micitt MINISTERIO
DE CIENCIA, TECNOLOGÍA
Y TELECOMUNICACIONES

COSTA RICA
GOBIERNO DE LA REPÚBLICA

National Cybersecurity Strategy - Costa Rica

Ministry of Science, Technology and Telecommunications, 2017

350
E82e

Costa Rica. Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT).

Estrategia Nacional de Ciberseguridad Costa Rica 2017. – San José, C. R.: MICITT, 2017.

ISBN: 978-9968-732-52-9

1. CIBERSEGURIDAD-POLÍTICA GUBERNAMENTAL-COSTA RICA 2. SEGURIDAD EN COMPUTADORAS 3. REDES DE COMPUTADORAS-MEDIDAS DE SEGURIDAD 4.TECNOLOGÍA DE INFORMACIÓN-MEDIDAS DE SEGURIDAD

Table of Contents

Index of Figures

List of Charts

Index of Tables

Abbreviations and Acronyms in spanish

AMERIPOL	*Police Community of the Americas*
BCCR	*Central Bank of Costa Rica*
BI	*Business Intelligence*
BID	*Inter-American Development Bank*
CENFOTEC	*Training Center for Information and Communication Technologies*
CGR	*Office of the Comptroller General of the Republic*
CII	*Critical Information Infrastructures*
COBIT	*Control Objectives for Information Technologies and Related*
CONARE	*National Council of University Rectors*
CONESUP	*National Council for Private Higher Education*
CONICIT	*National Council of Science and Technology*
CRIX	*Internet Exchange Point de Costa Rica*
DB	*Database*
DBA	*Database Administrator*
DCFD	*Digital Signature Certifiers Office*
DDoS	*Distributed Denial of Service*
FEM	*World Economic Forum*
FISMA	*Federal Information Security Management Act*
FONABE	*National Scholarships Fund*
ICE	*Costa Rican Institute of Electricity*
ICTA	*Information and Communication Technologies Authority*
IEC	*International Electrotechnical Commission*
IED	*Inversión Extranjera Directa*
IMEI	*International Mobile Equipment Identity*
INTERPOL	*International Police*

ISO	*International Organization for Standardization*
ITCR	*Costa Rica Institute of Technology*
ITU	*International Telecommunications Unit*
IXP	*Internet Exchange Point (Internet Exchange Point)*
MEIC	*Ministry of Economy, Industry and Commerce*
MEP	*Ministry of Public Education*
MICITT	*Ministry of Science, Technology and Telecommunications MRREE*
NIST	*National Institute of Standards and Technology*
NRI	*Networked Readiness Index*
OCDE	*Organization for Economic Cooperation and Development*
OEA	*Organization of American States*
OECD	*Organization for Economic Co-operation and Development*
ONU	*United Nations Organization*
OPES	*Higher Education Planning Office*
PGR	*Federal Attorney-General's Office*
RPKI	*Public Resources Key Infrastructure*
SCADA	*Supervisory Control and Data Acquisition Systems*
SCI	*Industrial Control Systems*
SCIJ	*Costa Rican Legal Information System*
SEI	*Software Engineering Institute*
SINAES	*National Accreditation System of Higher Education*
SUTEL	*Superintendency of Telecommunications*
ICT	*Information & Communication Technologies*
TSE	*Supreme Court of Elections*
ITU	*International Telecommunications Union*
UNESCO	*United Nations Education, Science and Culture Organization*
XML	*Extensible Markup Language*

Executive Summary

The concept of Cybersecurity has evolved since the dawn of the first computers until today; the greatest challenge is securing the data, systems and processes safeguarded in them and shared through data networks such as the Internet.

Already in 1961 appear the first articles on the creation of a global data network, and for 1980 the Internet network presentation is performed, based on two IP protocols (Internet Protocol) and TCP (Transmission Control Protocol). This being the beginning of the network as such, later the WWW (World Wide Web - 1991) services were added.

Every technological advance implies a security challenge, from avoiding data theft from computers, action applied directly to them, or else with the global data networks, avoid non-authorized accesses and malicious with the purpose of extracting data and using them for unethical ends.

The world does not stop; innovation and constant discovery are essential to the technological industry's survival and for the growth of people.

Governments are affected by different kinds of attacks and intentions; from the simple game of a youth experimenting and challenging the system, to the clear intention of harming a country's systems and infrastructure.

Today we are a village; as such we face powerful challenges; from the perspective of securing the world's people data to the protection of the values enshrined in the universal declaration of human rights.

Human beings' intelligence is always proactive, searches new solutions, seeks new paths; this is not unfamiliar to hackers, who from their perspective it's a challenge to undermine different bodies in order to obtain a personal achievement, an economic gratification or else contribute with governments and enterprises in the espionage of facilities and infrastructures.

But these attacks must be repelled, with intelligence and coordinated actions so that society, as we are structuring it today, is not prey of a few, who for fun or consciously are determined to infringe it.

It is for this reason that this strategy and initiatives of having a safer world shall have great benefits in the future, since our people shall grow in confidence and acceptance of the diverse ways of thinking and action, important to attain a concert of nations.

In our country, coordinating among the different sectors, searching for solutions to new issues required the cooperation of all. This document is only a first step in that search for knowledge; it's a strategy which as such sets the guideline to follow hereafter in matters of cybersecurity in our country, mainly glimpsing the challenges we must conquer.

Chapter 1- Introduction

At world level it is acknowledged that digital technologies and the information and communication technologies (ICT) in particular are catalyzers of economic, social and cultural development, since they facilitate access to immeasurable resources; and besides communication, they promote innovation, efficiency, transparency and economic prosperity of countries.

Aware of that Costa Rica has opted for a strong promotion of the use of ICT, to enhance national development, strengthening the valid regulatory framework, to promote the development and use of telecommunications/ICT services within the framework of the information and knowledge society and to support sectors such as health, citizen security, education, culture, commerce and electronic government.

Similarly, public policy has been aimed at fostering the incorporation of digital technologies, in public as private services alike, improving the efficiency of those rendering these services and searching to lower costs for those receiving them. Additionally, it enhances investment in the telecommunications sector, with a legal framework establishing in their principles the guarantee of transparency, non-discrimination, equity, legal security, technological neutrality, and training of human resources in the area of ICT.

The results of these actions are reflected in the improvement of the national indicators for access and use of technologies. Moreover, in the international map, Costa Rica continues to grow in the international classifications based on its development. According to the World Economic Forum (WEF) on its 2014-2015 report, the country shows a very steady profile based on its tradition assets despite suffering from some persistent weaknesses. It has been reported that the country is well-positioned to participate in a quick transition to knowledge-based activities. The country has one of the best educational systems of Latin America and the Caribbean (the 21st position). The report also notes Costa Rica has a high assimilation of ICT (45th position) with a high capacity of International Internet bandwidth (36th position); many mobile broadband subscriptions (20th position); and developed innovative capacity (36th position) and solid access to technology (39th position), owing to the relevant role of foreign direct investment (FDI) and technology transfer (5th position) in the country.[1]

However, with the high rates of Internet connectivity and access to ICT, as well as the generation and massive storage of sensitive data, arise risks and vulnerabilities exposing people, the corporate sector and the government too. Users who access the net with illicit purposes have taken advantage of this reality. Proof of this the increasingly sophisticated means to hide their

Identity and conceal their cybernetic attacks, which hampers recognition, as well as the timely collection of probative elements of the crime, which limits due process by the corresponding authorities.

The advantages offered by digital technologies, for example cloud services, are also exposed to attackers, since public clouds are not only more vulnerable targets, but are also virtually unlimited and anonymous network resources for attackers.

Therefore, there is an evident need to develop and implement specific solutions to the risks and special vulnerabilities of the ICT, which evolve on a daily basis. Facing this reality and to be able to respond in a prompt and diligent way, the collaboration and cooperation of different national and international player is required.

A decisive step towards the exploitation of digital technologies would be defining a strategy, including actions pertaining to security from a holistic perspective, which takes into account all the elements, including identification of risks and threats that could result and their possible prevention mechanisms, the adequate attention of incidents and implementation of corresponding corrective processes.

The attention of incidents and cyber-attacks requires flexibility and speed in the development of an articulate national response, considering the existing frameworks and processes. For this reason, a series of elements have been considered, integrated in a strategy, seeking to increase cybernetic resilience, the development of the required human and technological resources, the strengthening of specialized response teams, national and international cooperation to enable exchange of information and the investigation of the informatics crimes.

[1] *Reporte Global de Competitividad 2014-2015. Foro Económico Mundial. Available at: http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2014-15.pdf*

as well as the protection of freedom of expression and Internet privacy as the central principle of cybernetic security.

The National Cybersecurity Strategy proposes a joint and articulated effort among all the country's sectors, to be able to guarantee that the established objectives are balanced, effective and in agreement to the national reality, defining the general principles which will set the standards in this matter.

Chapter 2 – Construction of the strategy

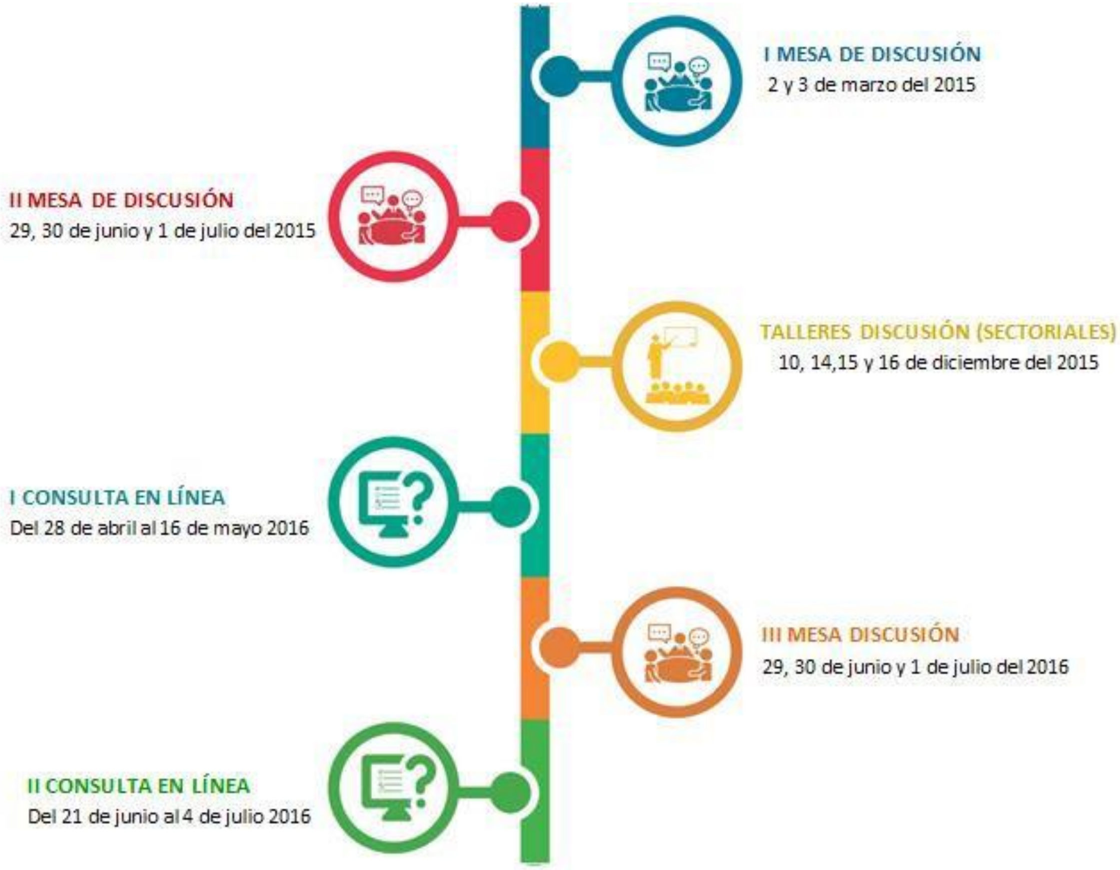
Cybernetic security requires a holistic vision and multi-sectorial attention; so, in the process of construction of this strategy, the Ministry of Science, Technology and Telecommunications (MICITT) had the specialized technical support of the Organization of American States (OAS) and enabled participation of the stakeholders to contribute in the development of this topic in the country.

The construction process was headed by MICITT; starting on the month of March of 2015 carried out three panel discussions, guided by OAS' specialized staff, four sectorial workshops and two online consultations.

On these encounters a participatory, open methodology was used with representatives of all sectors; presentations were made of OAS design structure, as well as proposals for approaching MICITT's vision; then, participants shared their vision and points of view about the principles, objectives and priority lines of action to be included in the strategy according to Costa Rica's reality.

Based on these discussions the participants' recommendations were extracted and a final draft elaborated, document exposed in the discussion panel, at the disposal of all everyone invited to the different workshops for 14 days, starting on June 21st of 2016 until July 04 of 2016 for reviewing and receiving comments and suggestions.

Figure 1 Multisectoral consultation process for the construction of the strategy


I MESA DE DISCUSIÓN
2 y 3 de marzo del 2015
II MESA DE DISCUSIÓN
29, 30 de junio y 1 de julio del 2015
TALLERES DISCUSIÓN (SECTORIALES)
10, 14,15 y 16 de diciembre del 2015
I CONSULTA EN LÍNEA
Del 28 de abril al 16 de mayo 2016
III MESA DISCUSIÓN
29, 30 de junio y 1 de julio del 2016
II CONSULTA EN LÍNEA
Del 21 de junio al 4 de julio 2016

Source: Own elaboration, 2016

After this stage, the corresponding observations of form and content were incorporated with the purpose of achieving a solid and consensual document; it was submitted to review by OAS' specialists.

Finally, on June 05 of 2017, it was submitted to non-binding Public Consultation through the Official Diary La Gaceta N. 105 process from which this document was obtained.

For the committed hard work done, we thank each one of the persons depositing their vast knowledge to the service of an instrument which shall be the roadmap in Cybersecurity matters for the coming years.

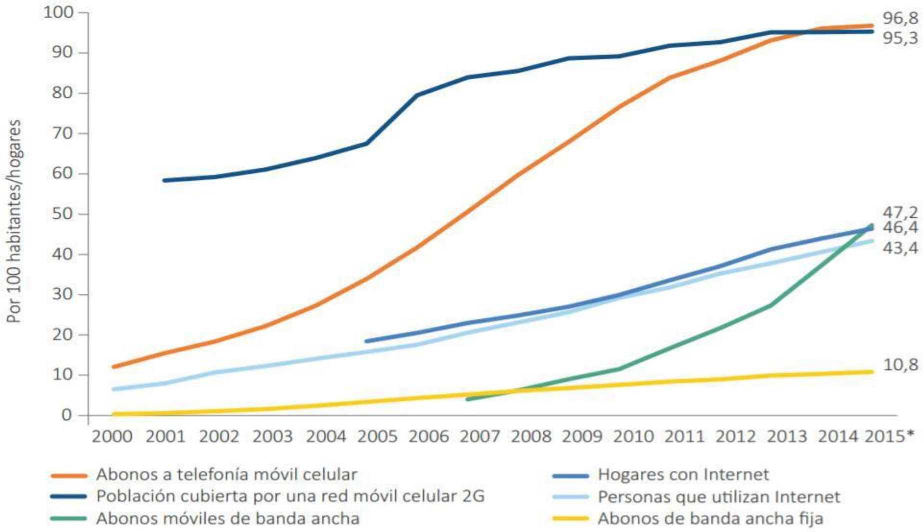
Chapter 3 – Current context

3.1.1 The impact of ICT on economic development

The use of the Internet has revolutionized people's way of interacting and of these with the outside world. Connectivity is a priority for countries today since it gives access to a platform allowing the collaboration, innovation and promoting different interaction mechanisms in the economic, political and social fields.

According to data from the International Telecommunications Union, "Measuring the Information Society, 2015" (ITU) the proportion of the world's population covered by mobile and cellular networks is now over 95 %, while the number of mobile cellular subscriptions has increased from 2 .200 million in 2005 to 7.100 million in
2015".[2]

*Chart 1 Changes of the main ICT at world level, 2000-2015**



**Estimates.*

Source: ITU. Taken from: Measuring the Information Society, 2015

[2] *Report on the Measurement of the Information Society 2015. International Telecommunication Union. (Available at: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2015-SUM-PDF-S.pdf. Page 1.*

The growing use of telecommunications and ICT has been parallel to a considerable increase of users exposed to criminal activities and risks related to data security, as well as equipment's intrusion and interruption.

According to the Cybersecurity Report 2016 issued by OAS and the Inter-American Development Bank, "… cybercrime has a world cost of up to US$575,000 million per year; this represents 0.5% of global GDP"[3]. Meanwhile, the same report indicates that for Latin America and the Caribbean, this type of crimes has an approximate cost of US$90,000 million per year[4].

Furthermore, the Connectivity Index or, Networked Readiness Index (NRI)[5] from the World Economic Forum, 2016, Costa Rica is at position 44 only surpassed by Chile (38th position) and Uruguay (43th position) of Latin American countries.

In addition, Costa Rica heads the exports of value-added services in Latin America, which includes: telecommunications, information and other services. The foregoing represents 6.8% of GDP according to 2015 statistics, Honduras in second place (1.5% of GDP)[6].

According to data presented on the National Science, Technology and Innovation Indicators Report, Costa Rica 2014 "The weight of ICT exports as regards export of the country's total goods, shows this sector is highly important. The 2006- 2014 period, it represented over 41% and in 2014, 56.6%, of the country's total exports."[7]

[3] *BID-OEA. (2016). Cybersecurity Report 2016.*

[4] *Idem.*

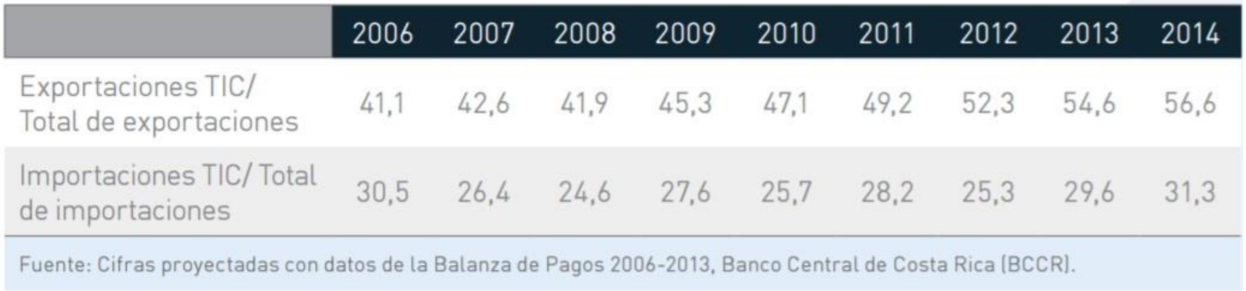
[5] *This index measures "…the propensitu of countries to take thes opportunities offered by information and communications technologies. It is published every year and seeks to better understand the impact of ICT on the competitiveness of nations". Available at http://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.1_2016.pdf*

[6] *Costa Rican Development Initiatives Coalition (CINDE) (2016). Investing on Costa Rica: Services. Costa Rica.*

CINDE: Costa Rica. Based on data of the Central Bank of Costa Rica, of the International Monetary Fund and Trademark.

[7] *MICITT (2014).National Indicators Report Science, Technology and Innovation. Available at http://cdn-s3.myvirtualpaper.com/i/intergraphicdesigns-micitt/indicadores-2014-vp/2016101901/upload/indicadores-2014-vp.pdf*

Table 1 Participation of exports and imports of the ICT sector as related to the country's total exports and imports, 2006-2014



	2006	2007	2008	2009	2010	2011	2012	2013	2014
Exportaciones TIC/ Total de exportaciones	41,1	42,6	41,9	45,3	47,1	49,2	52,3	54,6	56,6
Importaciones TIC/ Total de importaciones	30,5	26,4	24,6	27,6	25,7	28,2	25,3	29,6	31,3

Fuente: Cifras proyectadas con datos de la Balanza de Pagos 2006-2013, Banco Central de Costa Rica (BCCR).

Source: Extracted from National Science, Technology and Innovation Indicators Report, Costa Rica 2014

The telecommunications sector has shown great dynamism with important beneficial impacts for users and the country. As observed in the following table, both total income and the human resource employed in the sector have constantly increased since the year 2011.

Table 2 Data of the telecommunications sector, 2011-2015

Indicator	2011	2012	2013	2014	2015
Sector's aggregated data					
Total income (million colones)**	437,672	501,648	576,742	744,300	802,812
Total income/GDP (percentage)	2.3%	2.4%	2.6%	3.1%	3.1%
Total investment/GDP (percentage)	2.1%	2.4%	1.0%	1.0%	1.0%
Total human resource employed	9,618	9,900	10,422	11,002	11,426
Total human resource employed /Total economically active population	0.4%	0.4%	0.5%	0.5%	0.5%

*Notes: ** These figures don't include income associated to television service by subscription.*
Source: Statistics of the telecommunications sector 2015. SUTEL. Available at:
https://sutel.go.cr/sites/default/files/estadisticas_del_sector_telecomunicaciones_costa_rica_2015.pdf

As may be observed in the following table, this is accompanied by an increasing adoption of Internet access by Costa Ricans, fixed and mobile Internet services.

Table 3 Subscriptions to the data transfer service 2011-2015

Indicator	2011	2012	2013	2014	2015
Transfer of data					
Acces to Internet total subscriptions	2.008.763	3.118.155	4.028.302	4.806.217	5.420.554
Acces to fixed-wired Internet total subscriptions	414.384	439.043	474.433	503.347	545.813
Acces to fixed wireless Internet total subscriptions	5.398	8.904	10.450	12.493	12.843
Suscripciones totales acceso a Internet móvil	1.588.981	2.670.208	3.543.419	4.290.377	4.861.898
Suscripciones totales acceso a Internet fijo/100 habitantes	9%	10%	10%	11%	12%
Suscripciones totales acceso a Internet fijo/100 viviendas	32%	34%	36%	37%	39%
Suscripciones totales acceso a Internet móvil /100 habitantes	35%	57%	75%	90%	101%
Suscripciones totales acceso a Internet móvil /suscripciones totales telefonía móvil	38%	50%	50%	61%	65%
Cantidad total conexiones de lines ofdicadas	10.273	11.993	16.375	16.286	14.093

Source: Statistics of the telecommunications sector 2015. SUTEL. Available at:
https://sutel.go.cr/sites/default/files/estadisticas_del_sector_telecomunicaciones_costa_rica_2015.pdf

For 2015, the data show 39% of households had fixed Internet connection and mobile reached 101% so it's highly important adopting the necessary measures so the country is prepared for possible attacks and users know the risks, and actions to be taken to protect their data in the cyberspace, especially because the country is making efforts to expand networks throughout the territory; it is expected that with the network deployment financed with resources from the National Telecommunications Fund (FONATEL), all the population will have access to the technologies.

With the impending growth of broadband networks and the use of and utilization of ICT, the exposure of sensitive data is tangible as is the risk of the networks to possible cybernetic attacks.

3.2 ICT and cybersecurity: national planning perspective

Information and Communication Technologies are considered as invaluable tools for the country's development; evidence is the increase of access, use and appropriation indexes for these. In that sense, the Costa Rican State has tried to incentive the incorporation of ICT and Internet connectivity in every field of national life; this is reflected on national planning through its planning instruments. The foregoing shows the importance of mentioning the contents of some of these instruments on the matter.

3.2.1 Document "Costa Rica 2030: National Development Objectives"

The document sets the country's development objectives with a long-term vision; at the same time promotes cross-sectional collaboration and exchange of information. It establishes that development of ICT plays a supporting role in many dimensions, including economic growth, social and cultural investment, and infrastructure. On "Economic Dimension" includes the topic of infrastructure indicating that "… infrastructure (roads, ports, airports, schools, high schools, clinics, hospitals, EBAIS, power services, water supply, management of solid waste, telecommunications services, community infrastructure, etc.) constitute a support and inescapable condition to achieve sustained high growth rates" [8] . Among the objectives it highlights: "Guarantee telecommunications with diversity of services, coverage to every town in the country". This objective is to guarantee universal Internet access through incremental increases of connectivity at the national level[9].

3.2.2 "Alberto Cañas Escalante"National Development Plan 2014-2018

This plan sets out the priorities, objectives, programs and projects the Solís Rivera Administration has outlined over three pillars, namely: 1) drive economic growth and

[8] *Ministry of Planning and Economic Policy (MIDEPLAN). (2013). Costa Rica 2030: National Development Goal. San José: MIDEPLAN. P. 13. Recovered from, http://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/0311bebc-87c5-4c22-9731-21c04744f254/Costa%20Rica%202030%20web.pdf*

[9] *Idem, p. 30.*

generate quality employment; 2) combat poverty and reduction of inequality and 3) an open, transparent, efficient government, in frontal assault against corruption. In this plan telecommunications are regarded as a basic service to combat poverty and develops a strategic sectorial proposal for the Science, Technology and Telecommunications proposal establishing "…the development of projects stipulating the regulation through legal instruments and rules to potentiate performance, promoting the interaction of different actors, creating a physical space, to produce and multiply people's scientific technological capacities"10. This Plan underscores the importance of Cybersecurity with a Program to enhance the Electronic Government.

3.2.3 National Development Telecommunications Plan 2015-2021 "Costa Rica: a connected society"

This plan intends to put into practice the projects of universal access and service and solidarity, besides facilitating the increase of quality telecommunications services at commercial and residential level offered to the public, including the expansion of affordable and innovative services offered. The plan is articulated as three large pillars, namely: Digital Inclusion, Electronic and Transparent Government and Digital Economy. Its highest aspiration is: "Transform Costa Rica into a connected society, based on an inclusive approach to the access, use and appropriation of the information and communications technologies, safely, responsibly, and productively"[11].

The abovementioned subjects are drawn along three great aspirations:

1. Consolidate projects of universal access, universal service and solidarity of Telecommunications/ICT.
2. Create an enabling environment allowing the innovation of sound and television broadcasting towards its digitization.
3. Build the bases of the Digital Cities Model, jointly, with an imminent Electronic Government.

[10] *Ministerio de Planificación y Política Económica (MIDEPLAN). (2013). Plan Nacional de Desarrollo 2014-2018 "Alberto Cañas Escalante". San José: MIDEPLAN. p. 438. Recovered August 17th of 2016 from, http://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/cd1da1b4-868b-4f6f-bdf8-b2dee0525b76/PND%202015-2018%20Alberto%20Ca%C3%B1as%20Escalante%20WEB.pdf*

[11] *Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2015). Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021. Recovered August 17th of 2016 from, https://www.micit.go.cr/images/Telecomunicaciones/pndt/PNDT-2015-2021.pdf*

Likewise the NDP mentions Cybersecurity as a fundamental subject within the pillars of an Electronic and Transparent Government. It seeks for the country to have the Cybersecurity protocols implemented in the different Ministries comprising the Executive Power by 2021; therefore developing this strategy at national level is essential as baseline of what said instruments pursue.

3.3 Telecommunications sector and its advances

3.3.1Regulatory framework and its relationship with cybernetic security

By the General Law of Telecommunications, Act N° 8642 and the Law for the Strengthening and Modernization of Public Entities of the Telecommunications Sector, Act N° 8660 the Telecommunications Sector was created, designating the Ministry of Science, Technology and Telecommunications, as the sector's lead agency, in charge among other aspects of issuing the public policy; the Telecommunications Superintendency is constituted (SUTEL), as autonomous body attached to the Public Services Regulating Authority (ARESEP), in charge of the regulation.

The legal framework is also complemented with a series of regulations which implement the mandate of the laws mentioned. In particular, what refers to Cybernetic Security topics, the Regulation of Protection Measures for Privacy of Communications[12] can be noted which elaborates on what article 42 of the General Law of Telecommunications provides; Act N° 8642 and the Regulation for Protection to the Final User of Telecommunications Services.

In 2012 SUTEL promoted compliance to what's established in Costa Rican legislation as to what's provided by article 56 paragraph f) of the Regulation of Protection for Final User of Telecommunications Services, which refers to the subject of frauds against users, specifically in the field of cellular phones robbery and reactivation. During that year meetings were carried out with operators and suppliers of telecommunications services, to fulfill with compliance and determine the best practices for the inclusion of IMEIS to the blacklists; integration to Groupe Speciale Mobile Association (GSMA) was the chosen solution, due to the number of

[12] *Reference can also be made to Executive Decree DE 35.205 16-04-2009 Reglamento Protección Privacidad de Comunicaciones y el Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones, of ARESEP Reglamento 010 published in Gaceta N° 72 April 15th of 2010.*

countries integrated to it for the exchange of information. GSMA, grouping over 200 countries and approximately 800 mobile phone operators, has the databases of stolen terminals available for operators (blacklist).

In March of 2012 a Memorandum of Understanding was signed between the mobile telephone operators in the country and GSMA. In said Memorandum a public commitment was agreed of integrating the databases of the terminals stolen to such organization and thus blocking the use of such terminals at country level for the totality of countries integrated to GSMA. In so doing, Costa Rica was the first country in Latin America to connect all its operators with the database of GSMA's stolen terminals. This event made the difference in the region in the fight against theft of terminals[13].

With the aim of having a tool for addressing fraud by subscription, in conformity to what's provided in article 43 of the Protection Regime of Final User of Telecommunications Services[14], there is the obligation of carrying out an adequate record of the prepaid services users. For this, SUTEL has carried out proceedings to promote the filtering of information from these records, particularly considering the existence of a large number of reports of users, and reports showing inconsistencies in the record by the operators of prepaid services. Also, several entities such as the Judicial Power (PJ) and the Ministry of Public Security (MSP) have insisted on the need of having a more reliable record of users, even more when considering SUTEL's duty of veiling for the rights of telecommunications users, as established by valid legislation.

In compliance to Law Nº 8934, Childhood and Adolescents Protection Law Facing the Harmful Contents on the Internet and Other Electronic Media, SUTEL's council adopted agreement 024-019-2012 specifying the information and filters Internet cafés should implement for childhood's protection in agreement with the constant search of protecting the population, not only in the physical world but also in the digital that in spite of being virtual has real consequences.

[13] *GSMA. (20 de mayo de 2012). Mobile Phone Theft in Latin-America: The example of Costa Rica and the need of coordination among operators. Web site. [Online]. Available at: http://www.gsma.com/latinamerica/mobile-phone-theft-in-latin-america/*

[14] *Regulation for the Protection Regime of Telecommunications Services Final Users, ARESEP Reglamento 010 published in Gaceta N° 72 April 15th of 2010: https://sutel.go.cr/sites/default/files/normativas/reglamento_sobre_el_regimen_de_proteccion_al_usuario_final_de_los_servicios_de_telecomunicaciones.pdf*

In matters of generating capacities, SUTEL collaborates with the Judicial School giving lectures and training for the judges in matters of security, within the framework of the training program in telecommunications implemented by said School.

Within the regulatory framework, Costa Rica has updated its national regulations creating legal development for the protection of Costa Rican cyber-society, enabling the possibility for people to report breaches suffered in the virtual world which had no legal answer before. Among these, stands out the Law for Protection of Persons for the Processing of Personal Data and its Regulation, thus the creation of the Agency for Inhabitants' Data Protection (PRODHAB), governing body in this matter.

There is also the Law for Informatics Crimes, Act Nº 9048 and the Reform of various articles and amendment of section VIII, denominated Informatics Crimes and Related from title VII of the Criminal Code instituting a more complete legal framework and in agreement with the new crimes committed with technological means.

Searching to improve the Costa Rican regulatory framework and achieve a better operation before computer crime, Costa Rica consolidated the accession process to the “Convention o Cybercrime” known as the “Budapest Convention” by signing Executive Decree N° 40546-RREE on July 3 of 2017 which supports the fight against informatics crimes.[15]

With the purpose of having a unit in charge of collecting evidence for addressing crimes associated to technology, the Section of Informatics Crimes was created in 1997, as Unit of Informatics Investigation, attached to the Department of Criminal Investigations; it was born out of the need of processing information stored in computers and servers from important cases; it was constituted in 2002 as Section of Informatics Crimes.

This section carries out research of informatics crimes and others related to technologies where it's utilized to commit a criminal act or as evidence. Forensic computer techniques are used to that end, aligned with international standards in the collection, preservation and the

[15] *Ministerio de Relaciones Exteriores y Culto (2017). Executive Decree N°40546-RREE. Available at http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=84643&nValor3=109293&param2=1&strTipM=TC&lResultado=1&strSim=simp*

analysis of exhibits, guaranteeing the chain of custody in computers, telephones, and other data processing and storage devices.

3.3.2 Internet Exchange Point

According to studies of the project CEPAL @LIS2: Balances, challenges and projections "… 80% of internet's Latin American traffic still passes through networks in the United States; utilization of international connections in some countries increases prices up to 40%"[16].

In Costa Rica's case, for 2014 MICITT and the National Academy of Sciences (ANC) worked jointly to impulse the creation of the Costa Rican Internet Exchange Point (CRIX) constituted as project of public interest by Executive Decree Nº 38388- MICITT, "Declaratory of Public Interest: The Internet Traffic Exchange Point of the National Academy of Sciences" in La Gaceta Nº 93 of Friday, May 16 th of 2014[17].

Internet Exchange Point of Costa Rica (CRIX), is administered by NIC Costa Rica, entity in charge of the administration of the higher-level domain .cr and its categories . co.cr, .fi.cr, .or.cr, .sa.cr, .ed.cr, .ac.cr y .go.cr; which has managed to build a network of national confidence for local infrastructure of the Internet.[18]

Added to this, the country has become one of the first in the world implementing the origin validation (RPKI) in its Internet Exchange Point (IXP). This validation enables the strengthening of local Internet traffic in turn avoiding hijacking of routes, seeking among other things, the capture of

[16] *MICITT. Boletín Contacto Digital. IXP Costa Rica: A strategic opportunity. MICITT: Department for the Information Society. Recovered March 2nd of 2017 from, https://www.micit.go.cr/index.php?option=com_content&view=article&id=6329&catid=59&Itemid=1574*

[17] *MICITT. Boletín Contacto Digital. IXP Costa Rica: A strategic opportunity.. MICITT: Department for the Information Society. Recovered March 2nd of 2017 from, https://www.micit.go.cr/index.php?option=com_content&view=article&id=6329&catid=59&Itemid=1574*

[18] *NIC CR. (14 de mayo de 2015). Web site NIC CR. "Costa Rica among the first in the world to implement Origin Validation at Internet Exchange Points (IXP)". Recovered August 24th of 2015 from, https://www.nic.cr/en/article/costa-rica-among-first-world-implement-origin-validation-internet-exchange-points-ixp*

traffic with sensitive information (such as bank accounts, passwords, etc.), and distributed denial of service attacks o- DDoS.[19]

3.3.3 Cybernetic Security Practices of Operators in Costa Rica

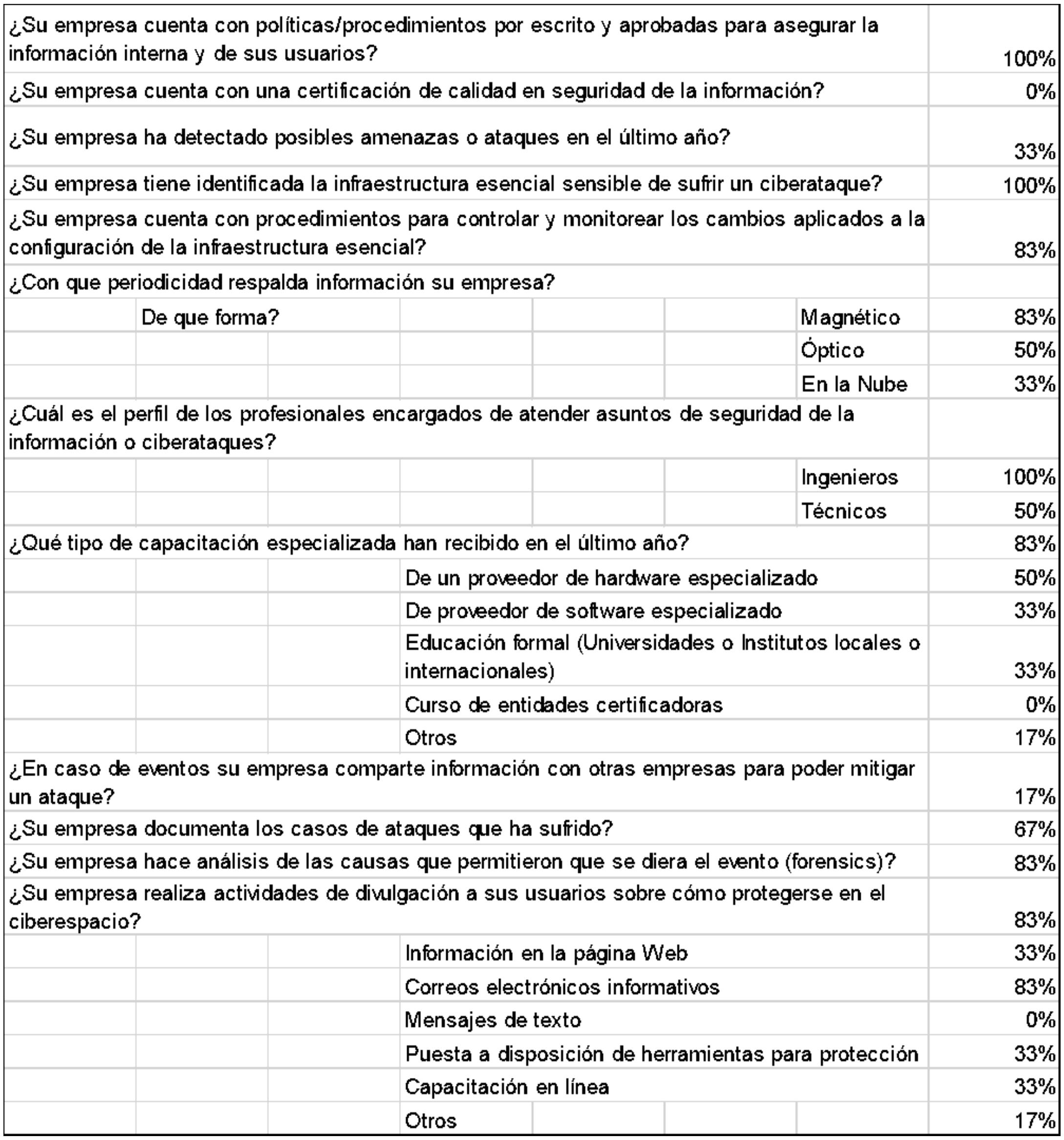
As part of the construction of this National Strategy of Cybernetic Security, SUTEL supported by carrying out a consultation aimed at operators and suppliers on the practices implemented on cybersecurity matters. A brief analysis of results is presented following.

The questionnaire was submitted to 17 companies of the sector in 2015[20], which included questions about frequent practices of information security that would be applied by operators and suppliers of telecommunications services; information on the type of personnel assigned to security tasks; identification of critical infrastructure; information sharing in case of events and documentation of cases. Following, a summary of the answers received is presented.

[19] *NIC CR. (14 de mayo de 2015). Web site NIC CR. "Costa Rica among the first in the world to implement Origin Validation at Internet Exchange Points (IXP)". Recovered August 24th of 2015 from, https://www.nic.cr/en/article/costa-rica-among-first-world-implement-origin-validation-internet-exchange-points-ixp*

[20] *Consultation done by official letter 04948-SUTEL-CS-2015 of July 24th of 2015.*

Table 4 Summary of the questionnaire's replies about cybernetic security practices carried out by SUTEL to operators and suppliers



¿Su empresa cuenta con políticas/procedimientos por escrito y aprobadas para asegurar la información interna y de sus usuarios?		100%
¿Su empresa cuenta con una certificación de calidad en seguridad de la información?		0%
¿Su empresa ha detectado posibles amenazas o ataques en el último año?		33%
¿Su empresa tiene identificada la infraestructura esencial sensible de sufrir un ciberataque?		100%
¿Su empresa cuenta con procedimientos para controlar y monitorear los cambios aplicados a la configuración de la infraestructura esencial?		83%
¿Con que periodicidad respalda información su empresa?		
De que forma?	Magnético	83%
	Óptico	50%
	En la Nube	33%
¿Cuál es el perfil de los profesionales encargados de atender asuntos de seguridad de la información o ciberataques?		
	Ingenieros	100%
	Técnicos	50%
¿Qué tipo de capacitación especializada han recibido en el último año?		83%
	De un proveedor de hardware especializado	50%
	De proveedor de software especializado	33%
	Educación formal (Universidades o Institutos locales o internacionales)	33%
	Curso de entidades certificadoras	0%
	Otros	17%
¿En caso de eventos su empresa comparte información con otras empresas para poder mitigar un ataque?		17%
¿Su empresa documenta los casos de ataques que ha sufrido?		67%
¿Su empresa hace análisis de las causas que permitieron que se diera el evento (forensics)?		83%
¿Su empresa realiza actividades de divulgación a sus usuarios sobre cómo protegerse en el ciberespacio?		83%
	Información en la página Web	33%
	Correos electrónicos informativos	83%
	Mensajes de texto	0%
	Puesta a disposición de herramientas para protección	33%
	Capacitación en línea	33%
	Otros	17%

Source: Own elaboration. SUTEL. Consultation done by official letter 04948-SUTEL-CS-2015 July 24th of 2015.

It's worth noting that 100% of the companies indicated they had a policy or internal procedures to guarantee the security and privacy of the internal information and their users. The above shows this is an important subject for the sector's companies and they have searched for mechanisms to ensure the integrity of that information.

Despite only one third of the consulted companies state having detected possible threats or experiencing an attack over the last year, 100% affirm having their essential infrastructure identified; 83% count with procedures to control and monitor changes made on it. Similarly, the totality of operators and suppliers of telecommunications services surveyed mention having engineers dedicated to cybernetic security-related labors, and in 83% of the cases, have received some kind of training last year. These results show how companies have taken measures on this subject and prepared their personnel.

However, from the answers we could extract companies do not coordinate between themselves facing cyberattacks or share information; also, cases are not all documented. In addition, the efforts to disseminate information between the users, made by operators and suppliers diverge and don't reflect a coordinated objective; this is also a topic which should be contemplated by the strategy.

3.3.4 National Digital Certification System

Through the enactment of Act Nº 8454, of Certificates, Digital Signatures and Electronic Documents, the legal grounds were implemented to issue and use digital signature certificates in the country, providing the legal security necessary so that electronic documents signed digitally had the same value as documents with handwritten signature.

In August of 2009, the Digital Certification System was launched; it was designed to offer safer online transactions. According to the Law, the agency issuing digital certificates should be registered with the Digital Signature Certifiers Management (DCFD) of MICITT and ensure compliance to the standards of security and operation endorsing electronic transactions.

The existing legal framework in the country allows guaranteeing the transactions' legal security; the protection of consumers' rights and credibility of the national digital certification system while endorsing the transactions electronically, giving legal equivalence to physical documents and those issued by electronic means. The system's regulation and the guidelines are enacted by the Ministry of Science, Technology and Telecommunications (MICITT).[21]

The Central Bank of Costa Rica has constituted a Certifying Authority for issuance of digital signature certificates for physical persons (CA SINPE – Physical Person) and legal persons (CA SINPE- Legal Person), besides enabling the service of time stamps (TSA SINPE)[22]. Use of these certificates has strengthened the public sector, as well as the services offered, guaranteeing safer online transactions.

3.3.5 Costa Rica Computer Security Incident Response Team: CSIRT-CR

This Team was formed by Executive Decree Nº 37052-MICIT of March 09 of 2012[23]. This provision designates CSIRT-CR as the agency in charge of coordinating everything related to matters of informatics and cybernetics security. It is further empowered to have a team of experts in Information and Communication Technologies security in charge of preventing and responding to incidents of informatics and cybernetic security affecting governmental institutions.

CSIRT-CR seeks the implementation and management of technological measures with the purpose of mitigating the risk of attacks against the community's systems providing the service, so as to incorporate the cybernetic security system and information technologies to the Central Government and Autonomous Entities' protection and decrease cybernetic risks and threats.

The team is in charge of MICITT's Directorate of Digital Governance; however, its operation is presently limited owing to lack of resources in the public sector. Tasks carried out to this date have mainly consisted of generation of capacities of the public sector's officials, through different cybersecurity trainings. In addition, CSIRT-CR, has assumed the task of raising awareness and informing, with support from specialists in different fields on relevant topics as Deep Web and security in bank transactions.

[21] *Digital Signature web site. [Online]. Available at: http://www.firmadigital.go.cr/Leyes.html*

[22] *Digital Signature web site. [Online]. Available at: http://www.firmadigital.go.cr/Leyes.html*

[23] *Creation of the Computer Security Incident Response Team CSIRT-CR, Decree Nº 37052-MICIT, Creates Computer Security Incident Response Team CSIRT-CR. Diario Oficial La Gaceta de la República de Costa Rica, March 09 of 2012. Available at: http://www.gaceta.go.cr/pub/2012/04/13/COMP_13_04_2012.html#_Toc321989832*

There is the need of having a specific approach in aspects of CSIRT- CR's development to guarantee a better functionality and sustainability. These measures will make it operate efficiently and be equipped to rapidly determine threats and apply measures against them, to prevent future threats and recover from existent ones. CSIRT shall require the assignment of an explicit budget and an operational plan to be able to materialize the functions assigned.

3.3.6 National Commission for Online Security

The National Commission for Online Security (CNSL)[24] was created in 2010, by Decree Nº 36274-MICIT with the main objective of designing the necessary policies for the good use of Internet and the Digital Technologies, contributing to create a culture of understanding, analysis and responsibility in people so they benefit from the advantages of using ICT and have aware and proactive attitude before the inherent risks of using these resources.

The commission is headed by MICITT and integrated by representatives of the Ministry of Public Education, Ministry of Culture and Youth, National Child Welfare Agency, Judicial Power, SUTEL, CAMTIC, Fundación Omar Dengo and Fundación Paniamor.

According to what the Executive Decree Nº 36274-MICIT points out many actions of the Commission should be aimed at vulnerable populations in the use of online technologies; one of these populations is childhood and adolescents in all the country. In this sense the commission formulated a work plan, based on four central themes from which derive a series of work lines; they include the strengthening of the regulatory framework, consolidation of inter-institutional articulation mechanisms, development of projects promoting online security and fostering research as basis for the formulation of actions.

3.3.7 Automation and Digitization of Online Services Available to Citizens

As regards development of projects in technology, the country has created a series of initiatives in different areas such as access to public information, automation of proceedings and

[24] *Costa Rican Legal Information System Web Site: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=69239&nValor3=83075&strTipM=TC*

citizen security where the following are to be mentioned:[25] Citizens' Portal, Open Data, Registry of Products of Health Interest, Electronic Services Window (VES), Crea Empresa, MuNet e-Government and most recently the Public Purchasing System (SICOP).

In health matters, the Single Digital Health Record (EDUS) is noteworthy, a program fostered by the Costa Rican Department of Social Security and defined as: "the set of informatics applications which automate health system at the three (3) levels of attention in agreement with the health services model the institution operates with"[26].

As relates to con citizen security, the Ministry of Public Security (MSP) has a platform for safety officers and company's registration procedures, as well Carrying Weapons Control and Private Private Security (ControlPas)[27].

As to the ICT's public management, it's necessary to underscore the inter-institutional coordination processes; such is the case with the drivers' licenses management and passports at the Bank of Costa Rica (BCR) agencies. This is owing to the systems' interoperability of the General Migrations and Foreign Citizens Bureau and the Ministry of Public Works and Transport (MOPT) with BCR's platform28

Another important body providing online administrative and electoral services is the Supreme Electoral Court (TSE); among the services offered is the management of documents of citizens and residents, civil records, marriage contracts and the electoral roll.

Additionally, Costa Ricans have online access to public legal information in virtue of a number of government entities having adopted the ICT to provide their services electronically. As part of the Modernization of Justice Administration project, the Judicial Power, the Attorney General's Office (PGR) and the Inter-American Development Bank (BID) came together and developed the Costa Rican Legal Information System (SCIJ) 29. The system contains regulatory and jurisprudential information on Costa Rican law.

[25] *Taken from Technical Report IT-DGE-2014-005. References can currently be found at: http://gob.go.cr/es/*

[26] *Medical Management's Official Letter GM-42211/GIT-411556-2010 October 20th of 2010.*

[27] *ControlPAS. Taken from: https://www.controlpas.go.cr/Inicio/Informacion*

[28] *http://bcrcita.bancobcr.com/cita/RequisitosPasaporte.aspx*

[29] *Costa Rican Legal Information System Web Site. [Online]. Available at: http://www.pgrweb.go.cr/scij/*

Costa Rica's legal system is also implementing a comprehensive electronic justice portal offering diverse online legal services.30 These include institutional audits and records available publically, missing persons, the most-wanted list, convicted fugitives' reports and literature on national statutes and laws. The portal also allows citizens to present police reports, pay for legal services and request legal consultation within the country's Court Circuit. At least nineteen courts have the capacity to receive online requests for consults. With these services, the judicial system has the objective of creating a more transparent and simple process for citizens searching legal assistance.

As regards the taking of evidence, the Judicial Power has jurisdictional authority, in conformity to article 24 of Act N° 7425, "Act Concerning Search, Seizure and Examination of Private Documents and Interception of Communications" 31 to intervene in any communication, oral, written or other type, including fixed, mobile, wireless and digital telecommunications. This aspect is quite important since electronic evidence implies both security and privacy elements.

With the increase in the number of cases of digital evidence, the interoperability within the judicial system should be taken into account to decide on these, and thus guarantee their safety and integrity.

In addition and in the interest of making judicial information known, the Judicial Power carries out this process taking as reference what's established by Act Nº 8968 "Act on Protection of Individuals with regard to the Processing of Personal Data" and the document Minimum Rules for Disclosure of Judicial Information on the Internet where they implement the best practices to find balance between privacy and transparency at the moment of making judicial data available to the public[32].

[30] *Judicial Power of the Republic of Costa Rica Web site. [Online]. Available at: http://www.poder-judicial.go.cr/*

[31] *Act Concerning Search, Seizure and Examination of Private Documents and Interception of Communications. Nº 7425. Diario Oficial La Gaceta de la República de Costa Rica, August 09 of 1994. Available at: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=16466&nValor3=17615&param2=1&strTipM=TC&lResultado=3&strSim=simp*

[32] *Heredia's rules: Minimum rules for the Disclosure of Judicial Information on the Internet, Seminar on Internet & Judicial System, Heredia, July 09 of 2003. [Online]. Available at: http://www.iijusticia.edu.ar/heredia/Heredia_Rules.htm*

3.4 Training in Cybernetic Security

The country is acknowleged for the important investment made on the education sector; by constitutional mandate the country dedicates 8% of the Gross Domestic Product to (GDP) education. Being a highly relevant area for the country, incorporation of ICT into education, has also been considered a national priority, and there are diverse projects since the late 80's.

At present, MEP, MICITT and SUTEL, in unison to other public organizations, non-governmental, private, academic and civil society have implemented projects to narrow the gaps in education through the use of ICT, employing resources of the National Telecommunications Fund (FONATEL). The objective of these initiatives has been to transform teaching and learning processes through the universal access to broadband connectivity, mobile technologies and the education support instruments of ICT for teachers and students.

At present 63% of educational institutions at secondary level have a computer laboratory, compared to 23% for primary schools 33 and efforts are on the way to improve these figures.

As refers to the training of professionals, public and private universities offer careers with graduate, post-graduate and specializations34 in themes related to ICT; however, not necessarily including specializations in Cybernetic Security, except for a private education center which offer training at master's level.

The program of this post-graduate in Cybersecurity, is oriented to the training of professionals of information and communication security; in the development of technical and management abilities, as well as an introduction to the required theoretical aspects in this field. To complete the program, students must perform two applied research projects, with the incorporation of the learned concepts, to solve a cybernetic security problem in the real world. This program is supported by a series of multinational ICT companies; notwithstanding since this career is in the

[33] *Use of ICT on Latin America and the Caribbean's education – Regional analysis of ICT's integration and digital aptitudel (e-readiness) - UNESCO Institute for Statistics: http://www.uis.unesco.org/Communication/Documents/ict-regional-survey-lac-2012-sp.pdf*

[34] *In diverse subjects as: computers and informatics, telematics and networks, information systems, IT management, project managements, IT audits and data base systems engineering.*

private education sector access possibilities are limited by the economic investment required.

When considering the association with higher education institutions, different approaches must be taken into account based on the nature of constituting each one. For example, public universities are autonomous, although having common standards and coordinating among them (National Council of Rectors (CONARE) / Higher Education Planning Office (OPES)); the National Council for Higher University Education (CONESUP) authorizes and supervises private universities and the National System for Higher Education Accreditation (SINAES) certifies authorized public and private academic programs.

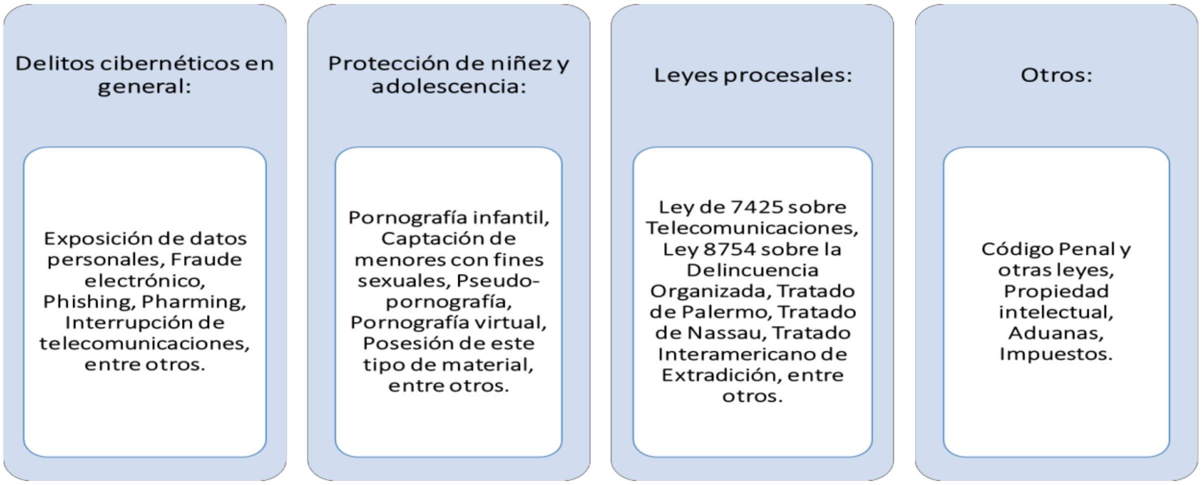
In view of the foregoing, there is a need for joint work with various educational institutions and accreditation organisms to open courses including relevant aspects of information/cybernetics security. In addition, it's important to take in consideration the scientific school's network and those having computer laboratories, to foster the teaching of the fundamental aspects of cybernetic security from secondary education.

3.4.1 Strengthening of the legal framework for addressing cybercrime

It is often complex to prevent a cybernetic crime and sometimes even more difficult identifying the author. Cybernetic crimes can be described in two ways: crimes against an informatics system (for example, harm or unauthorized access to data, programs or networks) and crimes facilitated through an informatics system (for example, publication of child pornography). Along these lines, there are various laws in Costa Rica[35] engaged in cybernetic crime, directly and indirectly. The next figure summarizes the topics included.

[35] *Computer-related crimes and associated, Act N° 9048. Diario Oficial La Gaceta de la República de Costa Rica, November 06 of 2012. Available at:*
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=101586&param2=1&strTipM=TC&lResultado=1&strSim=simp
Amendment of articles 196, 196 bis, 230, 293 and 295 and addition of article 167 bis to the Criminal Code, Act N° 9135. Diario Oficial La Gaceta de la República de Costa Rica, April 26th of 2013. Available at:
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74706&nValor3=92348&param2=1&strTipM=TC&lResultado=1&strSim=simp

Figure 2 Topics Treated by the Laws of Costa Rica Concerning Informatics Crimes



Delitos cibernéticos en general:	Protección de niñez y adolescencia:	Leyes procesales:	Otros:
Exposición de datos personales, Fraude electrónico, Phishing, Pharming, Interrupción de telecomunicaciones, entre otros.	Pornografía infantil, Captación de menores con fines sexuales, Pseudo-pornografía, Pornografía virtual, Posesión de este tipo de material, entre otros.	Ley de 7425 sobre Telecomunicaciones, Ley 8754 sobre la Delincuencia Organizada, Tratado de Palermo, Tratado de Nassau, Tratado Interamericano de Extradición, entre otros.	Código Penal y otras leyes, Propiedad intelectual, Aduanas, Impuestos.

Source: Own Elaboration, 2016.

Legislation on cybernetic crime should consider the national context, international conventions, mechanisms for enabling inter-institutional and multi-jurisdictional investigation and the greater complexity of technological advances. Costa Rica has legislation related to informatics crimes; notwithstanding, as the sophistication of these crimes changes, there should be a process dedicated to its review and updating to ensure there is the authority necessary to investigate and process it effectively. Adherence to the Convention on Cybernetic Crime (also known as Budapest Convention) is a fact and discussions are on the way within of the Judicial Power for the training of judges and prosecutors in cybernetic crime matters.

However, in achieving those goals, a distinction should be made between the technical capacity to detect and identify vulnerabilities and the procedural tools necessary so that law enforcement agencies effectively investigate cybernetic crimes (taking into account the speed and transient nature of digital data). The roles and responsibilities of the Internet services suppliers should be considered, as well as any other actor active in cyberspace; also balancing these actions with the need to respect the fundamental human rights while collecting digital evidence. So, given the nature of the digital world it’s necessary to count with the corresponding mechanisms to ensure the periodical review and update of informatics crimes legislation.

Chapter 4 – Guiding Principles

This strategy is motivated on the following guiding principles:

- People are the Priority
- Respect for Human Rights and Privacy.
- Coordination and co-responsibility of Multiple Stakeholders.
- International Cooperation

4.1 People are the Priority

People are the strategy's focus. The use of ICT in the different fields of daily life obliges us to include all country citizens in the strategy, so co-responsibility in the individual use of devices and networks shall be essential.

With the foregoing, use of ICT as an instrument for life quality improvement shall be safely promoted, seeking to raise awareness on the consequences of the responsible use through education from the earliest ages. Any action should have the priority of involving the attention and mitigation of risks having an impact mainly on vulnerable populations as childhood, adolescents, the elder adults, indigenous populations and people with some type of disability.

4.2 Respect for Human Rights and Privacy

Access to information and respect for privacy, are fundamental to guarantee respect for human rights, specifically those related with access to ICT. The resulting measures and actions from this strategy should always safeguard human rights and the privacy of the information for all citizens of the country.

Consequently, this strategy has been developed taking into account the need to balance the protection of every citizen and respect for the basic and essential human rights, with the need to implement measures to keep them safes online. This includes respecting liberty of expression, freedom of speech, right to privacy, freedom of opinion and freedom of association.

4.3 Coordination and Co-responsibility of Multiple Stakeholders

Cybersecurity is a responsibility shared by all actors participating in the digital ecosystem, which including users. Whenever relevant, it's imperative all actions derived from this strategy take into account, the participation and contribution of all stakeholders, co-responsibility of these and the need of coordination among different actors.

For the process of implementation, support of all sectors is essential; so, the public-public, public-private and public-civil society models should be considered and promoted; as appropriate, the requirements and outreach of the objectives to implement.

4.4 International Cooperation

The cross-border nature of digital technologies requires the subject of cybersecurity be addressed from a global perspective. Cybernetic threats have no borders; therefore, international cooperation becomes key element both for addressing threats and for the transfer of knowledge and development of local and global actions assisting to increase confidence and global security.

Hence, the construction of alliances, agreements and the strengthening of ties with other public and private entities attending Cybersecurity related topics at regional and international level should be key elements, among others.

Chapter 5 – Strategic Framework for Cybernetic Security

The advantages of Internet connection and the use of ICT are undeniable; they offer a platform potentiating each one of the country's economic sectors and can be put to use for improving public administration, competitiveness of the corporate sector and the quality of life of country residents; so, we should aim at developing an agile, modern, robust and safe digital infrastructure.

In this sense and given the rapid evolution of digital technologies, the National Cybersecurity Strategy of Costa Rica should be considered as a living document, establishing the country vision in these matters, resulting from the definition of a general objective and a series of specific objectives comprised by various strategic lines, to be developed as action plans in the short term and jointly making up the national cybernetic security.

The strategy shall seek support and participation of public and private entities, as well as non-governmental organizations, the technical community, the academy and civil society. MICITT as main responsible entity and for aspects related to incidents, CSIRT-CR.

Given the nature of the lines of action active participation shall be sought from state powers, as well as the corporate sector, civil society organizations, non-governmental organizations, the academy, the technical community, professional association and any other actor interested in participating on the strategy's implementation.

Once the National Cybersecurity Strategy is officially launched, MICITT shall have a term of three months to create, summon and gather an Advisory Board, comprised by:

- ✓ Two representatives of MICITT
- ✓ One representative of the Judicial Power
- ✓ One representative of SUTEL
- ✓ Two representatives of civil society
- ✓ Two representatives of the academy
- ✓ Two representatives of the Private Sector

MICITT shall also be established as national coordination figure, with the responsibility of supervising the strategy's application, including coordination with various entities involved in fulfillment of the established lines of action.

The Advisory Board, jointly with the National Cybersecurity Coordinator, will be in charge of arrange all actions necessary to start the process of implementation, with action plans for each one of the objectives proposed in this strategy, prior definition of goals, terms and accountable.

5.1 Overall Objective

Develop a guiding framework for the country's actions in matters of safety in the use of ICT, promoting the coordination and cooperation of the multiple stakeholders and fostering education, prevention and mitigation measures to face the risks related to the use of ICT to achieve a safer and reliable environment for all the country's residents.

5.2 Specific Objectives

Specific Objective 1: National Coordination

- **Coordinate with stakeholders to define their role and line of action in the process of mitigation, management, recovery and continuity in case of a cybernetic security incident.**

The coordination, collaboration and exchange of information between stakeholders is fundamental for the success of any national cybernetic security program. These interested parties include the public sector[36], the academy, non-governmental organizations, the private sector, civil society and the technical community[37].

[36] *Understood as "…the sum total of public organizations. Is integrated by the Powers of the Republic, the autonomous institutions, municipalities, state banks, public corporations and other public, non-state institutions. According to the Ministry of Economic Planning and Policies (MIDEPLAN) (2007). Explanatory handbook of the organization charts for Costa Rica's public sector. [Online]. Recovered August 16th of 2016 from, https://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/237a1427-b5f7-4b41-be16-8993ca567e32/organigrama_del_sector_publico.pdf?guest=true*

[37] *As part of the recommendations from the Organization for Economic Cooperation and Development (OECD) the technical community's participation is urged in order to avoid decision-making removed from industry standards. Example: IET, IAB, RIR's, ccTLD, RO's, ICANN, ISOC and W3C."The Internet technical community underlines its role as a source of independent advice regarding the potential intended and unintended consequences of planned policy decisions on the Internet and the way it functions, and stresses that policy-makers*

MICITT as National Coordinator shall supervise the efficacy and efficiency of the lines of action for implementation and recommend, in consultation with relevant stakeholders, about the measures to optimize the policies and procedures of cybernetic security in Costa Rica.

The above includes establishment of clear policies to define, regulate and promote the exchange of information among the various entities interested and work groups in each of the sectors, creating an environment of trust and strengthening existing lines of communication.

Dialogue and cooperation between the private sector and the State are essential requirements to achieve the strategy's objectives; therefore, exchange of information shall be promoted, supported by confidentiality agreements to create the necessary trust during the effective and timely treatment of incidents.

In addition, the State reserves the faculty of creating ad-hoc commissions as a mechanism for the study, analysis and recommendation in specific themes of cybernetic security. The sectors' representation and the conformation of these commissions shall be determined by the specific subject and the pertinent or affected sectors.

Strategic Line 1.1. National Coordinator

- Designate a national coordinator having the responsibility to articulate the actions in cybernetic security matters and giving follow-up to compliance to this strategy. The national coordination figure befalls on MICITT; it shall be the focal point at national and international level for any topic related to cybernetic security.

Strategic Line 1.2. Collaboration of the Public and Private Sectors

- Sustain the cordial and fluid dialogue with the private sector to develop initiatives so as to attract national attention to cybernetic security and involve an ample representation of the parties implied.

should seek such advice as early as possible in the policy development process in order to avoid pursuing technologically flawed decisions." Organization for Economic Cooperation and Development (OECD). (2012). Cybersecurity policy making at a turning point. [Online]. Available at: https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Specific Objective 2: Public Awareness

- **Develop and/or implement awareness and education campaigns on cybernetic security that foster responsibility for digital protection as a duty of all users of digital technologies.**

Measures should be taken for awareness regarding cybernetic security, among citizens, public officers and companies, to ensure they are well informed and educated about the existing risks. Cybernetic security is one of the most important economic and national challenges; it has an impact on all social actors. Educating our citizens is a fundamental step towards strong cybernetic resilience as a Nation, acknowledging many Costa Ricans use the security tools available on the open market (for example, antivirus and firewalls) and are responsible for their personal informatics systems security measures. Citizens also use computers and other mobile terminals at their work places and have access to sensible data which should be protected.

Strategic Line 2.1. Consciousness - General Public

- Develop awareness campaigns in cybersecurity for Costa Rica's residents so they get used to and accept good practices as part of their culture, regarding the strengthening of actions for the protection of vulnerable population groups as childhood and adolescents, elder adults, indigenous population, disabled population. Everything in alliance with the private sector, civil society and non-governmental organizations dedicated to the protection of childhood and adolescents.

Strategic Line 2.2. Public Sector

- Develop awareness and education campaigns aimed at public officers and focused on the type of institution where they work, emphasizing on better protection practices and safeguarding access details to information systems and sensitive or personal data contained in those systems.

Strategic Line 2.3. Micro, Small and Medium-sized Business

- Develop dialogues and fora for the exchange of information on cybernetic security topics; specifically for Micro, Small and Medium-sized companies.

Specific Objective 3. Development of National Capacity in Cybernetic Security

- **Carry out training campaigns exclusively for the public sector having the education of final users in cybernetic security concepts and good practices as objective and preparing expert users (developers, administrators, directives) in cybernetic security techniques.**

Many organizations have not been able to address cybernetic security comprehensively, either because the information security function has not been assigned to a specific person or unit, have not adequately addressed the need of including it in their commercial operations or simply don't have the resources necessary to assign it.

A comprehensive part of the strategy shall be the implementation of measures destined to literacy, awareness and training of human resources in themes of cybernetic security. The level of competence is highly important for all personnel with public institutions, especially administrators and those responsible of decision-making, since attacks are often done under the social engineering modality aimed at strategic employees or functionaries to have access to their protected information systems.

The main purpose of a cybernetic security culture is the protection of informatics systems and the adoption of good cybernetic practices by these users.

Strategic Line 3.1. Training of Specialized Human Resources

- Foster the dissemination and promotion of specialization or training opportunities in cybernetic security available locally or internationally to functionaries of the public sector.
- Propose and impulse adjustments in the academic offer that allow developing study plans in cybernetic security or add cybersecurity modules to pertinent pre-graduate, post-graduate and doctorate programs.
- Promote the inclusion of the cybersecurity topic in at least one course of non-technological careers.

Strategic Line 3.2. Research and Development

- Form alliances with public and private universities to develop research projects on the emerging threats and the development of innovative solutions to cybernetic incidents.

Specific Objective 4. Strengthening of Legal Framework in Cybersecurity and ICT

- **Conduct a review of the existing legal framework and propose the necessary adjustments to carry out legal proceedings and institutional arrangements which guarantee an adequate investigation and effective prosecution.**

Informatics crime evolves as fast as technology which means legal provisions should be reviewed and adapted permanently, to take into account new types and methodologies used by criminals when committing informatics crimes.

A national dialogue about the international cooperation agreements is necessary as relates to cybernetic security, with the purpose of creating greater conscience of the need to facilitate an unobstructed process for the application of valid norms, given the quick rhythm of development and change of ICT.

Costa Rica's legal framework shall take into account the cross-border nature of cyberspace; the need that those responsible for enforcing the law can effectively investigate cybernetic crimes (considering the speed and transitory nature of digital data), the need that incidents' response teams be able to detect an incident timely, and dote the corresponding entities with the necessary authority to dissuade identified threats

Strategic Line 4.1. Strengthening the normative and procedural framework in cybercrime

- Create a specialized commission for the review of valid existing regulations to guarantee there are adequate procedural tools in cybernetic crime matters.

Strategic Line 4.2. Create capacities in Cybersecurity for the application of the law in the criminal justice system

- Identify key areas of the criminal justice system which require strengthening their capacities and knowledge in Cybersecurity matters.
- Collaborate in the generation of capacities for identified key areas.

Strategic Line 4.3. Foster networks of trust for the exchange of information between stakeholders of the criminal justice system

- Create networks of trust supported by a non-disclosure legal instrument for the safe exchange of relevant information linked to cybernetic crimes.
- Design expedited procedures for the exchange of confidential information.

Specific Objective 5: Protection of Critical Infrastructures

- **Promote mechanisms for identification and protection of critical infrastructures, as well as for creation specific public policies, as essential step to prevent and/or mitigate cybernetic security incidents aimed at a damaging o discontinuing sensitive operations.**

By critical infrastructures is understood the group of facilities, systems, equipment, networks, data and services whose interruption or destruction would have a high negative impact on a country's basic services, seriously affecting the social and economic welfare of all inhabitants. The chain of supply of goods and services supporting the operation of critical infrastructures is a risk to be assessed taking account of the security measures implemented by these suppliers.

In view of the foregoing, this objective is seeking to define a series of activities to ensure the continuity, functionality and integrity of critical infrastructures; with the aim of preventing, managing, mitigating and/or restoring its functions before an eventual cybernetic attack.

It is crucial that critical infrastructures operators employ specific security frameworks to manage the evolution of security risks in the acquisition of ICT goods and services. For example, the outsourcing of network operations may increase the risks if suppliers of those services are not willing to agree on a minimum standard of provision, including acceptable response time and application of minimum-security measures.

As part of the process to safeguard the critical infrastructure, use of the Industrial Systems Control (SCI), Supervisory Control and Data Acquisition Systems (SCADA) should be specifically examined. Industrial systems are now designed with more connection capacity; therefore, they imply a greater threat to cybersecurity. It is crucial that regulatory entities of classified sectors such as the critical infrastructure assume a more significant role and start defining and dictating clear guidelines on cybernetic security and so that regulated entities comply with the existing regulations, standards and good practices of their particular sector as well as those nationally binding.

The implementation of guidelines and greater cooperation among the critical infrastructures operators, ICT services suppliers, systems suppliers and the State is vital.

Any infringement of security having a significant impact on the services supplier's operation should be mitigated; SCI and SCADA operators shall thus be encouraged to implement security policies which establish the approach of identified risks and possible vulnerabilities.

Some norms shall be considered in the construction of resilience in this sector; for example, the ISO 27001 and ISO 27002 norms shall be included; NERC CIP-002-3 through CIP-009-3[38], Special Publication NIST 800-82 and the Framework for Improving the Critical infrastructure Cybernetic Security[39], among others.

Strategic Line 5.1 Identification and Classification of Critical Infrastructures

- Identify the country's critical infrastructures as essential step for the application of security measures.
- Create a commission to create public policy comprised by a representative and a substitute from each one of the public institutions and private entities identified, with the purpose of ensuring the operating conditions and ongoing stability of these services.

Strategic Line 5.2. Implementation of security measures on the Public Administration's Information and Telecommunications Systems

- Design cybersecurity protocols for the executive Power's Ministries, consistent with the maturity of each of the institutions and the public sector's current needs.

MICITT's Computer Security Incident Response Team (CSIRT-CR) shall be in charge of collaborating and advising on the design of such instruments.

[38] *North American Electric Reliability Corporation (NERC). CIP Standards. [Online]. Recovered August 27th of 2015 from, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx*

[39] *National Institute of Standards and Technology (2014). Framework for Improving Critical Infrastructure Cybersecurity. [Online]. Recovered August 27th of 2015 from, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (updated December 5 2014).*

Specific Objective 6: Risk Management

- **Promote the implementation of a risk management model adapted to the own needs of each institution or organization.**

At managerial level of any organization, the adoption of a risk management process is basic for the review of important risks related to information technologies, which could occur regularly, and which would provide a consistent approach in the appropriation of this operation. Many entities have problems and deficiencies in that area; consequently there is no evaluation, measurement, nor adequate communication of the extent in which their operations are being affected by cybernetic attacks; nor the operations forwarded to build their cybernetic resilience. This understanding is essential to be able to effectively approach cybernetic risk.

An effective cybernetic security regime adopts or develops a framework with a continuous cycle of risk evaluation activity, risk control, development of general security policies, business continuity guarantee, allocation of responsibilities, promotion de awareness and follow-up of the effectiveness of controls implemented. Business Continuity planning is a proactive measure ensuring that in case of emergencies, system failures or disasters, it is possible to recover and keep up the normal business functions in case some serious risk occurs. Uncertainty is a central theme on Information Technologies Risks and consequently the implementation of the best management practices is required. [40]

Thus, the Software Engineering Institute Risk Management Model (SEI), the Federal Information Security Management (FISMA) Risk Management Framework and the ISO/IEC INTE 27000 norms, shall be taken in consideration, among others.

Strategic Line 6.1 Improve the security of products and services associated to information security.

- Promote the implementation of security norms for the operation of public and private organizations as a matter of priority, taking into account the international rules such as

[40] *Tripton, H. y Krause, M. (2004). Handbook of Information Security Management. USA: CRC Press. Available: http://index-of.co.uk/Computer-Security/CRC%20Press%20-%20Information%20Security%20Management%20Handbook,%20Fifth%20.pdf*

as NIST, INTE/ISO/IEC, COBIT, recommendations of the Organization for the Economic Cooperation and Development (OECD) and the International de Telecommunications Union (ITU).

- Set up negotiations with certifying authorities so certification of institutions and organizations interested is enabled.

Strategic Line 6.2. Implementation of Better Practices and Definition of Minimum Information Security Requirements in the Financing Sector

- Coordinate with the financial sector's regulating body to create a specific security framework for the entities of this type, taking into account the different levels of maturity and size of each organization of the sector.
- Create a permanent communication mechanism with the different institutions conforming the financial system to analyze the opportunities for improvement and challenges in the strengthening of cybersecurity.

Strategic Line 6.3. Adoption of reference security measures

- Promote the incorporation of appropriate security and privacy measures and property of data, for those services provided to citizens, favoring the use of authentication digital certificates and emphasis on the implementation of high standards for protection of data storage services such as cloud computing.

Strategic Line 6.4. Establishment of an information Exchange Network for government entities

- Facilitate and promote exchange of information between the responsible of government information security through a network of trust, where high levels of confidentiality and professionalism are applied. The attacks and events usually affect multiple organizations. Adequate communication and coordination could decrease risks and minimize the possible impact.
- Develop a legal instrument to establish the outreach and conditions of network participants.

Strategic Line 6.5. Strengthening of the Computer Security Incident Response Team CSIRT-CR

- Strengthen and improve resilience against informatics disturbance and incidents.
- Assign exclusive resources to address all CSIRT- CR components.

- Promote and endorse the creation of sectorial CSIRT coordinating with National CSIRT so as to provide specific solutions for each sector and thus contribute to a quicker, more effective recovery facing its incidents.

Specific Objective 7: International Cooperation and Commitment

- **Participate from international cooperation through mutual assistance and collaboration in criminal, technical and training matters and the development of security measures to approach issues related to cybersecurity matters.**

Internet is a global tool for collaboration and development; therefore, establishing collaboration and cooperation bonds in these matters to contribute to growth and development of national cybersecurity capacities.

Incorporation of the country to bilateral and multilateral efforts, deployed by various States and international organizations shall be promoted, to work in the cybernetic security field. World dialogue on cyberspace shall shape our future as Nation and enable State efforts to contribute in this discussion.

Strategic Line 7.1. Involvement of the international community in support of the National Strategy’s objectives

- Foster participation in specialized for a at national and international level with the purpose of strengthening cooperation in cybersecurity with other allies.
- Administer national e international cooperation to allow strengthening of essential cybersecurity resources and infrastructure of the country through de internships, trainings, workshops, among others.

Specific Objective 8: Implementation, Follow-up and Evaluation

- **Design and apply a methodology of implementation and follow-up to evaluate the fulfillment of the lines of action and propose required adjustments.**

Internet is a rapidly changing ecosystem; therefore, mechanisms to keep up to date with changes and close the gaps that could occur as a consequence of changes and the new risks, should be applied as soon as possible.

Deficiencies in cybernetic security often result from inadequate allocation of human and financial resources. The country has many capacities to effectively approach the cybernetic security issues, but the definition of responsibility and assignment of efficient resources is required.

The concept of a risk-based approach ensures the cybernetic security resilience construction process is interactive and follow-up may be done.

Thus, to measure the progress and success of this strategy, MICITT shall be entitled to request reports from the different actors, about the advance of the tasks assigned. Consequently, as National Coordinator it will evaluate the advance of the activities, propose recommendations and inform the President of the Republic and the Governing Board annually on the strategy's implementation advances.

Strategic Line 8.1. Monitor the application of the National Cybersecurity Strategy, and assess the degree of success in the fulfillment of its objectives

- Design the methodology for the systematic monitoring of the actions operating the National Cybersecurity Strategy.
- Specify the control mechanisms in the action plan to track the advances and efficacy of the objectives proposed in the present strategy

Strategic Line 8.2. Conduct a review and update of the National Cybersecurity Strategy every two years or as necessary.

- The Advisory Board shall be responsible of analyzing the strategy and issue reports, including duly justified recommendations to carry out the required modifications.

Chapter 8 –Final Reflections

Costa Rica shall initiate the establishment of a solid base for the next generations by delimiting the areas of interest for the application of the National Cybersecurity Strategy.

Investment in ICT solutions shall not only continue improving the quality of life of inhabitants, but also significantly transform the way we see the world and how we interact.

Through the systematic application of lines of action, it is intended Costa Rica continue to be a leader in the area of ICT research and development, also a source of qualified human resources in the field of cybernetic security and information.

From a national perspective, cybernetic security can only be implemented from an approach with multiple phases and perspectives. This shall ensure the key areas necessary are developed simultaneously for national cybernetic resilience.

Acknowledging the fact that an informatics threat is not a future development but a current reality, Costa Rica shall destine the necessary government resources to ensure success of this strategy and make alliances with all stakeholders to advance in its objectives and goals. The Executive Power shall promote a cybersecurity culture at the public sector level with the aim the budgetary assignment in this area is established.

Glossary

Term	Definition
Academy	Official institution constituted by distinguished persons of humanities, arts or science who collectively carry out certain activities.
Cybernetic Threat	Action in or through an information system that may result in a non-authorized effort negatively affecting the security, confidentiality, integrity or availability of a system or information transiting on it or stored or processed.
Cybernetic Attack	Action whose purpose is interrupting, deactivating, destroying or maliciously controlling an informatics environment/infrastructure; or destroying data integrity de or controlled theft of information. Synonym of cyber-attack.
Digital Breach	The separation existing between people (communities, states, countries…) using Information and Communication Technologies (ICT) as a routine part of their daily life and those who do not have access to the same and those, who although having them do not know how to use them.
Cybercrime	Group of persons and organizations committing crimes through the Internet or some computer network.
Cyberspace	Complex environment resulting from the interaction of people, software and internet services by means of technological devices and networks connected to this, not existing physically.
Cybersecurity	Group of instruments, policies, concepts of security, security safeguards, guidelines, risk management methods, actions, training, best practices, insurance and technologies which may be used to protect assets of the organization and users of cyberspace.
Cloud Computing	According to ITU, cloud computing is a model which allows offering users ubiquitous, practical usage, on demand, through a network to a shared group of

	of configurable informatics resources: networks: servers, storage, applications and services supplied rapidly and released with a minimum management labor or a minimum interaction with the supplier of the service.
Organized Crime	Is that group of three or more persons which was not formed randomly; which has existed for some time; acting premeditatedly with the purpose of committing a punishable crime; with the purpose of obtaining, directly or indirectly a financial or material benefit.
Cybersecurity Crisis	An extraordinary event deferring from the normal and consisting of a serious perturbation or risk of perturbation of society's vital functions and who have the participation of information and communication technologies.
Cyber Resilience	The ability to prepare for, adapt, endure, and quickly recover from interruptions resulting from deliberate attacks, threats or accidental incidents or occurring naturally.
Deep Web	The part of the World Wide Web (www), which is not indexed or catalogued by means of standard search engines (as google.com) and includes dynamic pages or protected by a password and encrypted networks.
Hacking	Intentional access to a computer system without the authorization of its user or owner.
Hacker	Person interested in understanding in an advanced way the internal functioning of a system, computers, and computer networks in particular.
Ethical Hacker	An ethical hacker (certified) is a professional with abilities who understands and knows how to seek for weaknesses and vulnerabilities of systems' objectives and uses the same knowledge as a malicious hacker, but in a legitimate and legal way to evaluate the security posture of a system(s) objective(s).
Hacktivism	Use of computer technologies to achieve a political agenda by ambiguously legal means and generally

	obstructing computer activity somehow, and not causing damage or significant monetary loss.
Cybernetic Security Incident	Action through the use of computer networks which has the result of a real or potentially adverse effect in an information system and/or la information existing in one.
Critical Information Infrastructure	IT Systems supporting key goods and services of the national infrastructure, when an occurring incident causes or may cause serious damage to national security, national economy or social well-being.
Critical Infrastructures	Information systems and networks that should they fail could have a serious impact on health, physical and operational safety, the economy and well-being of citizens, or the effective functioning of the government and the economy of the country.
Information Exchange	Open and reliable exchange of data, ideas and contents among different actors and technologies.
Digital Evidence	Electronic Information stored or transferred digitally
Internet exchange point	An internet exchange point (IXP or IX) is a physical infrastructure through which suppliers of Internet services (ISP) and content distribution networks (CDN) exchange local traffic of Internet among their networks.
Cybernetic Resilience	Ability to prepare for, adapt, endure and, and rapidly recover from interruptions resulting from deliberate attacks, threats or accidental incidents or those occurring naturally. Synonym or equivalent to cyber resilience. REPETIDA en el original
Private Sector	That part of the economy not controlled by the State, and is directed by individuals and profit-seeking corporations.

Public Security	Group of public organizations. Integrated by the Powers of the Republic, autonomous institutions, municipalities, State Banks, the public companies and other public, non-state institutions.
Cybernetic Security	Conservation, through policies, technology and education, Of the availability, confidentiality and integrity of the information and subjacent infrastructure so as to preserve people’s safety, online as off the line. Considered analogous or synonym of cybersecurity and digital security.
Digital Security	Term recommended by OECD in its document OECD Perspectives on digital economy, 2015. Considered analogous or synonym of cybersecurity and cybernetic security.
Information Security	The protection of information and information systems from the access, use, dissemination, alteration, modification or non-authorized destruction, with the purpose of guaranteeing their confidentiality, integrity and availability.
Civil Society	Group of subjects, assuming their role as citizens, develop certain actions to impinge on the public sphere.
Terrorism	Domination through the use of terror and control, searching Through the violent acts to create fear. Terrorism, therefore seeks to coerce and pressure governments or society at large to impose their claims and proclamations.

References

- Aguilera, R. (05 de enero de 2014). The World Post. “Costa Rica: life after Intel”. Recovered from, http://www.huffingtonpost.com/rodrigo-aguilera/costa-rica-life-after-int_b_5246788.html
- Aguilera, R. (05 de enero de 2014). The World Post. “Costa Rica: life after Intel”. Recovered from, http://www.huffingtonpost.com/rodrigo-aguilera/costa-rica-life-after-int_b_5246788.html
- Artículo 59. Ley de la Autoridad Reguladora de los Servicios Públicos (ARESEP), Ley N° 7593. Diario Oficial La Gaceta de la República de Costa Rica, 05 de setiembre de 1996. Available at: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=26314&nValor3=80920&strTipM=TC ´
- Asamblea General de las Naciones Unidas. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Consejo de Derechos Humanos, Decimoséptima sesión Punto 3 del orden del día. UN. Recovered 21 de agosto de 2015 de, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
- Asamblea General de las Naciones Unidas. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Consejo de Derechos Humanos, Decimoséptima sesión Punto 3 del orden del día. UN. Recovered 21 de agosto de 2015 de, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
- Bermúdez, M. (24 de agosto de 2015). Gobierno CR. “Costa Rica se potencia como un país exportador de tecnología”. Recovered from, http://gobierno.cr/costa-rica-se-potencia-como-un-pais-exportador-de-tecnologia/http://gobierno.cr/costa-rica-se-potencia-como-un-pais-exportador-de-tecnologia/
- Bermúdez, M. (24 de agosto de 2015). Gobierno CR. “Costa Rica se potencia como un país exportador de tecnología”. Recovered from, http://gobierno.cr/costa-rica-se-potencia-como-un-pais-exportador-de-tecnologia/http://gobierno.cr/costa-rica-se-potencia-como-un-pais-exportador-de-tecnologia/
- BID-OEA. (2016). Informe Ciberseguridad 2016. Banco Interamericano de Desarrollo.
- Chief Judge Stein Schjølberg (2008). REPORT OF THE CHAIRMAN OF HLEG. Norway: ITU. Recovered August 01 of 2016 from, https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf
- Chief Judge Stein Schjølberg (2008). Report of the Chairman of HLEG. Norway: ITU. Recovered August 01 of 2016 from, https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf
- Chief Judge Stein Schjølberg (2008). Report of the Chairman of HLEG. Norway: ITU. Recovered August 01 of 2016 from, https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

- Coalición Costarricense de Iniciativas de Desarrollo (CINDE) (2016). Invirtiendo en Costa Rica: Servicios. Costa Rica. CINDE: Costa Rica. Basado en datos del Banco Central de Costa Rica, del Fondo Monetario Internacional y Trademark.
- CONICIT-Fundación Paniamor-MICITT. Web site Crianza Tecnológica. [Online]. Available at: http://crianzatecnologica.paniamordigital.org/index.html
- CONICIT-Fundación Paniamor-MICITT. Web site Crianza Tecnológica. [Online]. Available at: http://crianzatecnologica.paniamordigital.org/index.htm l
- Contraloría General de la República (CGR). (2009). Normas Técnicas en Tecnologías de Información y Comunicaciones. San José: CGR. Recovered from, https://cgrfiles.cgr.go.cr/publico/jaguar/Documentos/cgr/Sistemas/Normas_Tecnicas/Informe%20NTI_doc.pdf
- Contraloría General de la República (CGR). (2009). NTP3: Evaluación de Risks de Tecnologías de Información. San José: CGR. Recovered from, https://cgrfiles.cgr.go.cr/publico/jaguar/Documentos/cgr/Sistemas/Normas_Tecnicas/Informe%20NTI_A_3.pdf
- Contraloría General de la República (CGR). (2012). R-DC-120-2012: Marco General para la Gestión de la Calidad en TIC. San José: CGR. Recovered from, http://cgrw01.cgr.go.cr/pls/portal/docs/PAGE/PORTAL_FUNCIONARIOS_2008/SECCIONES%20FUNCIONARIOS/DOCUMENTOS/TECNOLOGIA/R-DC-120-2012%20GESTION%20CALIDAD.PDF
- Creación de la Comisión nacional de seguridad en línea, Decreto N° 36274. Diario Oficial La Gaceta de la República de Costa Rica, 09 de diciembre de 2010. Available at: http://www.pgrweb.go.cr/TextoCompleto/NORMAS/1/VIGENTE/D/2010-2019/2010-2014/2010/10E77/69239_83075-1.html
- Creación de la Comisión nacional de seguridad online, Decreto N° 36274. Diario Oficial La Gaceta de la República de Costa Rica, 09 de diciembre de 2010. Available at: http://www.pgrweb.go.cr/TextoCompleto/NORMAS/1/VIGENTE/D/2010-2019/2010-2014/2010/10E77/69239_83075-1.html
- Creación del Centro de Respuesta de Incidentes de Seguridad Informática CSIRT-CR-CR, Decreto N° Nº 37052-MICIT. Diario Oficial La Gaceta de la República de Costa Rica, 09 de marzo de 2012. Available at: http://www.gaceta.go.cr/pub/2012/04/13/COMP_13_04_2012.html#_Toc321989832
- Creación del Centro de Respuesta de Incidentes de Seguridad Informática CSIRT-CR-CR, Decreto N° Nº 37052-MICIT, Crea Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR-CR. Diario Oficial La Gaceta de la República de Costa Rica, 09 de marzo de 2012. Available at: http://www.gaceta.go.cr/pub/2012/04/13/COMP_13_04_2012.html#_Toc321989832
- Decreto ejecutivo DE 35.205 16-04-2009 Reglamento Protección Privacidad de Comunicaciones y el Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones, de la ARESEP Reglamento 010 de 18 de marzo de 2010.

- Decreto No. 7425. Diario Oficial La Gaceta de la República de Costa Rica, 09 de agosto de 1994. Available at en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=16466&nValor3=17615&param2=1&strTipM=TC&lResultado=3&strSim=simp
- Deibert, R. (s.f.). Towards a cyber security strategy for global civil society? [En línea]. http://www.giswatch.org/sites/default/files/gisw_-_towards_a_cyber_security_strategy.pdf
- Foro Económico Mundial (FEM). (2014). Informe de Competitividad Global 2014-2015. Ginebra: FEM. Recovered August 19 of 2015 from, http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2014-15.pdf

- Foro Económico Mundial (FEM). (2014). Informe de Competitividad Global 2014-2015. Ginebra: FEM. Recovered August 19 of 2015 from, http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2014-15.pdf

- Fundación Karisma (traductor). (2013). Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Available at: https://karisma.org.co/wp-content/uploads/2014/03/13Principios_es.pdf

- Fundación Karisma (traductor). (2013). Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Available at: https://karisma.org.co/wp-content/uploads/2014/03/13Principios_es.pdf

- Green, N. y Rosinni, C. Cyber Security and Human Rights. USA: Public Knowledge. Available at: https://www.gccs2015.com/sites/default/files/documents/Introduction%20Document%20for%20GCCS2015%20Webinar%20Series%20-%20Cybersecurity%20and%20Human%20Rights%20(1).pdf
- GSMA. (20 de mayo de 2012). Mobile Phone Theft in Latin-America: The example of Costa Rica and the need of coordination among operators. Web site. [Online]. Available at: http://www.gsma.com/latinamerica/mobile-phone-theft-in-latin-america/

- GSMA. (20 de mayo de 2012). Mobile Phone Theft in Latin-America: The example of Costa Rica and the need of coordination among operators. Web site. [Online]. Available at: http://www.gsma.com/latinamerica/mobile-phone-theft-in-latin-america/

- http://www.hacienda.go.cr/cifh/sidovih/spaw2/uploads/images/file/Normas%20t%C3%A9c%20en%20TI%20y%20comunics.pdf
- INTERPOL. (30 de enero de 2015). Capacidad policial de Costa Rica impulsada con nueva tecnología de la INTERPOL. [Online]. Web site. Recovered September 14 of 2015 from, http://www.interpol.int/News-and-media/News/2015/N2015-008
- Kovacs, A. y Hawtin, D. (2013). Un enfoque de derechos humanos para la seguridad cibernética. [Online]. Available at: http://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security- Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf
- Ley de Delitos Informáticos y Conexos, Ley N° 9048. Diario Oficial La Gaceta de la República de Costa Rica, 06 de noviembre de 2012. Available at:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=101586&param2=1&strTipM=TC&lResultado=1&strSim=simp

- Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones
- MICITT. Boletín Contacto Digital. IXP Costa Rica: Una oportunidad estratégica. MICITT: Departamento de Sociedad de la Información. Recovered March 2nd of 2017 from, http://www.micit.go.cr/index.php?option=com_content&view=article&id=6329&catid=59&Itemid=1574
- Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). Op. Cit. PNDT. [Online]
- Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). (2014). Indicadores Nacionales de Ciencia, Tecnología e Innovación. San Jos: MICITT.
- Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2015). Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021. Recovered August 17 of 2016 from, http://micit.go.cr/images/Telecomunicaciones/pndt/PNDT-2015-2021.pdf
- Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2015). Plan Nacional de Ciencia, Tecnología e Innovación 2015-2021. San José: MICITT. Recovered from, http://pncti.micit.go.cr/
- Ministerio de Planificación Nacional y Política Económica (MIDEPLAN). (2013). Costa Rica 2030: Plan Nacional de Desarrollo. San José: MIDEPLAN. P. 13. Recovered from, http://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/0311bebc-87c5-4c22-9731-21c04744f254/Costa%20Rica%202030%20web.pdf
- Ministerio de Planificación Nacional y Política Económica (MIDEPLAN). (2013). Costa Rica 2030: Plan Nacional de Desarrollo. San José: MIDEPLAN. P. 30. Recovered from, http://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/0311bebc-87c5-4c22-9731-21c04744f254/Costa%20Rica%202030%20web.pdf
- Ministerio de Planificación y Política Económica (MIDEPLAN) (2007). Manual explicativo de los organigramas del sector público costarricense. [Online]. Recovered August 16 of 2016 from, https://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/237a1427-b5f7-4b41-be16-8993ca567e32/organigrama_del_sector_publico.pdf?guest=true
- Ministerio de Planificación y Política Económica (MIDEPLAN). (2013). Plan Nacional de Desarrollo 2014-2018 "Alberto Cañas Escalante". San José: MIDEPLAN. p. 438. Recovered August 17 of 2016 from, http://documentos.mideplan.go.cr/alfresco/d/d/workspace/SpacesStore/cd1da1b4-868b-4f6f-bdf8-b2dee0525b76/PND%202015-2018%20Alberto%20Ca%C3%B1as%20Escalante%20WEB.pdf
- Ministerio de Planificación y Política Económica (MIDEPLAN). Op. Cit. PND. [Online]. En el Programa Gobierno Electrónico establecido en el Plan Nacional de Desarrollo se establece la meta que reza: "50% de cumplimiento Programa de Gobierno Electrónico (Una Estrategia Nacional de Ciberseguridad y 9 Ministerios con un Protocolo de Ciberseguridad implementado)"

- National Institute of Standards and Technology (2014). Framework for Improving Critical Infrastructure Cybersecurity. [Online]. Recovered August 27 of 2015 from, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (updated December 5, 2014).
- NIC CR. (14 de mayo de 2015). Web site NIC CR. "Costa Rica among the first in the world to implement Origin Validation at Internet Exchange Points (IXP)". Recovered August 24 of 2015 de, https://www.nic.cr/en/article/costa-rica-among-first-world-implement-origin-validation-internet-exchange-points-ixp
- North American Electric Reliability Corporation (NERC). CIP Standards. [Online]. Recovered August 27 of 2015 de, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- Oficio 04948-SUTEL-CS-2015 del 24 de julio de 2015
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (2012). Uso de TIC en educación en América Latina y el Caribe –Análisis regional de la integración de las TIC y de la aptitud digital (e-readiness) – Instituto de Estadística de UNESCO-. Recovered from, http://www.uis.unesco.org/Communication/Documents/ict-regional-survey-lac-2012-en.pdf
- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2012). Cybersecurity policy making at a turning point. [Online]. Available at: https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf
- Protección de childhood y la adolescents frente al contenido nocivo de Internet y otros medios electrónicos, N° 8934, Diario Oficial La Gaceta de la República de Costa Rica, 08 de setiembre de 2011. Available at en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=71024&nValor3=86030&param2=1&strTipM=TC&lResultado=2&strSim=simp
- Reforma de los artículos 196, 196 bis, 230, 293 y 295 y adición del artículo 167 bis al Código Penal, Ley N° 9135. Diario Oficial La Gaceta de la República de Costa Rica, 26 de abril de 2013. Available at en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74706&nValor3=92348&param2=1&strTipM=TC&lResultado=1&strSim=simp
- Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones, de la ARESEP Reglamento 010 publicado en Gaceta n° 72 15 de abril de 2010: https://sutel.go.cr/sites/default/files/normativas/reglamento_sobre_el_regimen_de_proteccion_al_usuario_final_de_los_servicios_de_telecomunicaciones.pdf
- Reglas de Heredia: Reglas mínimas para la Difusión de la Información Judicial en Internet, Seminario Internet y Sistema Judicial, Heredia, 09 de julio de 2003. [Online]. Available at: http://www.iijusticia.edu.ar/heredia/Heredia_Rules.htm

- Sala Constitucional de la Corte Suprema de Justicia, de Costa Rica. (2010). Sentencia N.º 2010012790. San José: Corte Suprema. Recovered from, http://200.91.68.20/pj/scij/busqueda/jurisprudencia/jur_texto_sentencia.asp?nValor2=483874&tem1=013141&param7=0&lResultado=3&nValor1=1&strTipM=T&strLib=LIB
- Secretaría Técnica de Gobierno Digital. (2011). Plan Maestro de Gobierno Digital 2011-2014. San José: Secretaría Técnica de Gobierno Digital. P. 81.
- Sitio web del Poder Judicial de la República de Costa Rica. [En línea]. Available at: http://www.poder-judicial.go.cr/
- Digital Signature web site. [Online]. Available at: http://www.firmadigital.go.cr/Leyes.html
- Sitio web Sistema Costarricense de Información Jurídica. [En línea]. Available at: http://www.pgrweb.go.cr/scij/
- SUTEL. (6 de abril de 2010), Reglamento sobre el Régimen de Protección del Usuario Final de los Servicios de Telecomunicaciones. Available at: https://sutel.go.cr/sites/default/files/normativas/reglamento_sobre_el_regimen_de_proteccion_al_usuario_final_de_los_servicios_de_telecomunicaciones.pdf
- Tripton, H. y Krause, M. (2004). Handbook of Information Security Management. USA: CRC Press. Available at: https://imcs.dvfu.ru/lib.int/docs/Networks/Security/Information%20Security%20Management%20Handbook,%20Fifth%20Edition.pdf
- Uso de TIC en educación en América Latina y el Caribe –Análisis regional de la integración de las TIC y de la aptitud digital (e-readiness) – Instituto de Estadística de UNESCO- http://www.uis.unesco.org/Communication/Documents/ict-regional-survey-lac-2012-sp.pdf
- Unión Internacional de Telecomunicaciones (ITU). (2014).Actas Finales de la Conferencia de Plenipotenciarios (Busán, 2014). Busán: UIT. Recovered August 01 of 2016 de, https://www.itu.int/en/plenipotentiary/2014/Documents/final-acts/pp14-final-acts-es.pdf
- Unión Internacional de Telecomunicaciones (UIT). (2014).Actas Finales de la Conferencia de Plenipotenciarios (Busán, 2014). Busán: UIT. Recovered August 01 of 2016 de, https://www.itu.int/en/plenipotentiary/2014/Documents/final-acts/pp14-final-acts-es.pdf
- Unión Internacional de Telecomunicaciones. (2015). Informe sobre Medición de la Sociedad de la Información 2015. Ginebra: UIT. Recovered in, https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-S.pdf