

- Mr Luis Diego Espinoza, Director of Information Technologies
- Ms Jéssica Calvo, Manager

Judicial System

National Commission for the Improvement of the Justice Administration (CONAMAJ)

- Ms Sara Castillo, Director

Computer Crimes Section of the Organism of Judicial Investigation

- Mr Erick Lewis, Chief, Computer Crimes Section

Private sector

National Chamber of ICTs (CAMTIC)

- Mr Otto Rivera, Executive Director

Microsoft

- Ms Vilma Villalobos, Government Affairs, Latin America New Markets and Puerto Rico, Microsoft

[82] This list reflects the positions held by these persons at the time of the field research.

BIBLIOGRAPHY

ARESEP. Decree-law creating ICE N° 449. www.aresep.go.cr/docs/Ley%20449_CREACION%20DEL%20ICE.pdf

El Financiero, Unimer (2011). Survey: *El uso de Internet y de las redes sociales*, 18-30 March 2011. www.elfinancierocr.com/ef_archivo/2011/julio/31/enportada2850796.html

Livingstone, S., Haddon, L., Gorzig, A. & Olafsson, K. (2011). Final Report: EU Kids Online II. The London School of Economics and Political Science. London. www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf

Ministry of Environment, Energy and Telecommunications (MINAET). Demoscopía S.A. (2011). National survey: *Acceso, Uso y Calidad de los Servicios de Telecomunicaciones*, October-November 2011. www.telecom.go.cr/index.php/publicaciones2/publicaciones

The National Institute for Statistics and Census (2010). National Households Survey (ENAHO), San José, Costa Rica. www.inec.go.cr/Web/Home/GeneradorPagina.aspx

Official Gazette (2009). Law N°8754, published in the Official Gazette N°143, 24 July 2009. www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=65903&nValor3=87003&strTipM=TC

Official Gazette (2011). Law N°8961, published in the Official Gazette N°139, 19 July 2011. www.pgr.go.cr/Scij/scripts/TextoCompleto.dll?Texto&nNorma=70707&nVersion=0&nTamanoLetra=10&strWebNormativa=http://www.pgr.go.cr/scij/&strODBC=DSN=SCIJ_NRM;UID=sa;PWD=scij;DATABASE=SCIJ_NRM;&strServidor=\\pgr04&strUnidad=D:&strJavaScript=NO

Official Gazette (2010). Decree N° 36.274, published in the Official Gazette N°239, 9 December 2010. http://historico.gaceta.go.cr/pub/2010/12/09/COMP_09_12_2010.html#_Toc279571975

Official Gazette (2009). *Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones.* Nº 35205-MINAET, 16 April 2009. http://historico.gaceta.go.cr/pub/2009/05/18/COMP_18_05_2009.html#_Toc230147025

Official Gazette (2011). *Protección de la persona frente al tratamiento de sus datos personales*, Law N°8968, 7 July 2011. http://historico.gaceta.go.cr/pub/2011/09/05/COMP_05_09_2011.html#_Toc302738759

Official Gazette (2011). *Reglamento sobre la Limitación a la Responsabilidad de los Proveedores de Servicios por Infracciones a Derechos de Autor y Conexos con el Artículo 15.11.27 del Tratado de Libre Comercio República Dominicana-Centroamérica-Estados Unidos*. N° 36880-COMEX-JP, published in the Official Gazette N°242, 16 December 2011. http://historico.gaceta.go.cr/pub/2011/12/16/COMP_16_12_2011.pdf

Official Gazette (2008). *Ley General de Telecomunicacione,* Law N° 8642, published in the Official Gazette N° 125, 30 June 2008. http://historico.gaceta.go.cr/pub/2008/06/30/COMP_30_06_2008.pdf

Official Gazette (2008). Law N° 8660, *Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones (LMFT),* published in the Official Gazette N° 156, 13 August 2008. http://historico.gaceta.go.cr/pub/2008/08/13/COMP_13_08_2008.html#_Toc206304472

Official Gazette (2007). Executive Decree N°33629, 20 February 2007. http://historico.gaceta.go.cr/pub/2007/03/21/COMP_21_03_2007.html

Paniamor Foundation (2010). Survey: *Conocimientos, Actitudes y Prácticas Asociados al Uso de Internet en Adolescentes*, May 2010.
http://paniamor.org/interactivo/centrodoc/uit.html

Programa Estado de la Nación (2011). XII Report: *Estado de la Nación*, San José, Costa Rica.
www.estadonacion.or.cr/images/stories/informes/017/cap_1_sinopsis.pdf

Programa Estado de la Nación (2011). Report: *El Estado de la Education*, San José, Costa Rica.
www.estadonacion.or.cr/index.php/biblioteca-virtual/costa-rica/english

United Nations Human Development Programme (2011). Human Development Report 2011.
http://hdr.undp.org/en/reports/

Villalobos, V. and Monge-González R. (2011). Costa Rica´s Effort Toward an Innovation-Driven Economy: The Role of the ICT Sector, the World Economic Forum Global Technology Report 2010-2011, 119-126.

INTERNATIONAL TELECOMMUNICATION UNION
PLACE DES NATIONS
CH-1211 GENEVA 20
SWITZERLAND

PRINTED IN SWITZERLAND
GENEVA, 2013

www.itu.int/cop