Stiftung Neue Verantwortung

Exercise Background Material

Costa Rica
Country Profile

Points of Contact: Rebecca Beigel, Julia Schuetze | Stiftung Neue Verantwortung e. V.
Beisheim Center | Berliner Freiheit 2 | 10785 Berlin

This document is exercise-specific information material and was developed for the purpose of a cybersecurity policy exercise only.

Disclaimer:

The research only represents a country's cybersecurity policy to a limited extent and is not an in-depth or complete analysis or assessment of current policy. In order to adapt the exercises to specific countries, it is important to understand the broader strokes of cybersecurity policies of other countries. Our team, therefore, researches publicly available information on cybersecurity policies of countries to adapt the exercises to country-specific needs. The research is shared with participants as background material in preparation for the exercise. Therefore, the documents have a timestamp and consider policy up until the date of publication. In the interests of non-profitability, we decided to make the background research publicly available. If you are using these materials, please include the disclaimer. Please also do not hesitate to contact us.

This background research has been made possible by the financial support of the Konrad-Adenauer-Stiftung Costa Rica.

Points of Contact:

Rebecca Beigel

Project Manager for International Cybersecurity Policy

rbeigel@stiftung-nv.de

+49 (0)30 40 36 76 98 3

Julia Schuetze

Junior Project Director for International Cybersecurity Policy

jschuetze@stiftung-nv.de

+49 (0)30 81 45 03 78 82

Research support by:

Christina Rupp

Student Assistent for International Cybersecurity Policy

crupp@stiftung-nv.de

Table of Contents

This document is exercise-specific information material and was developed for the purpose of a cybersecurity policy exercise only.

Political System and Socio-Political Background

Key Facts

- Official Country Name: Republic of Costa Rica, the capital is San José.[1]
- Population: Population of about 5.15 million people (2021).[2]
- Official language: Spanish.[3]
- Currency: Costa Rican colón.[4]

Political System

- Form of Government: Democratic presidential republic.[5]
  - Head of State and Government: Carlos Alvarado Quesada, President of the Republic of Costa Rica since May 2018, member of the Citizens' Action Party (Partido Acción Ciudadana, PAC)[1] party.[6]
    - According to Article 139 of the Costa Rican constitution, the President is mandated inter alia with the authority to appoint and remove Cabinet Ministers as well as act as commander-in-chief of the law enforcement forces.[7]
    - The Costa Rican government consists of 21 ministries.[8] The main governmental entity in Costa Rica in charge of developing, coordinating, and implementing the nation's cybersecurity policy is the Ministry of Science, Technology and Telecommunications (Ministerio de Ciencia Tecnología y Telecomunicaciones, MICITT), headed by Minister Paola Vega Castillo (more information on the MICITT to be found in section 2.3).
- Legislature: consists of a unicameral legislative assembly (Asamblea Legislativa).[9]

Since 1948, Costa Rica's constitution does not foresee the maintenance of a permanent military force. Responsible for any defensive actions are since then its civil police Public Force (Fuerza Pública de la República de Costa Rica).[10]

1 Disclaimer on translation: The Spanish names of stakeholders, organizations, and (legal) documents were translated to English for better readability. These English names are not official translations. The official Spanish names are provided right after the English version, together with the respective abbreviations.

Socio-Political Context

Many commentators describe Costa Rica as an "outpost of political and economic stability in an often-turbulent region"[11] or "development success story".[12] These assessments are often inter alia based on Costa Rica's status as a

- middle-income country,
- one of the lowest poverty rates in Latin America (10.6%, 2019[13]),
- economic growth (average of 4.13% annual GDP growth between 2000-2019[14]),
- as well as an early focus on environmental policies.[15]

Reporters Without Borders refers to Costa Rica as the Latin American country "with the best record on respecting human rights and freedom of expression [...and] remarkable exception in a region characterized by corruption, violent crime and constant violence against the media"[16], which is supported by its very high placement in the 2021 World Press Freedom Index (5th out of 180 countries).[17]

In the World Economic Forum's Global Competitiveness Report of 2019, Costa Rica's Adoption of Internet Communication Technologies (ICTs) ranks 63rd out of 141 countries.

- In 2019, around 81.2% of adults used the Internet.[18]
- The report moreover assessed a level of 97.2 mobile and 16.6 fixed broadband subscriptions per 100 people in Costa Rica.[19]
- In terms of the digital skills of its current workforce, Costa Rica ranks 33rd worldwide.[20]
- Between 2020 and 2021, the "number of internet users in Costa Rica increased by 397,000 (+ 11%)".[21]

When compared with other Latin American countries, income inequality in Costa Rica is high with a Gini index of 48.2 (2019).[22]

Since May 2021, Costa Rica has been a member of the Organisation for Economic Co-operation and Development (OECD).[23]

The COVID-19 pandemic poses socio-economic challenges to Costa Rica's past achievements. Within the year of 2020, its GDP is observed to have diminished by 4.6%, its poverty rate has risen to 13%, and by the fourth quarter of the year, its unemployment rate has increased to 20%.[24]

Vulnerability and Threat Landscape

Within the past years, Costa Rica is known to have fallen victim to multiple cyber operations and intrusions. For the first half of 2020, cybersecurity firm Fortinet reported the detection of "more than 51 million computer attacks against institutional, business and personal systems and devices [...] in Costa Rica".[25] This elevated number is connected to new intrusion vectors closely linked to the COVID 19 pandemic, such as increased remote working or reports of a ransomware app COVIDLock which has claimed to help mitigate the virus' spread via the provision of interactive maps.[26]

When taking a look at publicly known cyber incidents pre-COVID, it becomes evident that particularly financial institutions and government websites appear to constitute desired and frequently exploited targets in Costa Rica.

Cybersecurity firm Kaspersky places Costa Rica on the fifth rank in terms of the highest share of affected users by financial threats worldwide.[27] A news report moreover suggests that the Costa Rican banking system is the main Costa Rican target for cybercriminals[28]. Known cases of cyber-enabled financial theft in Costa Rica originate from both state-sponsored and non-state actors.

- In 2020, it was revealed that Costa Rican private sector entities have been among the suspected victims of an operation attributed to the Lazarus Group with ties to the North Korean regime, which has targeted ATMs by "manipulating transaction-processing software to initiate fraudulent cash-outs"[29].

- Moreover, unknown non-state perpetrators, operating via the usage of Maze ransomware, have been able to gain access into the networks of Costa Rican state-owned bank Banco BCR in 2019 and 2020, which has allowed them to steal a data set containing inter alia 11 million credit card details.[30] The first intrusion took place in August 2019. Then the Maze ransomware group did not refrain from encrypting files and devices because according to them "the possible damage was too high"[31]. In 2020, the same group accessed the BCR system again after finding that the bank had not secured their network after their first operation. In May 2020, the Maze ransomware group asserted publicly that it would not sell the user data or use their credentials to acquire money but instead would be trying to "alert people and financial institutions about the poor security"[32]. The group further threatened to publish this data set if they should not receive information about newly installed IT security features from the side of the BCR. Due to an absent response by the BCR, the Maze ransomware group then continuously published leaks of acquired data and further threatened to expose information about BCR's processing methods and network structure.[33]

- Other financial institutions of Costa Rica's financial sector have been compromised by the Silence Group in August 2019 and in January 2018[34].

Over the last years, many Costa Rican government entities also have been the target of cyber operations.

- Most recently, in April 2021, it was revealed that nearly 4,500 passwords associated with e-mail addresses of Costa Rican government agencies were among the 3 billion published credentials of the Compilation of Many Breaches (COMP) leak.[35]
- In 2018, Pakistani group Pak Monster Cyber Thunders is claimed to have been able to take down websites of inter alia the **Costa Rican Presidency** (Presidencia de la República de Costa Rica), the **Ministry of Environment and Energy** (Ministerio de Ambiente y Energía, MINAE), the **Ministry of Public Security** (Ministerio de Seguridad Pública de Costa Rica, MSP), the **Judicial Investigation Department** (Organismo de Investigación Judicial, OIJ) as well as multiple municipalities.[36] Reports suspect a political motive behind the incident and perceive it as a possible "response to the departure of the United States from the nuclear agreement"[37] (referring to the Joint Comprehensive Plan of Action), among others.

Other operations in the past have targeted and, in consequence, compromised an internal webpage of the **MINAE** in December 2015[38], the website of the **Costa Rican Ministry of Foreign Affairs** (Ministerio de Relaciones Exteriores y Culto, MREC) in March 2019[39], as well as the website of the **Costa Rican Immigration Administration** (Dirección General de Migración y Extranjería, DGME) in February 2020[40].

Costa Rica's Cybersecurity Policy

Cybersecurity Policy

According to the Global Cybersecurity Index (GCI) 2020, Costa Rica ranks 8th in the Americas region comprising 35 countries regarding its commitment to cybersecurity policy.[41] The GCI is calculated by the International Telecommunications Union (ITU) on the basis of five pillars containing, for instance, legal measures or international cooperation. Globally, Costa Rica ranks 76th out of 182 countries.[42]

Costa Rica's interests and policies in cyberspace are primarily defined by its **National Cybersecurity Strategy** (Estrategia Nacional de Ciberseguridad)[43]. The strategy was adopted in 2017 as a guiding framework for the country's activities and was developed with the support of the Organization of American States (OAS).[44] Currently, Costa Rica is in the process of evaluating and updating its National Cybersecurity Strategy.[45]

The strategy seeks to provide guidance for the country's action regarding security in the use of ICTs, foster multi-stakeholder coordination and cooperation as well as promote education, prevention, and mitigation measures with respect to the use of ICTs in order to achieve a safer and more reliable environment for its citizens.[46]

The main defined principles of the strategy and hence Costa Rica's cybersecurity policy are

1. a human-centered approach
2. respect for human rights and privacy
3. necessity for multi-stakeholder coordination and co-responsibility
4. engagement in international cooperation.

In accordance, the country's policy objectives in the area of cybersecurity are to:

- Increase national coordination via the assignment of a national coordinator (located in the MICITT), who is not only in charge of coordinating actions but also monitoring compliance in the implementation of the strategy and continued public-private collaborations[47];
- Implement public cybersecurity awareness and education campaigns among Costa Rican citizens, the public sector and public officials as well as micro, small and medium-sized companies[48];
- Advance national cybersecurity capacity-building by realizing training for the public sector to support a culture of cybersecurity, share best practices and engage in alliances with universities to foster research and development[49];
- Strengthen the legal framework for cybersecurity and ICTs by consolidating the framework applicable to cybercrime, building respective capacities for law enforcement, and promoting information exchange in the field of criminal justice[50];

- Protect critical infrastructure inter alia by identifying them, adopting a critical infrastructure classification, and promoting mechanisms as well as public policies for their protection, which also include the implementation of security measures for the information and telecommunications systems of the Public Administration[51];
- Promote risk management, e.g., by strengthening the Costa Rican Computer Security and Incident Response Team, establishing an information exchange network for government entities, and defining minimum information security requirements in the financial sector[52];
- Engage in international cooperation, e.g., through mutual assistance and collaboration in criminal, technical, and educational matters[53];
- Commit to follow up on and evaluate the strategy's implementation[54].

In addition, the Costa Rican government has published a **National Telecommunications Development Plan** (Plan Nacional de Desarrollo de las Telecomunicaciones, PNDT) for the years 2015-2021, which shall contribute to an outlined vision of Costa Rica in 2021 as a "connected society, based on a comprehensive approach on access, use, and appropriation of information and communication technologies, in a safe, responsible and productive manner".[55]

Legal Framework

In Costa Rica, the **General Telecommunications Law** (Ley General de Telecomunicaciones, No. 8642, 2008)[56] as well as the **Law for the Strengthening and Modernization of Public Entities in the Telecommunications Sector** (Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones, No. 8660, 2008)[57] constitute the country's regulatory framework with respect to the Telecommunications Sector. They inter alia designate the MICITT as a primary governing body and have established the Superintendency of Telecommunications (Superintendencia de Telecomunicaciones, SUTEL), a regulatory authority that guarantees the protection of users' rights and the universalization of services.[58]

Another regulatory law of importance to the field of cyber security and cybercrime in Costa Rica is the **Law for the Protection of the Person against the Processing of Personal Data** (Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, No. 37554, 2012)[59], which has established the Agency for the Protection of Personal Data (Agencia de Protección de Datos de los Habitantes, PRODHAB).

Costa Rica's national legal framework facilitating the prosecution and investigation of cybercrime is centered around its **National Criminal Code** (Código Penal, No. 4573) and the **Law on Intervention of Telecommunications** (Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, No. 7425, 1994)[60].

In the last decade, the country's criminal code was amended via Law No. 9048 (2012)[61] and Law No. 9135 (2013)[62], allowing for the inclusion of "new types of crime [...] including those committed through the use of computer systems and technologies"[63] and thereby "formally introduced cybercrime into the country's penal code".[64] Among others, they inter alia prohibit the "installation and dissemination of software programs and malicious code in computer, information systems and servers" (Art. 232 Código Penal) or "phishing and usurpation of Internet websites and the obtaining of confidential information of individuals and legal entities for self-profit for the profit of third parties" (Art. 233 Código Penal)[65].

Moreover, Costa Rica ratified the **Budapest Convention on Cybercrime** (Treaty No. 185) in 2017 after completion of the designated accession process.[66] The Budapest Convention is the first international treaty to pursue a common criminal policy through cooperation and adoption of legislation against cybercrime.[67] The convention inter alia mandates signing entities to adopt legislation that penalizes various forms of cybercrimes and makes investigations into cyber-related crimes possible.[68]

Cybersecurity Architecture - Selected Institutions

Various government actors work on enhancing cybersecurity in Costa Rica. Most of them are located institutionally within the purview of the Costa Rican **Ministry of Science, Technology and Telecommunications** (Ministerio de Ciencia, Technología y Telecomunicaciones, MICITT).

The **Ministry of Science, Technology and Telecommunications** (Ministerio de Ciencia, Technología y Telecomunicaciones, MICITT) constitutes the main governmental entity in Costa Rica in charge of developing, coordinating, and implementing the nation's cybersecurity policy.[69] The MICITT houses the National Cybersecurity Coordinator as well as the country's Computer Security and Incident Response Team (CSIRT-CR). Moreover, the National Cybersecurity Strategy mandated the MICITT to establish an intra-departmental and multi-sectoral Cybersecurity Advisory Board, which shall inter alia develop action plans for each of the strategy's objectives.

Costa Rica's Computer Security Incident Response Team (Centro de Respuesta de Incidentes de Seguridad Informática, CSIRT-CR) was constituted in 2012 within the MICITT as "agency in charge of coordinating everything related to matters of informatics and cybernetics security"[70]. At the time of writing of the national cybersecurity strategy, CSIRT-CR tasks were described to be mainly centered around capacity-building measures in the public sector and awareness-raising. Moreover, CSIRT-CR's establishing Decree No. 37052- MICIT[71] also mandated it with authority to set up an expert team tasked with "prevent[ing] and respond[ing] to cyber incidents against government institutions"[72]. A national Cybersecurity Incident Management Protocol was agreed upon in July 2018.[73] CSIRT-CR is composed of heads of selected national ministries and oversees the MICITT's Directorate of Digital Governance (Dirección de Gobernanza Digital).[74]

Cybercrime and technology-related investigations in Costa Rica are mainly conducted within a **Specialized Division on Cybercrime at the Judicial Investigation Department** (Sección Especializada contra el Cibercrimen en Organismo de Investigación Judicial, OIJ), which is subordinate to the country's Supreme Court of Justice (Corte Suprema de Justicia de Costa Rica). The Sección Especializada contra el Cibercrimen was established in 1997 and added by a Computer Crimes Section (Sección de Delitos Informáticos) in 2004[75]. As a whole, the division is capable of conducting investigations via means of evidence collection and methods of forensic analysis[76].

In 2010, a **National Online Security Commission** (Comisión Nacional de Seguridad en Línea, CNSL) was created by Decree No. 36274-MICIT[77] under the leadership of the MICITT. It is tasked with "designing the necessary policies for the good use of Internet and the Digital Technologies" and setting upon a National Online Safety Plan (Plan Nacional de Seguridad en Línea)[78].

The National Cybersecurity Strategy tasked the MICITT to convene a **Cybersecurity Advisory Board** (Comité Consultivo en Ciberseguridad) within three months after the strategy's publication. It is composed of representatives of MICITT, the Judiciary, SUTEL, as well as representatives of civil society, academia, and private sector.[79] The Advisory Board is mandated as the responsible entity for operationalizing Costa Rica's National Cybersecurity Strategy. Together with the MICITT's National Cybersecurity Coordinator, the Advisory Board is responsible for "arrang[ing] all actions necessary to start the process of implementation, with action plans for each one of the objectives proposed in this strategy"[80] based on a prior definition of goals, deadlines, and responsible parties. Its first meeting took place in January 2018.[81] In March 2019, MICITT and the Cybersecurity Advisory Board have launched a National Information Security Literacy Campaign (Campaña Nacional de Alfabetización en Seguridad de la Información).[82]

Following the compromise of Costa Rican government websites in May 2018 by a Pakistani group, the Costa Rican government decided to establish a **Cybersecurity Liaison Network** (Red de Enlaces de Ciberseguridad), which began its work in July 2018.[83] It was created as a mechanism to allow connecting those in charge of cybersecurity in public sector institutions and facilitates coordination in general information security but also incident-related matters. CSIRT-CR communicates periodic alerts on vulnerabilities as well as incident-related information with the network.[84] It is comprised of a group of experts from the MICITT, OIJ, the Ministry of Public Security (Ministerio de Seguridad Pública, MSP), the Directorate of Intelligence and Security (Direccion de Inteligencia y Seguridad Nacional, DIS), the Costa Rican Institute of Electricity (Instituto Costarricense de Electricidad, ICE) and the NIC Costa Rica.[85] In the past, meetings were also attended by representatives of the Institute of Municipal Development and Advisory (Instituto de Fomento y Asesoría Municipal, IFAM), the Agency for Data Protection (Agencia de Protección de datos de los Habitantes, PRODHAB) as well as the Latin America and Caribbean Network Information Centre (LACNIC).[86]

Bilateral and Multilateral Cooperation

Costa Rica is a Member State of the Organization of American States (OAS), the International Telecommunications Union (ITU), and the United Nations (UN).[87] All these international organizations deal with and discuss cybersecurity-related topics. In the past, the OAS has inter alia concluded declarations titled "Strengthening Hemispheric Cooperation to Counter Terrorism and Promote Security, Cooperation and Development in Cyberspace" (2016)[88], "Protection of Critical Infrastructure from Emerging Threats" (2015)[89]. Moreover, OAS Member States have agreed on a set of cyber-related confidence-building measures (CBM) in March 2018.[90] In the field of cybersecurity, the OAS also maintains Memoranda of Understanding with Spain (2015) and Estonia (2014).[91]

Additionally, Costa Rica took part in the recently concluded first **Open-Ended Working Group (OEWG) on Developments in the Field of ICTs in the Context of International Security** which was established in 2018 under the auspices of the UN General Assembly First Committee. In its final report[92], the OEWG confirmed the notion that international law and the UN Charter are applicable in cyberspace and that states should voluntarily identify and cooperate on confidence-building measures in their local contexts. Costa Rica's input within the sessions inter alia revolved around issues of human rights and privacy, which it considered should constitute the "focus of the group's work".[93] Costa Rica is also among the 32 Member States of the **Freedom Online Coalition** (FOC), which seeks to "coordinate [...] diplomatic efforts [of its members] and engage with civil society and the private sector to support Internet freedom [...] worldwide"[94].

In addition to the OAS, Costa Rica is regionally engaged in the **Network of e-Government of Latin America and the Caribbean** (Red de Gobierno Electrónico de América Latina y el Caribe, Red GEALC), whose primary aim constitutes the "support [for] the development of digital government public policies".[95] In the framework of Red GEALC, Costa Rica has, e.g., proposed the later adopted San José Declaration[96] (November 2020), which has incorporated the issue of cybersecurity as a line of work within the network.[97]

The CSIRT-CR is represented in the **CSIRT Americas Network** as well as the **Cybersecurity Alliance for Mutual Progress** (CAMP). CAMP serves as a network platform to enhance the level of cybersecurity of its members through sharing development experiences and trends of cybersecurity.[98]

Moreover, Costa Rica is among the nine priority countries of the EU-funded **Cyber Resilience for Development** (Cyber4Dev) project, which is inter alia aimed at increasing cyber resilience and cybersecurity policy.[99] Cyber4Dev is implemented by British, Dutch, and Estonian government agencies.[100]

In the context of its accession to the Budapest Convention, Costa Rica has additionally been designated as one of the fifteen "priority and hub countries" of the joint **GLACY+ project** of the European Union (EU) and the Council of Europe (CoE). GLACY+ seeks to "strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area".[101]

Regarding bilateral cooperation in the field of cybersecurity, Costa Rica maintains several agreements with third states:

- A **MoU for Cooperation in Cybersecurity** as a follow-up to a previously concluded Co-operation Agreement in Economic, Cultural, Technical and Scientific Cooperation was concluded with the State of **Israel** in May 2021. Among others, it shall strengthen the implementation of Costa Rica's Digital Transformation Strategy and help digitize Costa Rican public institutions.[102]
- In September 2019, Costa Rica and **Estonia** signed a **MoU on Cooperation in the field of Digital Government and the "Fourth Industrial Revolution"**. It includes inter alia the training and exchange of experiences in cybersecurity, critical infrastructure protection as well as the development of effective solutions for the digital economy and government as mutual objectives.[103]
- A **cooperation agreement with China on Economic and Technical Matters** was concluded in September 2017. Among other issues, cybersecurity is referred to as a priority area of action.[104]

Moreover, the Costa Rican Ministry of Foreign Affairs has reported of cooperative relations and exchanges in the field of cybersecurity that are entertained with governmental representatives of **Austria, Singapore** and **South Korea**.[105]

Costa Rica's CSIRT was supported by the **United Kingdom** in terms of training and advice between 2014 and 2015.[106] Moreover, personnel of Costa Rica's Specialized Division on Cybercrime at the Judicial Investigation Department have received training in the **United States of America** and **Canada** in the past.[107]

Sources

1 Central Intelligence Agency (2021): The World Factbook: Costa Rica. https://www.cia.gov/the-world-factbook/countries/costa-rica/

2 Central Intelligence Agency (2021): The World Factbook: Costa Rica. https://www.cia.gov/the-world-factbook/countries/costa-rica/

3 Central Intelligence Agency (2021): The World Factbook: Costa Rica. https://www.cia.gov/the-world-factbook/countries/costa-rica/

4 Global Exchange: The Costa Rica colon. https://www.globalexchange.es/en/currencies-of-the-world/costa-rica-colon

5 Auswärtiges Amt (2021): Costa Rica: Steckbrief. https://www.auswaertiges-amt.de/de/aussenpolitik/laender/costarica-node/costarica/224814

6 Auswärtiges Amt (2021): Costa Rica: Steckbrief. https://www.auswaertiges-amt.de/de/aussenpolitik/laender/costarica-node/costarica/224814

7 Republic of Costa Rica: Constitution of The Republic of Costa Rica. https://www.wipo.int/edocs/lexdocs/laws/en/cr/cr039en.pdf

8 Presidencia de la República de Costa Rica: El Gabinete. https://www.presidencia.go.cr/autoridades/el-gabinete/

9 Central Intelligence Agency (2021): The World Factbook: Costa Rica. https://www.cia.gov/the-world-factbook/countries/costa-rica/

10 Alejandro Zúñiga (2020): Costa Rica celebrates 72 years without an army. https://ticotimes.net/2020/11/30/costa-rica-celebrates-72-years-without-an-army

11 Congressional Research Service (2021): Costa Rica: An Overview. https://sgp.fas.org/crs/row/IF10908.pdf

12 The World Bank (2021): The World Bank in Costa Rica. https://www.worldbank.org/en/country/costarica/overview#1

13 The World Bank (2021): The World Bank in Costa Rica. https://www.worldbank.org/en/country/costarica/overview#1

14 The World Bank (2019): GDP growth (annual %) - Costa Rica. https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?end=2019&locations=CR&start=2009&view=chart

15 The World Bank (2021): The World Bank in Costa Rica. https://www.worldbank.org/en/country/costarica/overview#1

16 Reporters Without Borders: Costa Rica. https://rsf.org/en/costa-rica

17 Reporters Without Borders (2021): 2021 World Press Freedom Index. https://rsf.org/en/ranking

18 The World Bank (2020): Individuals using the Internet (% of population) - Costa Rica. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=CR

19 World Economic Forum (2019): The Global Competitiveness Report 2019. https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

20 World Economic Forum (2019): The Global Competitiveness Report 2019. https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

21 Simon Kemp (2021): Digital 2021: Costa Rica. https://datareportal.com/reports/digital-2021-costa-rica

22 Organisation for Economic Co-Operation and Development (2016): Costa Rica Policy Brief. https://www.oecd.org/policy-briefs/costa-rica-towards-a-more-inclusive-society.pdf

The World Bank (2019): Gini index (World Bank estimate) - Costa Rica. https://data.worldbank.org/indicator/SI.POV.GINI?locations=CR

23 Organisation for Economic Co-operation and Development: OECD welcomes Costa Rica as its 38th Member. https://www.oecd.org/costarica/oecd-welcomes-costa-rica-as-its-38th-member.htm

24 The World Bank (2021): The World Bank in Costa Rica. https://www.worldbank.org/en/country/costarica/overview#1

25 TCRN Staff (2020): More than 51 Million Attacks by Hackers During the Pandemic in Costa Rica. https://thecostaricanews.com/more-than-51-million-attacks-by-hackers-during-the-pandemic-in-costa-rica/

26 Anastasia Austin (2020): Latin America Under Threat of Cybercrime Amid Coronavirus. https://insightcrime.org/news/analysis/threat-cyber-crime-coronavirus/

27 Kaspersky (2020): Kaspersky Security Bulletin 2020. Statistics. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf

28 Julieta Cambronero (2020): Una cuarta parte de ciberataques al sector financiero son únicamente destructivos sin ningún beneficio económico. https://costaricamedios.cr/2020/06/04/una-cuarta-parte-de-ciberataques-al-sector-financiero-son-unicamente-destructivos-sin-ningun-beneficio-economico/

29 Council on Foreign Relations: Targeting of automated teller machines worldwide. https://microsites-live-backend.cfr.org/cyber-operations/targeting-automated-teller-machines-worldwide

30 Carnegie Endowment for International Peace (2021): Timeline of Cyber Incidents Involving Financial Institutions. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

The Tico Times (2020): BCR confirms financial information has leaked after cybercrime group claims to publish private data. https://ticotimes.net/2020/05/24/bcr-confirms-financial-information-has-leaked-after-cyber-crime-group-claims-to-publish-private-data-updated

31 Lawrence Abrams (2020): Hackers say they stole millions of credit cards from Banco BCR. https://www.bleepingcomputer.com/news/security/hackers-say-they-stole-millions-of-credit-cards-from-banco-bcr/

32 Cyble (2020): Maze Ransomware Operators Targets Banco de Costa Rica, One of the Strongest Banking Companies in Both Costa Rica and Central America. https://blog.cyble.com/2020/05/01/maze-ransomware-operators-targets-banco-de-costa-rica-one-of-the-strongest-banking-companies-in-both-costa-rica-and-central-america/

This document is exercise-specific information material and was developed for the purpose of a cybersecurity policy exercise only.

33 Cyble (2020): Maze Ransomware Operators Release the Banco De Costa Rica Data Leak Part 3. https://blog.cyble.com/2020/05/22/maze-ransomware-operators-release-the-banco-de-costa-rica-data-leak-part-3/

Cyble (2020): Maze Ransomware Operators Release the Banco de Costa Rica Data Leak Part 2. https://blog.cyble.com/2020/05/05/maze-ransomware-operators-targets-banco-de-costa-rica-for-the-second-consecutive-time/

34 Carnegie Endowment for International Peace (2021): Timeline of Cyber Incidents Involving Financial Institutions. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

35 Erick Murillo (2021): Se filtran miles de claves de correo electrónicos del Gobierno. https://www.crhoy.com/tecnologia/se-filtran-miles-de-claves-de-correos-electronicos-del-gobierno/

36 Rico (2018): Pakistani Hackers In Massive Attack On Costa Rica Government Websites. https://qcostarica.com/pakistani-hackers-in-massive-attach-on-costa-rica-government-websites/

37 Rico (2018): Pakistani Hackers In Massive Attack On Costa Rica Government Websites. https://qcostarica.com/pakistani-hackers-in-massive-attach-on-costa-rica-government-websites/

38 Cf. Jaime Lopez (2015): Costa Rica Government Website Hacked by Pro-ISIS Group. https://news.co.cr/costa-rica-government-website-hacked-by-pro-isis-group/43541/

39 Cf. RedaQted (2019): Chancellery website suffered a “cyber attack”. https://qcostarica.com/chancellery-website-suffered-a-cyber-attack/

Ministerio de Ciencia, Tecnología y Telecomunicaciones (2019): CSIRT-CR atiende alerta de incidente en Ministerio de Relaciones Exteriores. https://www.micit.go.cr/noticias/csirt-cr-atiende-alerta-incidente-ministerio-relaciones-exteriores

40 Cf. The Tico Times (2021): Immigration services impacted by cybersecurity issue. https://ticotimes.net/2021/02/04/immigration-services-impacted-by-cybersecurity-issue

41 International Telecommunication Union (2021): Global Cybersecurity Index 2020. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/

42 International Telecommunication Union (2021): Global Cybersecurity Index 2020. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/

43 MICITT (2017): Estrategia Nacional de Ciberseguridad de CostaRica. https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

44 Organization of American States (2015): OAS Supports Costa Rica in Development of a National Cyber Security Strategy. https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-063/15

45 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2020): Este lunes se llevó a cabo el III Encuentro de la Red de Enlaces de Ciberseguridad, como parte de las actividades... [Facebook Status Update]. https://www.facebook.com/micitcr/posts/3747180185292345

46 Ministerio de Planificación Nacional y Política Económica (2020): Ciberseguridad en el Sistema de Planificación Nacional. https://www.hacienda.go.cr/Sidovih/uploads/Archivos/Articulo/Ciberseguridad%20en%20el%20Sistema%20Nacional%20de%20Planificaci%C3%B3n-MIDEPLAN.pdf

47 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

48 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

49 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

50 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

51 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

52 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

53 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

54 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

55 Viceministerio de Telecomunicaciones (2015): National Telecommunications Development Plan 2015-2021.
https://www.micit.go.cr/sites/default/files/pndt_2015-2021._english_version_web_1_0.pdf

56 La Asamblea Legislativa De La República De Costa Rica: Ley General de Telecomunicaciones.
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=63431

57 La Asamblea Legislativa De La República De Costa Rica: Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones.
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=63786

58 La Asamblea Legislativa De La República De Costa Rica: Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones.
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=63786

SUTEL (2021): Visión y Misión. https://sutel.go.cr/pagina/vision-y-mision

59 La Presidenta De La República Y El Ministro De Justicia Y Paz (2012): Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales.
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74352&nValor3=106487&strTipM=TC

60 Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones (1994).
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRM&nValor1=1&nValor2=16466&strTipM=FN

61 La Asamblea Legislativa De La República De Costa Rica (2012): Law No. 9048.
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=73583

62 La Asamblea Legislativa De La República De Costa Rica (2013): Law No. 9135.
http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74706&nValor3=92348&strTipM=TC

63 Council of Europe (2020): Costa Rica.
https://www.coe.int/fr/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/costa-rica/pop_up?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=print&_101_INSTANCE_CmDb7M4RGb4Z_languageId=en_GB

64 Inter-American Development Bank (2016): Cybersecurity Are We Ready in Latin America and the Caribbean? 2016 Cybersecurity Report.
https://publications.iadb.org/publications/english/document/Cybersecurity-Are-We-Ready-in-Latin-America-and-the-Caribbean.pdf

65 Council of Europe (2020): Costa Rica.
https://www.coe.int/fr/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/costa-rica/pop_up?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=print&_101_INSTANCE_CmDb7M4RGb4Z_languageId=en_GB

66 Council of Europe (2021): Chart of signatures and ratifications of Treaty 185.
https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

Inter-American Development Bank and Organization of American States (2020): 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean.
https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean

El Presidente De La República Y El Ministro A.L. De Relaciones Exteriores Y Culto (2017): Adhesión de la República de Costa Rica al Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001).
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

67 Council of Europe (2021): Details of Treaty No. 185.
https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

68 Council of Europe (2021): Convention on Cybercrime.
https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

69 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2021): Ciberseguridad.
https://micit.go.cr/tags/ciberseguridad

70 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica.
https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

71 La Presidenta De La República Y El Ministro De Ciencia Y Tecnología (2012): N 37052-MICIT. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=72316&nValor3=88167&strTipM=TC

72 Inter-American Development Bank and Organization of American States (2020): 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean. https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean

73 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2018): Comisión de Ciberseguridad actúa y reacciona ante potenciales incidentes informáticos en el país. https://www.micit.go.cr/noticias/comision-ciberseguridad-actua-y-reacciona-potenciales-incidentes-informaticos-el-pais

74 Council of Europe (2020): Costa Rica. https://www.coe.int/fr/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/costa-rica/pop_up?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=print&_101_INSTANCE_CmDb7M4RGb4Z_languageId=en_GB

UNIDIR (2020): Costa Rica. https://unidir.org/cpp/en/states/costarica

75 Organismo de Investigación Judicial: Sección Especializada contra el Cibercrimen. https://sitiooij.poder-judicial.go.cr/index.php/oficinas/departamento-de-investigaciones-criminales/delitos-informaticos

76 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica. https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

Organismo de Investigación Judicial (2021): Cibercrimen. https://sitiooij.poder-judicial.go.cr/index.php/component/k2/itemlist/search?searchword=cibercrimen&categories=&__ncforminfo=4RGrTo1JVkmEHCjcxREZI7I5sKm1fcc26tZvrBf2P72qcgo2wXeyted3a1riV3R3styBJIGYXXJGBrK8TIitL1-IPQv9ytGWoXwHdEqfubRgFc-aSNa6DCP8iGAKkYUC

77 MICITT, Nº 36274-MICIT.

78 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica. https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

79 Ministerio de Planificación Nacional y Política Económica (2020): Ciberseguridad en el Sistema de Planificación Nacional. https://www.hacienda.go.cr/Sidovih/uploads/Archivos/Articulo/Ciberseguridad%20en%20el%20Sistema%20Nacional%20de%20Planificaci%C3%B3n-MIDEPLAN.pdf

80 Ministry of Science, Technology and Telecommunications (2017): National Cybersecurity Strategy - Costa Rica. https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

81 Ministerio de Ciencia Tecnología y Telecomunicaciones de Costa Rica (2018): MICITT es sede de primera reunión del Comité Consultivo en Ciberseguridad. https://www.micitt.go.cr/portaldos/index.php?option=com_content&view=article&id=10286:micitt-es-sede-de-primera-reunion-del-comite-consultivo-en-ciberseguridad&catid=40&Itemid=1917

82 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2019): MICITT y Comité Consultivo de Ciberseguridad lanzan Campaña en Seguridad de la Información. https://www.micit.go.cr/noticias/micitt-y-comite-consultivo-ciberseguridad-lanzan-campana-seguridad-la-informacionv

83 Johnny Castro (2018): Costa Rica crea alta comisión de seguridad informática. https://www.larepublica.net/noticia/costa-rica-crea-alta-comision-de-seguridad-informatica

Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2018): Comisión de Ciberseguridad actúa y reacciona ante potenciales incidentes informáticos en el país. https://www.micit.go.cr/noticias/comision-ciberseguridad-actua-y-reacciona-potenciales-incidentes-informaticos-el-pais

84 Erick Murillo (2021): Se filtran miles de claves de correos electrónicos del Gobierno. https://www.crhoy.com/tecnologia/se-filtran-miles-de-claves-de-correos-electronicos-del-gobierno/

85 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2018): Comisión de Ciberseguridad actúa y reacciona ante potenciales incidentes informáticos en el país. https://www.micit.go.cr/noticias/comision-ciberseguridad-actua-y-reacciona-potenciales-incidentes-informaticos-el-pais

86 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2020): Este lunes se llevó a cabo el III Encuentro de la Red de Enlaces de Ciberseguridad, como parte de las actividades... [Facebook Status Update]. https://www.facebook.com/micitcr/posts/3747180185292345

87 UNIDIR (2020): Costa Rica. https://unidir.org/cpp/en/states/costarica

88 Organisation of American States (2016): Strengthening Hemispheric Cooperation to Counter Terrorism and Promote Security, Cooperation and Development in Cyberspace. http://www.oas.org/en/sms/cicte/documents/2016/declaration/cicte%20dec%201%20declaration%20english%20cicte01037e04.pdf

89 Organisation of American States (2015): Protection of Critical Infrastructure from Emerging Threats. https://www.oas.org/en/sms/cicte/documents/sessions/2015/CICTE%20DOC%201%20DECLARATION%20CICTE00955E04.pdf

90 Organization of American States (2018): Regional Confidence-Building Measures (CBMs) To Promote Cooperation And Trust In Cyberspace. https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/Multilateral/OAS+Regional+Confidence-Building+Measures+%28CBMs%29+to+Promote+Cooperation+and+Trust+in+Cyberspace+%28Agreed+During+the+First+Meeting+of+the+Working+Group+on+Cooperation+and+Confidence-Building+Measures+in+Cyberspace%2C+Held+on+February+28+-+March+1%2C+2018%29.pdf

91 Theresa Hitchens and Nilsu Goren (2017): International Cybersecurity Information Sharing Agreements. https://www.jstor.org/stable/pdf/resrep20426.pdf?refreqid=excelsior%3Aafff0b1a0413ce710ab5b22e-5ae99fd8

92 Open-ended working groupon developments in the field of information and telecommunications in the context of international security (2021): Final Substantive Report. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

93 Digital Watch (2019): 2nd Meeting of the third substantive session of the Open-Ended Working Group (OEWG). https://dig.watch/resources/2nd-meeting-third-substantive-session-open-ended-working-group-oewg

This document is exercise-specific information material and was developed for the purpose of a cybersecurity policy exercise only.

94 Freedom Coalition (2021): Aims and Priorities. https://freedomonlinecoalition.com/about-us/

Freedom Online Coalition (2021): Members. https://freedomonlinecoalition.com/members/

95 Network of e-Government of Latin America and the Caribbean: About Red Gealc. https://www.redgealc.org/sobre-red-gealc/que-es-la-red-gealc/

96 VI Reunión Ministerial y XIV Asamblea anual de laRed de Gobierno Electrónico de América Latina y el Caribe (2020): DECLARACIÓN MINISTERIAL DE SAN JOSÉ 2020. https://www.redgealc.org/site/assets/files/12593/declaracionministerialsj2020.pdf

97 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2020): Países miembros de la Red Gealc firman la Declaración de San José que incorpora el tema de Ciberseguridad propuesto por Costa Rica. https://www.micit.go.cr/noticias/paises-miembros-la-red-gealc-firman-la-declaracion-san-jose-que-incorpora-el-tema

Network of e-Government of Latin America and the Caribbean: Cibersecurity. https://www.redgealc.org/lineas-de-trabajo/ciberseguridad/

98 Cybersecurity Alliance for Mutual Progress: About CAMP. https://www.cybersec-alliance.org/camp/about.do

Cybersecurity Alliance for Mutual Progress: Members. https://www.cybersec-alliance.org/camp/membership.do

Inter-American Development Bank and Organization of American States (2020): 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean. https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean

99 Cybil (2021): EU Cyber Resilience for Development Cyber4Dev (*GFCE Initiative). https://cybilportal.org/projects/eu-cyber-resilience-for-development-cyber4dev-gfce-initiative/

100 Global Forum on Cyber Expertise: Cyber4Dev. https://thegfce.org/initiatives/cyber4dev/

101 Council of Europe (2021): Global Action on Cybercrime Extended (GLACY)+. https://www.coe.int/en/web/cybercrime/glacyplus

102 Ministerio de Relaciones Exteriores y Culto República de Costa Rica (2021): Costa Rica e Israel firman Memorándum de Entendimiento para la Cooperación en Ciberseguridad. https://www.rree.go.cr/?sec=servicios&cat=prensa&cont=593&id=6008

103 Ministerio de Relaciones Exteriores y Culto República de Costa Rica (2019): Costa Rica y Estonia firman convenios de cooperación en temas de Gobierno Digital y La Cuarta Revolución Industrial. https://www.micit.go.cr/noticias/costa-rica-y-estonia-firman-convenios-cooperacion-temas-gobierno-digital-y-la-cuarta

104 Ministerio de Relaciones Exteriores y Culto República de Costa Rica (2017): Costa Rica recibe al Canciller de la República Popular de China y firma convenio de cooperación económica y técnica. https://www.rree.go.cr/?sec=servicios&cat=prensa&cont=593&id=3641

105 Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (2019): MICITT fortalece alianza con Corea en temas de Ciberseguridad.
https://www.micit.go.cr/noticias/micitt-fortalece-alianza-corea-temas-ciberseguridad

Ministerio de Relaciones Exteriores y Culto República de Costa Rica (2021): Costa Rica y Austria sostienen diálogo sobre ciberseguridad.
https://www.rree.go.cr/?sec=servicios&cat=prensa&cont=593&id=5973

Ministerio de Relaciones Exteriores y Culto República de Costa Rica (2021): Smart Nation: Strategies, Opportunities and Cybersecurity Management.
https://www.rree.go.cr/index.php?sec=servicios&cat=becas&cont=579&beca=4613

106 Cybil (2015): Support to Costa Rica's CSIRT. https://cybilportal.org/projects/support-to-costa-ricas-csirt/

107 International Telecommunication Union (2015): Cyberwellness Profile Republic of Costa Rica.
https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Costa_Rica.pdf