MINISTERIO DE CIENCIA,
INNOVACIÓN, TECNOLOGÍA
Y TELECOMUNICACIONES

GOBIERNO
DE COSTA RICA

COSTA RICAN NATIONAL CYBERSECURITY STRATEGY 2023 - 2027

003.5
Teoría de la comunicación y el control
Cibernética

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

Estrategia Nacional de Ciberseguridad, Costa Rica 2023-2027. -San José, C.R.: MICITT, 2023.

ISBN: 978-9968-732-90-1.

1. SOCIEDAD Y CIENCIAS SOCIALES. 2. POLÍTICA Y GOBIERNO
3. GOBIERNO CENTRAL. 4. POLÍTICAS DEL GOBIERNO CENTRAL.

Dear Costa Ricans,

I am honored to share with Costa Rica the vision and mission of the new National Cybersecurity Strategy 2023-2027. This strategy marks an important milestone in protecting our nation in the digital sphere, strengthening cybersecurity, and building a safer country for all people.

In recent years, Costa Rica has experienced a significant increase in cyberattacks which have had an impact on the digital economy and national security. In response to these constantly evolving threats, the Government of the Republic has chosen to rethink its approach to care through a robust and effective National Cybersecurity Strategy.

The new National Cybersecurity Strategy 2023-2027 is focused on the entire society, with special emphasis on risk management and mitigation, and a high focus on Human Rights and centered on the human being. Key and fundamental aspects that will guide our actions.

Our vision is clear: By 2027, Costa Rica's digital ecosystem will be reliable and contribute to the global effort to secure cyberspace. We want to be an example in the region, demonstrating that we can create a robust cybersecurity culture that enhances all sectors of society.

Our mission is to establish a comprehensive action framework that allows us to prevent and mitigate risks and threats in the digital environment, promote innovation and the development of cybersecurity solutions, strengthen the response capacity to cybersecurity incidents, and promote a solid security culture. and protect personal and critical information of the State and citizens.

The National Cybersecurity Strategy 2023-2027 will focus on guiding principles, pillars, work objectives and lines of action; that will guide our actions and help us achieve our objectives; which are focused on strengthening national cybersecurity governance, adapting the cyber legal framework, strengthening infrastructure protection and national cyber resilience, strengthening the capabilities of the cybersecurity ecosystem, and cooperating in the digital environment.

Cybersecurity is essential in the digital age and is a fundamental pillar to guarantee national security. We are committed to protecting the citizens, economy, and stability of our country. Together, working in collaboration with all sectors, we can successfully confront cyber threats and ensure a secure digital future for Costa Rica.

Paula Bogantes Zamora
Minister of Science, Innovation, Technology and Telecommunications

GOVERNMENT OF THE REPUBLIC OF COSTA RICA

Rodrigo Chaves
President

Paula Bogantes
Minister of Science, Innovation, Technology and
Telecommunications -MICITT-

Gezer Molina
Director of Cybersecurity of the Ministry of Science,
Innovation, Technology and Telecommunications
-MICITT-

Margarita Vargas Ramos
Antonette Williams Barnett
Michelle Dayanna Mejía García
Raquel Cantillo Gamboa
Alejandro Obando Porras
MICITT Team

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

Luis Almagro
Secretary General

Ivan Marques
Secretary of Multidimensional Security
-SMS-

Alison August Treppel
Executive Secretary
Inter-American Committee against Terrorism -
CICTE-

Kerry-Ann Barrett
Orlando Garces
David Moreno
Cybersecurity Program

EXECUTIVE SUMMARY

The digital transformation taking place globally is a powerful facilitator of sustainable and inclusive development. However, it can also pose a new source of risks if the underlying infrastructure and the services that depend on it are neither safe nor protected against cyber threats, which can bring serious economic and social consequences. Governments around the world have worked to address this situation in various ways, one of them being the formulation and implementation of national cybersecurity policies and/or strategies.

The Government of Costa Rica formulated its 2017-2021 National Cybersecurity Strategy, which established an institutional framework that has advanced its functions and activities under the leadership of the Ministry of Science, Innovation, Technology, and Telecommunications (MICITT, from its acronym in Spanish) and the Computer Security Incident Response Center (CSIRT-CR, from its acronym in Spanish). While this strategy has also allowed for significant progress in matters of cooperation, education, and socialization regarding the safe use of Information and Communication Technologies (ICT), it is essential to reinforce efforts to close cybersecurity capacity gaps so that the various involved parties can seize any present and future opportunities offered by the Fourth Industrial Revolution.

In 2022, the country experienced large-scale cyberattacks against a group of public institutions, affecting information system structures through the use of ransomware. This experience, combined with the rise of new cyber threats and risks, has impacted the digital economy, as well as national security and defense. As a result, the national government has decided to reevaluate its stance on cybersecurity at all levels.

The new 2023-2027 National Cybersecurity Strategy articulates a strategic vision under an efficient institutional model, strengthening the national government's leadership and linking all stakeholders under a human rights focus, in line with building an inclusive society in all areas of Costa Rican life.

This strategy includes an action plan to strengthen cybersecurity governance, adapt the cyber-legal framework, enhance protection for infrastructures and national cyber resilience, bolster the cybersecurity ecosystem, and actively cooperate in the digital environment. These documents have been developed and agreed upon within the cybersecurity ecosystem and are strategically linked with other current policy instruments to ensure the country achieves the objectives set forth in the 2023-2026 National Development and Public Investment Plan (PNDIP); the 2018-2030 National Policy for Effective Equality between Women and Men; the 2022-2027 National Science, Technology, and Innovation Plan; and the 2023-2027 National Digital Transformation Strategy.

To harness the current benefits that technology provides and to manage the challenges brought about by the country's digitalization and digital transformation with a holistic vision and multisectoral attention, the Government of Costa Rica reaffirms its commitment to maintaining a secure cyberspace by updating its National Cybersecurity Strategy. It also appreciates the specialized technical support from the Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS).

TABLE OF CONTENTS

LIST OF GRAPHICS

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

APC	Association for Progressive Communications
IDB	Inter-American Development Bank
GCI	Global Cybersecurity Index
CGR	Comptroller General of the Republic (CGR, from its acronym in Spanish)
CISTE	Interinstitutional Council on Terrorism (CISTE, from its acronym in Spanish)
CMM	Cybersecurity Capacity Maturity Model for Nations
CNE	National Commission for Risk Prevention and Emergency Response (CNE, from its acronym in Spanish)
CNSL	National Online Safety Commission (CNSL, from its acronym in Spanish)
CSIRT	Computer Security Incident Response Center
CSIRT-CR	Computer Security Incident Response Center in Costa Rica
Cyber4Dev	Cyber Resilience for Development
DIS	Intelligence and Security Directorate (DIS, from its acronym in Spanish)
FNE	National Emergency Fund (FNE, from its acronym in Spanish)
GFCE	Global Forum on Cybersecurity Expertise
GPD	Global Partners Digital
INAMU	National Institute for Women of Costa Rica (INAMU, from its acronym in Spanish)
INTERPOL	International Criminal Police Organization
MICITT	Ministry of Science, Innovation, Technology, and Telecommunications (MICCIT, from its acronym in Spanish)
MCJ	Ministry of Culture and Youth (MCJ, from its acronym in Spanish)
MCM	Ministry of the Status of Women (MCM, from its acronym in Spanish)
MDHIS	Ministry of Human Development and Social Inclusion (MDHIS, from its acronym in Spanish)
MEIC	Ministry of Economy, Industry, and Commerce (MEIC, from its acronym in Spanish)
MEP	Ministry of Public Education (MEP, from its acronym in Spanish)
MH	Ministry of the Treasury (MH, from its acronym in Spanish)
MNA	Ministry of Children and Adolescents (MNA, from its acronym in Spanish)
MP	Ministry of the Presidency (MP from its acronym in Spanish)
MTSS	Ministry of Labor and Social Security (MTSS, from its acronym in Spanish)
MREC	Ministry of Foreign Affairs and Culture (MREC, from its acronym in Spanish)
NCSI	National Cyber Security Index
OAS	Organization of American States
CICTE-OAS	Cybersecurity Program of the Inter-American Committee against Terrorism of the Organization of American States
OIJ	Judicial Investigation Agency (OIJ, from its acronym in Spanish)
PICTTI	2018-2027 National Policy for Men and Women's Equality in Training, Employment, and the Enjoyment of Science, Technology, Telecommunications, and Innovation (PICTTI, from its acronym in Spanish)
PNDIP	2023-2026 National Development and Public Investment Plan (PNDIP, from its acronym in Spanish)
SOC	Security Operations Center
SUTEL	Superintendence of Telecommunications (SUTEL, from its acronym in Spanish)
ICT	Information and Communications Technology
UEI	Special Intervention Unit (UEI, from its acronym in Spanish)
ITU	International Telecommunications Union
UNIDIR	United Nations Institute for Disarmament Research
WEF	World Economic Forum

1. CURRENT CYBERSECURITY CONTEXT

The COVID-19 pandemic and its aftermath have had a significant impact on the global economy, hastening digitalization and digital transformation processes[1], expanding the threat and risk landscape, and causing a major shift in how organizations work. Furthermore, there is an aging population, major issues due to high unemployment, and a reversal in gender parity progress[2] (OAS, 2023). Against this backdrop, cybersecurity has become a priority and is now essential to ensuring safety and economic stability.

This threat[3] and risk landscape is constantly expanding[4] due to a series of factors, such as increasing interconnectivity, the high complexity of new technologies, and the growing sophistication of malicious actors[5]. The adoption of emerging technologies[6] has led to a range of cybersecurity risks, which include new attack vectors and complicates both the implementation and maintenance of security controls.

Ransomware, phishing, online scams, and computer intrusions are the cybercrime trends that countries most frequently perceive as “high” or “very high” threats on a global scale (INTERPOL, 2022). These lead to the unavailability of services offered virtually, information theft, or even impacts on essential services, causing negative consequences for citizens’ economic well-being[7] and/or the effective functioning of private or public organizations.

[1] Digital transformation is poised to be a force that enhances the exercise of citizens’ rights and responsibilities and accelerates productivity, competitiveness, and socio-economic development (MICITT, 2023).

[2] According to the World Economic Forum, the global gender gap in 2023 is 68.6% closed; it will take another 131 years to close the global gender gap and 53 years in Latin America and the Caribbean (WEF, 2023a).

[3] The eight most common cybersecurity threats currently are: ransomware, malware, social engineering, threats against data, threats against availability - denial of service, threats against availability - threats against the internet, misinformation/misuse of information, and attacks on the supply chain (EUROPEAN PARLIAMENT, 2023).

[4] Latin America and the Caribbean suffered more than 360 billion cyberattack attempts in 2022, according to data from FORTINET’s threat analysis and intelligence laboratory. Mexico received the highest number of attack attempts (187 billion), followed by Brazil (103 billion), Colombia (20 billion), and Peru (15 billion) (FORTINET, 2023).

[5] Ransomware and extortion attacks continue to grow with new attempts to compromise information technology supply chains. Ransomware groups are becoming more sophisticated and attacks are becoming more targeted, with certain industries and critical infrastructures being particularly at risk.

[6] (MCKINSEY, 2023) presents the most significant technological trends in 2023.

[7] Online Child Sexual Exploitation and Abuse ranked among the top ten crime trends perceived as a ‘high’ or ‘very high’ threat by member countries, and 62 percent of member countries strongly expected these crimes to ‘increase’ or ‘increase significantly’ in the future (INTERPOL, 2022).

The cost of recovering from a cyberattack, based on factors such as downtime, network costs, working hours, missed opportunities, and more, is growing ever higher. For instance, the average global total cost of a data breach reached US$4.5 million in 2023, while this average cost for the Latin American region reached US$2.8 million (IBM, 2023).

Recent geopolitical events have also significantly influenced cyber strategy and tactical cybersecurity operations worldwide. Efforts are being made to strengthen internal policies and processes, as well as to increase the effectiveness of cybersecurity controls with third parties. These geopolitical tensions have been responsible for greater volatility in the nature of cyber threats, with a broader variation in the types of widely available malware, as well as shifts in the type of assets or value creation processes targeted by cyber attackers (WEF, 2023b).

Governments around the world are collaborating to develop and implement effective national cybersecurity strategies, investing in new technologies to enhance their cyber defense, such as artificial intelligence, machine learning, and blockchain. Likewise, they are working to educate, train, and raise awareness among the public regarding cybersecurity risks, as well as to provide them with the tools and resources they need to protect themselves.

The processes for formulating these types of national strategies are incorporating new topics associated with the latest conditions and trends in cybersecurity at the international level. These include cyber-diplomacy and international security, supply chain security, cloud security, security by design and by default, the safe and secure adoption of emerging technologies, and developing a cybersecurity workforce with focuses on human rights, gender equality, diversity, and social inclusion[8][9].

Lastly, organizations are addressing key priorities, such as creating receptive ecosystems that enhance organizational preparedness, restructuring approaches to solutions and broader attack coverage; rebalancing practices to focus on people, processes, and technology; and designing sustainable and balanced cybersecurity programs (GARTNER, 2023).

[8] The contributions made by international organizations on these topics are highlighted, such as those of the United Nations Institute for Disarmament Research (UNIDIR, 2023), the Association for Progressive Communications (APC, 2023), Global Partners Digital (GPD, 2023), the Global Forum on Cybersecurity Expertise (GFCE, 2023), Chatham House (CHATHAM HOUSE, 2023), and national organizations like Cooperativa Sulá Batsú.

[9] The CICTE-OAS Cybersecurity Program, with the support of the Government of Canada, is advancing the project "Closing the Gender Gap in the Cybersecurity Agenda of the Americas and the Caribbean 2022-2026," promoting the incorporation of a gender and a diversity perspective in national cybersecurity policies/strategies in the region.

2. REGULATORY FRAMEWORK

Costa Rica maintains a legal and regulatory framework to protect society against cybercrime and to promote a secure cyber environment, aligned with the principles of inclusion and a trustworthy environment.

The country has signed international agreements and treaties, undertaking various international commitments related to cybersecurity. For example, these include instruments:

i) to protect and guarantee human rights, especially the basic human rights of children and adolescents;

ii) to eliminate discrimination against women;

iii) to prevent, punish, and eradicate all forms of violence against women;

iv) to promote sustainable development;

v) to develop comprehensive national legislation on cybercrime;

vi) to combat the impunity of those who have committed extremely serious crimes; and

vii) to more effectively prevent and combat transnational organized crime, among others.

The country has also formalized legal cooperation instruments on cybersecurity matters, in partnership with international agencies (transcontinental/regional), multilateral development agencies, and with other independent states that are legally equal.

Table 1. Primary International Instruments Related to the 2023-2027 National Cybersecurity

INTERNATIONAL COMMITMENTS	Agenda for Sustainable Development	European Convention on Cybercrime (Budapest, 2001) and the Second Additional Protocol	Rome Statute	European Union-Central America Association Agreement	Declarations and Resolutions from the CICTE-OAS	Other multilateral and bilateral agreements on the topic
	United Nations Convention against Transnational Organized Crime (Palermo Convention)	Convention on the Elimination of All Forms of Discrimination against Women	Women, Peace, and Security Agenda, and its resolutions	Inter-American Convention to prevent, punish, and eradicate violence against women	United Nations Convention on the Rights of the Child	International Covenant on Civil and Political Rights

Source: Own Creation (2023), considering (APC, 2022)

In relation to the fight against cybercrime, after the promulgation of Law No. 9452, for which the Legislative Assembly approved its adherence on September 22, 2017, Costa Rica signed the accession to the Convention on Cybercrime (Budapest Convention), which went into effect on January 1, 2018[10]. In that same year (2018), Costa Rica was chosen as a beneficiary of the GLACY+ Program, a support initiative from the Council of Europe in implementing the Convention. This reflects the country's commitment to strengthening its capacities to prevent and combat computer crimes, improving international cooperation in this area, and protecting citizens in the digital environment. Additionally, on June 13, 2022, Costa Rica signed the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention), aimed at improving cooperation and the disclosure of electronic evidence.

Costa Rica also has a constitutional, legal, and regulatory framework developed around the dynamics of the digital economy and its inherent uncertainties. On the one hand, the constitutional foundations regarding cybersecurity are found in the Constitution of the Republic of Costa Rica, with standout attention to those related to individual and social rights and guarantees; the order, defense, and security of the country; and sovereignty.

On the other hand, highlights from the legislation issued in the country consider:

i) the promotion of scientific and technological development;

ii) the protection and privacy of personal data;

iii) online child protection;

iv) the promotion of social equality for women;

v) consumer defense;

vi) legal intervention in communications; and

vii) the adoption of certificates, digital signatures, and electronic documents, among others.

Regarding comprehensive legislation against cybercrime at the substantive law and procedural law levels, the promulgation of several laws that reform and add various computer crimes and related offenses to Costa Rican criminal legislation stands out.

[10] Costa Rica presented two (2) interpretative observations on Articles 10 and 24 of the Convention on Cybercrime (Budapest Convention).

Table 2. Constitutional and Legal Framework Related to the 2023-2027 National Cybersecurity Strategy

CONSTITUTIONAL AND LEGAL FRAMEWORK

- Political Constitution of 1949
- Law 7472 on the Promotion of Competition and Effective Consumer Defense
- Law 8488 on Emergencies and Risk Prevention
- Law 9048 on Computer and Related Crimes
- Law 10235 to Prevent, Attend, Punish, and Eradicate Violence Against Women in Politics
- Law 4573 Penal Code
- Law 7594 Criminal Procedure Code
- Law 8642 General Telecommunications Law
- Law 9135 that reforms and adds computer crimes
- Law 10238 on the Protection of the Image, Voice, and Personal Data of Minors
- Law 6683 on Copyright and Related Rights
- Law 7975 on Undisclosed Information
- Law 8660 of Strengthening and Modernization of Public Entities in the Telecommunications sector
- Law 9162 on Single Digital Health Record
- Law 7142 on the Promotion of Social Equality for Women
- Law 8039 on Procedures for the Enforcement of Intellectual Property Rights
- Law 8719 on Strengthening Legislation against Terrorism
- Law 9452 adheres to the European Convention on Cybercrime (Budapest, 2001)
- Law 7169 on the Promotion of Scientific and Technological Development
- Law 8148 to Repress and Punish Computer Crimes
- Law 8934 on the Protection of Children and Adolescents against harmful content on the Internet and other electronic media
- Law 9738 to Regulate Remote Working
- Law 7425 on Registration, Seizure and Examination of Private Documents and Intervention of Communications
- Law 8454 on Certificates, Digital Signatures and Electronic Documents
- Law 8968 on the Protection of Individuals against the Processing of their Personal Data
- Law 9975 on Penalization of Violence Against Women

Source: Own elaboration (2023) considering (SULA BATSU & GPD, 2023)

Regarding the regulatory framework related to cybersecurity, a highlight is that in which the Ministry of Science, Innovation, Technology, and Telecommunications (MICITT) is granted leadership in matters of science, technology, telecommunications, and digital governance for the country. Technical standards are established, and several bodies are created to address related topics; these include the Inter-institutional Council on Terrorism (CISTE), the National Online Security Commission (CNSL), and the Computer Security Incident Response Center (CSIRT-CR) under the MICITT[11].

[11] Decree No. 37052-MICITT establishes the Computer Security Incident Response Center (CSIRT-CR) with adequate powers to coordinate with state powers, autonomous institutions, state companies, and banks, on all matters related to computer security and cybersecurity. It specifies the team of Information Technology security experts who will work to prevent and respond to cybersecurity and computer incidents affecting government institutions.

Table 3. Regulatory Framework Related to the 2023-2027 National Cybersecurity Strategy

REGULATORY FRAMEWORK	Decree 31659-MP-RE Creation of the Interinstitutional Commission on Terrorism (CISTE)	Decree 33018-MICIT Regulations to the Law on Certificates, Digital Signatures and Electronic Documents	Decree 36274-MICIT Creation of the National Online Safety Commission (CNSL)	Decree 37052-MICIT Creation of the CSIRT-CR	Decree 37554-JP Regulations to the Law on the Protection of Individuals against the Processing of their Personal Data	Decree 40199-MP Opening of Public Data
	Decree 40546 - RREE Adhesion of the Republic of Costa Rica to the European Convention on Cybercrime (Budapest, 2001)	Decree 41187-MP-MIDEPLAN Organic Regulations of the Executive Branch	Decree 43542-MP-MICITT State of Emergency Due to the Cybercrimes of 2022	Guideline 133-MP-MICITT Recommendations and Technical Measures for the MICITT and CSIRT-CR	National Code of Digital Technologies	Technical standards for the government and management of information technologies

Source: Own elaboration (2023)

Finally, the government has issued guidelines that provide instructions to entities of the Central Public Administration, regarding reporting cybersecurity incidents to the CSIRT-CR and promoting implementation of security measures and mechanisms.

3. DIAGNOSTIC

Costa Rica has undergone a profound digital transformation over the past decade. According to the Telecommunications Superintendency (SUTEL), the internet has become an essential service for consumers, both through fixed and mobile networks. This growth has been significant, in terms of the number of users, speeds, and volume of information traffic (SUTEL, 2023).

Table 4. Evolution in Mobile and Landline Subscribers and Traffic in Costa Rica

		2019	2020	2021	2022
Mobile Phones	Mobile Phone Subscribers / 100 inhabitants	145%	147%	152%	151%
	Mobile Internet Access Subscribers / 100 inhabitants	92%	93%	95%	96%
	Traffic, Internet access via mobile network (thousands of TB)	160	223	269	332
Landline Phones	Landline Phone Subscribers / 100 inhabitants	13%	11%	10%	9%
	Landline Internet Access Subscribers / 100 inhabitants	18%	19.4%	20.5%	21.2%
	Traffic, Internet access on the landline network (thousands of TB)	1162	2212	3280	3557

Source: (SUTEL, 2023)

Within the country, the evolution of the digital environment has led to an increase in society's participation in economic and social activities supported by Information and Communication Technologies (ICT), creating greater inclusion for the population, reducing barriers, and increasing productivity and competitiveness, and thus, economic growth. However, Costa Rican society's increased presence of in the digital environment has created more risks and uncertainties in recent years. Aware of this situation, the Government of Costa Rica issued the 2017-2021 National Cybersecurity Strategy.

3.1. Implementation of the 2017-2021 National Cybersecurity Strategy

Costa Rica has undergone a process and executed actions to improve national cybersecurity, helping close digital gaps[12]. In 2017, this led the country to set a common purpose, by developing its 2017-2021 National Cybersecurity Strategy. The overall objective of this national strategy was to develop a guiding framework for the country's actions, regarding security in the use of ICT, promoting the coordination and cooperation of the various stakeholders, while promoting measures for education, prevention, and mitigation against the risks related to the use of ICT, in order to achieve a safer and more reliable environment for all of the country's inhabitants.

[12] In particular, the MICITT has documented the persistence of a gender digital gap in the access, use, and professionalization that needs to be addressed through the coordination of public policies, government agendas, action plans, and various interventions (MICITT, 2017). During the implementation period for the 2017-2021 National Cybersecurity Strategy, Costa Rica made progress in reducing its digital divide, according to the 2016-2018 Digital Divide Index (IBD) from MICITT (MICITT, 2019).

The Global Cybersecurity Index (GCI) is a trusted benchmark that measures countries' commitment to cybersecurity globally (ITU, 2023).

To achieve this objective, actions would be implemented to extend to eight (8) work areas:

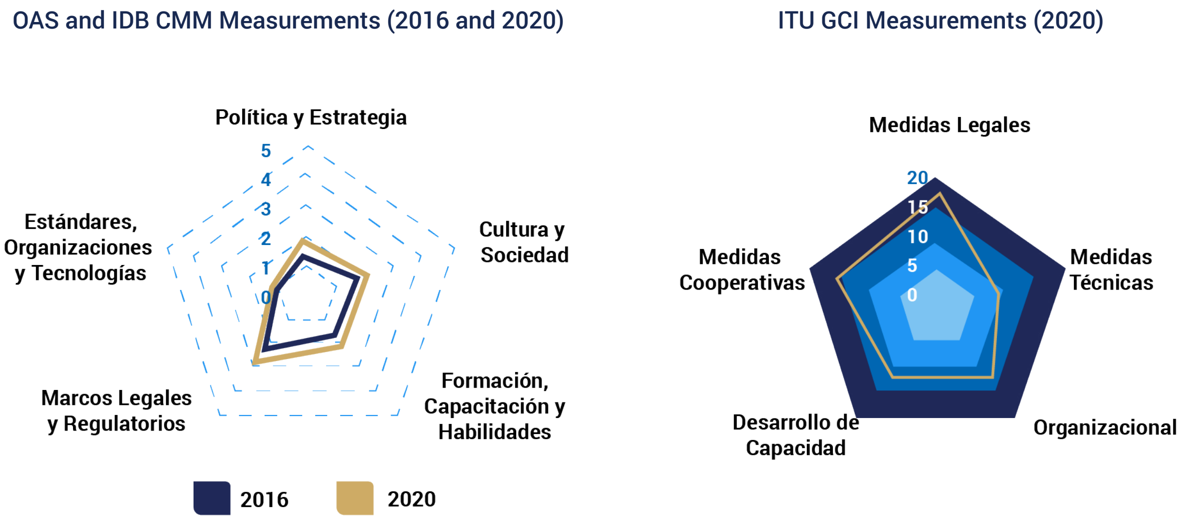
- **National coordination**
- **Public awareness**
- **Capabilities**
- **Legal framework**
- **Critical infrastructures**
- **Risk management**
- **International cooperation**
- **Implementation, monitoring, and evaluation**

Considering its specific conditions during the period of formulation and implementation, the country made progress in this area. MICITT was established as the leading entity in national cybersecurity. The CSIRT-CR was created and strengthened as a leading institution in cybersecurity topics, and as the coordinator of other country agencies, as the institution responsible for improving institutional capabilities. Joint efforts were coordinated with the National Online Security Commission (CNSL). Some best practices and information exchange initiatives, training sessions, and study programs were implemented. Valuable training initiatives were executed, focusing on digital hygiene and cybersecurity best practices for minors and teenagers, along with certain awareness campaigns, thus strengthening the country's culture of cybersecurity. Various collaborative projects were advanced through some public-private partnerships, as well as with international partners in various distinctive areas of cybersecurity, thus demonstrating the country's commitment to international cooperation.

These advances managed to position the country by improving several aspects related to the maturity of cybersecurity capabilities. The 2020 Global Cybersecurity Index (GCI) measurement[13] on the International Telecommunication Union (ITU) placed Costa Rica in position 76 globally, improving 39 places compared to its 2018 measurement. Reports on the state of cybersecurity in the Latin America and the Caribbean region, as issued by the Organization of American States (OAS) and the Inter-American Development Bank (IDB) applying the Cybersecurity Capability Maturity Model[14], also reflected national improvement between the 2016 and 2020 measurements (OAS & IDB, 2020), especially with regard to legal and regulatory frameworks and professional training frameworks.

[13] The Global Cybersecurity Index (GCI) is a trusted benchmark that measures countries' commitment to cybersecurity globally (ITU, 2023).
[14] The Cybersecurity Capacity Maturity Model for Nations (CMM) is a methodical framework designed by the Global Cybersecurity Capacity Centre of the Computer Science Department at the University of Oxford to review a country's cybersecurity capability (GCSCC, 2023).

Chart 1. Costa Rica in International Measurements of Cybersecurity Capabilities


OAS and IDB CMM Measurements (2016 and 2020)

ITU GCI Measurements (2020)

Source: Own elaboration from (OAS & IDB, 2020) and (UIT, 2023)

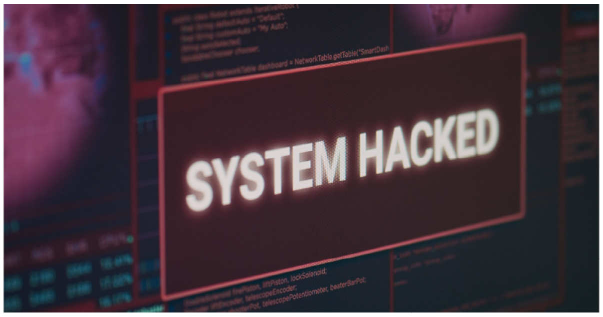
Once the established period to implement the 2017-2021 National Cybersecurity Strategy was completed, a review of the same was carried out under the leadership of the MICITT and with the specialized technical support of the OAS/CICTE Cybersecurity Program and the European Union's Cyber Resilience for Development (Cyber4Dev) project. The results of the review were captured in a report (MICITT, 2021) that presented a situational analysis for each of the set objectives, along with recommendations (see Annex 1) regarding the implementation of organizational, legal, and technical measures, as well as capacity building and cooperation to enhance the country's capabilities.

3.2. Recent Challenges at the National Level

In 2022, the Government of Costa Rica experienced large-scale cyberattacks against a set of public institutions, affecting the structure of information systems through the use of ransomware. Some identified damages were the loss of operability in computer systems, data theft, and data leaks.

In response, the national Government issued Executive Decree No. 43542-MP-MICITT of 2022, declaring a State of National Emergency throughout the Costa Rican public sector and quickly recognizing the value of international cooperation to address the challenge. This situation led to the development of a General Emergency Plan (CNE, 2022), facilitating the availability of resources and the necessary administrative acts for its attention. This plan states that the estimated response cost to address the cyberattacks amounted to ₡15.949 billion, of which ₡11.158 billion come from the institutions' own resources and ₡4.791 billion are contributed by the National Emergency Fund (FNE).

According to the Comptroller General of the Republic (CGR, 2023), the cyberattacks affected the ordinary duties of at least 45,535 public servants, impacting 49 types of procedures and services, and causing a loss of institutional revenues, as well as the loss of information or its quality or availability, which influenced decision-making, transparency, and accountability. The CGR analyzed the implications and costs of the cyberattacks for the Public Treasury and society, in general, and presented recommendations (see Annex 2) to both the executive and legislative powers in the country, regarding the need to implement organizational, legal, and technical measures, as well as capacity building and cooperation.



In this way, these cyberattacks have significantly influenced the way the Government views cybersecurity and risk management, in both public and private organizations. Given the significant socio-economic impact that cybersecurity incidents like these can have, there is a willingness at the highest level to invest political capital, time, money, and resources into ensuring a safer cyberspace for Costa Rican citizens. However, this must be weighed against the reality of the limited cybersecurity capability that exists at the national level and which requires addressing. For instance, in the National Cyber Security Index (NCSI), Costa Rica dropped from the 42nd rank globally in 2020 to the 77th rank in 2023, meaning it lost 35 positions.

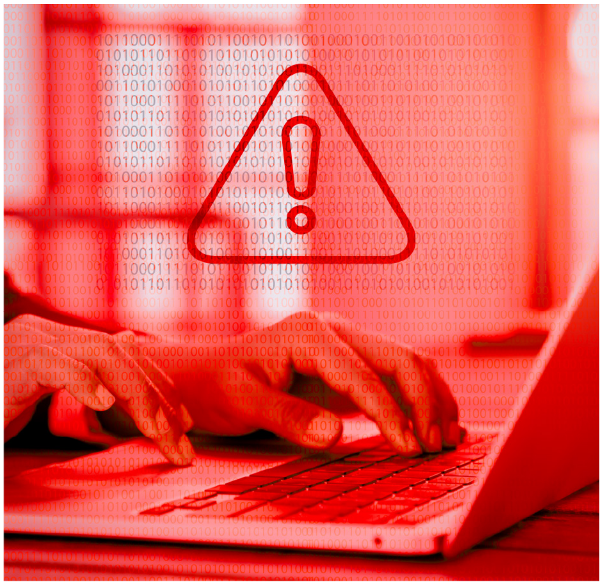
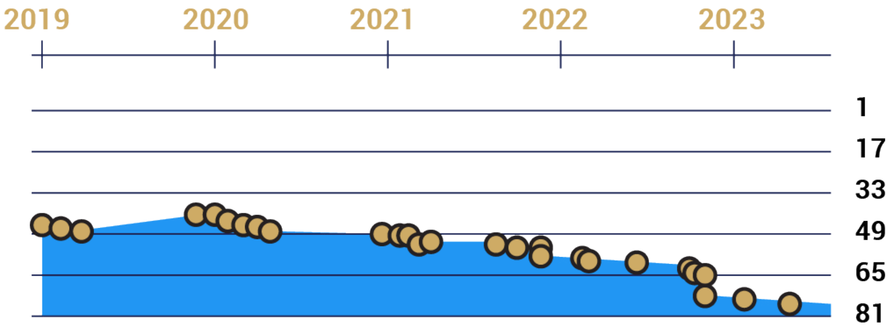


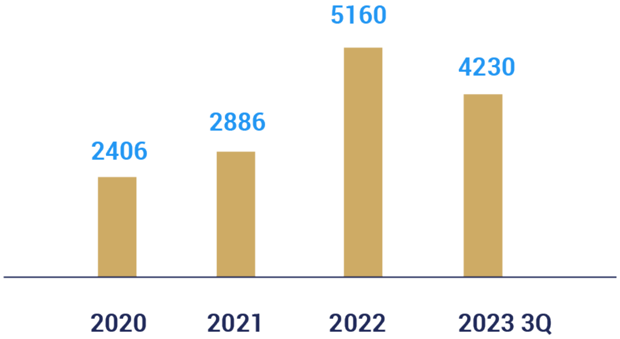
Chart 2. Evolution of Costa Rica's Measurement on the *National Cyber Security Index* (NCSI), from the e-Governance Academy of Estonia



Source: (e-Governance Academy, 2023)

The conditions for developing socio-economic activities in Costa Rica changed drastically after the cyberattacks of 2022. The increase in digital cybersecurity threats and risks has impacted and created problems for the State, the economy, and society, and these need to be addressed under a new national strategy that integrates a new strategic vision with fresh approaches that adopt international best practices.

Chart 3. Evolution of Reports on Computer & Technology Crimes in Costa Rica



Source: *Judicial Branch (2023)*

During 2022 and 2023, the MICITT and the CSIRT-CR continued to coordinate and lead national cybersecurity initiatives, making significant efforts under a dynamic framework of cooperation at the national level, in partnership with other branches of public power and internationally, aiming to improve cybersecurity capabilities at Central Public Administration institutions, as well as those of other stakeholders in the country.

4. STRATEGIC FRAMEWORK

The 2023-2027 National Cybersecurity Strategy[15] provides a cohesive and compelling vision built with the participation from all the multiple stakeholders, including the public and private sectors, civil society organizations, academia, and the general community, addressing the unique needs and challenges of Costa Rican citizens, while promoting equal opportunities and inclusive participation in cybersecurity initiatives.

The government also builds on the achievements, goals, and criteria of the 2017-2021 National Cybersecurity Strategy, and on the experiences addressed during 2022 and 2023. The institutions and initiatives developed in recent years have helped establish significant cybersecurity capabilities in Costa Rica, and these need to be enhanced.

To mitigate the multiple threats and protect Costa Rica's interests in cyberspace, a strategic approach is needed to guide all collective and individual actions in the digital realm over the next four years. This section establishes the strategic framework, considering Costa Rican citizens' various perspectives and experiences, to ensure a comprehensive and equitable cybersecurity strategy.

4.1. Strategic Alignment

The 2023-2027 National Cybersecurity Strategy is strategically aligned with various public policy instruments and national planning. On the one hand, it aligns with the strategic framework related to the science, innovation, technology, and telecommunications sectors, emphasizing the development of Costa Rican society and the economy. On the other hand, it aligns with the strategic framework, which promotes the cessation of all inequality and integrates a gender perspective into the activities of public institutions, to build an inclusive society in all areas of Costa Rican life[16].

[15] The 2023-2027 National Cybersecurity Strategy takes into account the national planning guidelines established in the following strategic documents: i) Guidelines to incorporate Strategic Prospective Planning in the National Planning System (SNP) (MIDEPLAN, 2023b); ii) Intervention Theory Guide (MIDEPLAN, 2018a); iii) Indicator Guide - Basic guidelines for its preparation (MIDEPLAN, 2018b); iv) Guide on the gender equality and human rights approach (MIDEPLAN, 2017b); v) 2017-2032 National Policy for the Care, Prevention, and Protection of Violence against Women of All Ages (PLANOVI) (INAMU, 2018); and vi) Planning Guide with a Focus on Results in Development – Theoretical and Practical Framework (MIDEPLAN, 2016).
[16] In line with national challenges, as related to the prevention and attention of online risks faced by minors, historically discriminated individuals, and groups living in vulnerable conditions, as well as online gender violence affecting women with multiple identities and members of the LGBTI community (Lesbians, Gays, Bisexuals, Transgender, and Diverse Gender and Intersex individuals), the incidence of which saw a considerable increase throughout Latin America due to the accelerated use of digital technologies during the COVID-19 pandemic (OAS, 2021) (OAS & UN Women, 2021) (ECLAC, 2022).

Table 5. National Policies, Plans, and Strategies Related to the 2022-2050 National Policy on the Knowledge-Based Economy and Society

PUBLIC POLICY	2022-2050 National Knowledge-Based Economy and Society Policy	2018-2030 National Policy for Effective Equality between Women and Men (PIEG)	2018-2027 National Policy for Men and Women's Equality in Training, Employment, and the Enjoyment of Science, Technology, Telecommunications, and Innovation (PICTTI)	2014-2025 National Policy for a Society Free of Racism, Racial Discrimination, and Xenophobia	2017-2032 National Policy for the Care, Prevention, and Protection of Violence against Women of All Ages (PLANOVI)	2016-2030 National Risk Management Policy
PLANS	2023-2026 National Development and Public Investment Plan (PNDIP)	2022-2027 National Science, Technology, and Innovation Plan (PNCTI)	2022-2027 National Telecommunications Development Plan (PNT)	2022-2026 Education Route	National Action Plan for Resolution 1325 (2000) of the United Nations Security Council on Women, Peace and Security	
STRATEGIES	2023-2027 National Digital Transformation Strategy[17]*	2021-2027 National Strategy for the Prevention of and Response to Online Sexual Exploitation and Online Abuse of Children and Adolescents	2022-2026 National Strategy to Combat Sexual Harassment and Harassment against Women			

Note: * Document under non-binding Public Consultation during the month of June 2023[18]
Source: Own elaboration (2023)

[17] The National Digital Transformation Strategy 2023-2027 establishes Cybersecurity as a pillar for the development of *Digital Government.*

[18] See https://www.micitt.go.cr/consultas-publicas/

The 2023-2027 National Cybersecurity Strategy will include public interventions with the goal of achieving objectives established in the *2023-2026 National Development and Public Investment Plan (PNDIP)* (MIDEPLAN, 2023a) and that are related to cybersecurity. For instance, this includes a goal of 25,938 individuals participating in spaces to promote awareness on cybersecurity[19] between 2023 and 2026, as well as the goal of 40 security and disarmament diplomacy activities[20] to be implemented during the same period.

Similarly, public interventions will support the creation of safe cyberspaces that reduce risk factors, as well as the vulnerability of certain groups of women – particularly, training sessions on addressing and preventing gender violence, digital risk, and digital vulnerability for personnel working in the computer crime sector. This goal is established in the *2018-2027 National Policy for Men and Women's Equality in Training, Employment, and the Enjoyment of Science, Technology, Telecommunications, and Innovation (PICTTI)* (MIDEPLAN, 2017a).

4.2. Guiding Approaches

The 2023-2027 National Cybersecurity Strategy is formulated for implementation under national strategic approaches that underpin the actions taken and help guide decision-making:

- **Whole-Society approach,** wherein effective coordination is promoted among state and non-state actors, such as essential service providers, internet service providers, the digital ecosystem, academia, civil society organizations, etc.

- **Risk Management and Mitigation approach,** wherein the need to ensure that adopted measures address or keep pace with evolving threats is recognized, ensuring an adequately trained workforce with sufficient agility to respond.

- **Human Rights approach[21],** which places the people of Costa Rica at the center and ensures the full exercise of individuals' rights, demonstrating that the outcomes of implementing public cybersecurity interventions will not result in discrimination due to ethnicity, age, sex, religious belief, place of residence, or disability status, among other factors.

- **Human-centered approach[22],** addressing the differentiated risks and impacts of cyber threats, so that cybersecurity responds to the complex, differentiated, and intersectional needs of people in Costa Rica, based on gender, sexual orientation, race, religion, ethnicity, ability, class, nationality, rurality, and political affiliation, among other factors.

[19] The 2023-2026 PNDIP defines Cybersecurity Promotion Spaces as, *"spaces or activities, such as events, webinars, talks, courses, or workshops."* It also defines *"Cybersecurity Promotion"* as topics *"ranging from computer culture in cybersecurity, digital literacy, advice, best practices, online life, including specialized actions on issues of incidents, responses, networks, software development, analytics, and legal aspects."* (emphasis not in the original text)

[20] The 2023-2026 PNDIP defines security and disarmament diplomacy activities as, *"activities implemented refers to activities carried out in coordination with governing entities, diplomatic missions, international organizations, and organized civil society, in areas such as: Disarmament, nuclear disarmament, arms trade, security, fight against organized crime, fight against drug trafficking, fight against corruption, fight against terrorism, nuclear use for peaceful purposes, cybercrime, cybersecurity, peace, and conflict prevention, among others."* (emphasis not in the original text)

[21] In line with the Human Rights approach of the 2018-2027 PICTTI (MIDEPLAN, 2017a).

[22] In line with the Gender and Diversity approach of the 2018-2027 PICTTI (MIDEPLAN, 2017a).

4.3. Vision

By 2027, Costa Rica's digital ecosystem will be trustworthy and will contribute to the global effort to secure cyberspace, offering an exchange of knowledge and experiences from the country's developed cybersecurity workforce.

4.4. Mission

To establish a comprehensive action framework that allows for preventing and mitigating risks and threats in the digital environment, promoting innovation and the development of cybersecurity solutions, strengthening the response capacity to cybersecurity incidents, and fostering a strong security culture, all with the goal of helping ensure the country's stability and its economy, protecting the state's and citizens' personal and critical information, and maintaining trust in the use of digital systems.

4.5. Guiding Principles

The 2023-2027 National Cybersecurity Strategy applies the following guiding principles:

- **Comprehensive risk management.** All stakeholders must understand cybersecurity risks and assess the potential impact of comprehensive cybersecurity risk management decisions on their socio-economic activities and the digital environment, in general.

- **Respect for human rights and fundamental values.** All stakeholders must manage cybersecurity risks in a manner both transparent and consistent with human rights and the fundamental values of the Costa Rican Republic.

- **Shared Responsibility.** All stakeholders must take responsibility for comprehensive cybersecurity risk management, observing the role they hold under the country's cybersecurity governance framework.

- **Cooperation.** All stakeholders must cooperate, even beyond the country's borders, to promote a secure cyber environment.

- **Innovation.** Leaders and decision-makers representing stakeholders must ensure that innovation is considered when implementing cybersecurity initiatives.

4.6. Pillars

The 2023-2027 National Cybersecurity Strategy establishes five *"priority actions"* that set strategic objectives and are used as pillars for the strategic framework, guiding and organizing the specific lines of action to be taken, as well as the intended results, to be achieved by 2027:

- **Pillar 1:** Strengthen Cybersecurity Governance, optimizing public investment and deepening coordination among government, industry, academia, society, and the international community (MORE CYBER-COORDINATED).

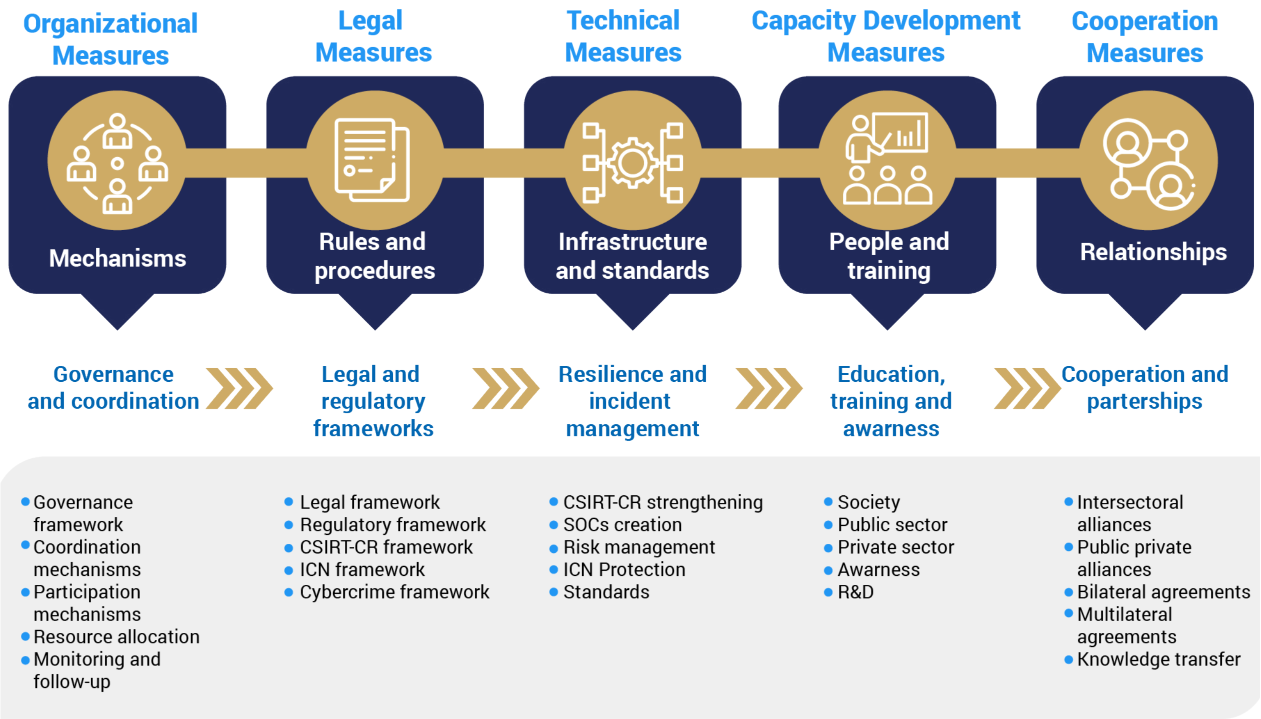
- **Pillar 2:** Adapt the Cyber Legal Framework, promoting a culture of compliance and considering evolving cyber threats, technological advances, and the unique needs of the Nation (MORE CYBER-UPDATED).

- **Pillar 3:** Strengthen the Protection of Infrastructures and National Cyber Resilience, safeguarding national critical infrastructures and managing cybersecurity risks appropriately, so that stakeholders can maximize the benefits of the digital environment and citizens are safer online (MORE CYBER-SECURE).

- **Pillar 4:** Enhance the Capabilities of the Cybersecurity Ecosystem, educating, training, forming, and raising awareness among all multiple stakeholders, and promoting cybersecurity research and development (MORE CYBER-PREPARED).

- **Pillar 5:** Cooperate in the Digital Environment, building public-private partnerships and exercising cyber-diplomacy in favor of a safer, prosperous, and open international order (MORE CYBER-INTEGRATED).

Chart 4. Pillars of the 2023-2027 National Cybersecurity Strategy



Organizational Measures – Mechanisms – Governance and coordination
- Governance framework
- Coordination mechanisms
- Participation mechanisms
- Resource allocation
- Monitoring and follow-up

Legal Measures – Rules and procedures – Legal and regulatory frameworks
- Legal framework
- Regulatory framework
- CSIRT-CR framework
- ICN framework
- Cybercrime framework

Technical Measures – Infrastructure and standards – Resilience and incident management
- CSIRT-CR strengthening
- SOCs creation
- Risk management
- ICN Protection
- Standards

Capacity Development Measures – People and training – Education, training and awarness
- Society
- Public sector
- Private sector
- Awarness
- R&D

Cooperation Measures – Relationships – Cooperation and parterships
- Intersectoral alliances
- Public private alliances
- Bilateral agreements
- Multilateral agreements
- Knowledge transfer

Source: Own elaboration (2023)

4.7. Primary Objective

To ensure and guarantee the conditions required for a national cybersecurity ecosystem that is safe, resilient, and inclusive, effectively protecting national critical infrastructures, the public and private sectors, and citizens from cyber threats.

4.8. Specific Objectives and Lines of Action

The 2023-2027 National Cybersecurity Strategy establishes actions dedicated to all sectors of the economy and society, from central government administrative institutions to leaders across all industries and citizens, in order to achieve both strategic objectives and the overall goal. The strategy aims to increase cybersecurity at all levels, for the collective benefit, and will form the foundation from which Costa Rica will participate internationally, to promote a safer cyberspace.

PILLAR 1

STRENGTHEN CYBERSECURITY GOVERNANCE

MORE CYBER-COORDINATED

Costa Rica will establish a governance framework that defines the roles, responsibilities, and coordination, collaboration, and communication mechanisms among government entities, private sector organizations, academia, civil society organizations, and the international community. This pillar focuses on overall coordination, leadership, and decision-making processes in cybersecurity.

• Line of Action 1.1. Consolidate the National Cybersecurity Coordination Body

- Establish and launch a roadmap to restructure the MICITT, by consolidating and centralizing cybersecurity efforts and activities at the national level.
- Strengthen the national coordination body to direct the implementation of the 2023-2027 National Cybersecurity Strategy and carry out continuous monitoring, thus equipping it with legal and technical tools that allow it to perform its functions most effectively.
- Ensure that the national coordination body has a specialized, qualified, and technical team dedicated to cybersecurity actions that promote gender equality and diversity.

• Line of Action 1.2. Establish a Whole-Society Cybersecurity Governance Framework

- Design and launch a national cybersecurity governance framework, promoting participation from multiple stakeholders, including national authorities and civil society organizations, and defend people's rights based on their diverse needs.
- Renew the highest intergovernmental and intersectoral strategic planning body to guide cybersecurity management within the country, to promote gender equality and diversity.
- Create tactical planning bodies to advise on the implementation of established and prioritized actions, taking into account cooperation with technological leaders and experts in the field.
- Create and launch dynamic coordination, collaboration, and intergovernmental and intersectoral information exchange mechanisms that link multiple stakeholders.
- Create a liaison figure (a person responsible for cybersecurity) at public institutions, in local governments, and in other organizations at the operational level.
- Develop strategies, protocols, and communication mechanisms that promote participation from all stakeholders, especially from academia and the private sector, and that account for execution of the action plan.
- Establish mechanisms for monitoring and controlling key performance indicators and comprehensive cybersecurity risk management, including indicators that contribute to measuring gender impact with an intersectional perspective.
- Conduct socio-economic impact assessments regarding implementation of the 2023-2027 National Cybersecurity Strategy.

• Line of Action 1.3. Efficiently Allocate Resources for the Implementation of Cybersecurity Initiatives

- Establish and launch a roadmap for the transition to end the state of emergency declared by Executive Decree No. 43542-MP-MICITT of 2022.
- Develop an investment plan that ensures the availability and allocation of sufficient resources at public institutions, to carry out cybersecurity initiatives.

- Strengthen the capacity of public institutions by ensuring suitable human resources, promoting gender equality and diversity, and creating specialized cybersecurity job profiles.

- Encourage public institutions to guarantee financial resources by annually budgeting those necessary for comprehensive cybersecurity risk management.

- Establish efficient processes for the acquisition and purchase of technological resources at public institutions, to ensure comprehensive cybersecurity risk management.

- Promote the design of incentives for private sector investment in financing cybersecurity projects.

PILLAR 2

ADAPT THE CYBER LEGAL FRAMEWORK

MORE CYBER-UPDATED

Costa Rica will develop cyber legislation and regulation along with a technical regulatory framework for cybersecurity. This pillar ensures the existence of robust legal and regulatory frameworks to promote comprehensive cybersecurity risk management and address cyber threats.

• Line of Action 2.1. Strengthen the Cyber Legal and Regulatory Framework

- Support the Legislative Assembly in processing initiatives or projects to adjust, adapt, and/or harmonize the legal framework, as related to cybersecurity.

- Assist sectoral regulators in processing initiatives or projects to adapt, adjust, and/or harmonize the regulatory framework, as related to cybersecurity, as well as in exercising supervision and verification of compliance with sectoral regulatory framework provisions, as related to cybersecurity.

- Thoroughly review and update the cyber legal and regulatory framework, emphasizing legal protections against gender-based cyber threats from an intersectional perspective, to prevent, sanction, and eradicate the gender violence that is facilitated by digital technologies.

• Line of Action 2.2. Strengthen the Technical Regulatory Framework related to Comprehensive Cybersecurity Risk Management

- Update the regulatory framework to strengthen administrative and technical processes for the Computer Security Incident Response Center (CSIRT-CR).

- Establish standards, protocols, and technical procedures for the prevention, containment, resolution, and response to national cybersecurity incidents, including:
    - Guidelines to evaluate inter-institutional ICT security programs.
    - Contingency plans for ICT security in the public sector.
    - Guidelines to reduce the impact and likelihood of ransomware and data extortion incidents in public and private organizations, including best international practices to prepare, prevent, and mitigate these incidents.

- Develop a regulatory framework to protect national critical infrastructures and essential service operators, adopting international standards and norms, including:
    - A national protocol for the management of and response to cyber crises and emergencies.
    - Contingency and recovery plans for national critical infrastructures and essential services.
    - A manual for conducting national cybersecurity exercises and drills.

- Promote compliance with the technical regulatory framework, as related to comprehensive cybersecurity risk management.

PILLAR 3

STRENGTHEN THE PROTECTION OF INFRASTRUCTURES AND NATIONAL CYBER RESILIENCE

MORE CYBER-SECURE

Costa Rica will establish a comprehensive cybersecurity risk management framework that allows for the detection, reporting, analysis, and timely response to cybersecurity incidents. This pillar focuses on developing capabilities for responding to cybersecurity incidents, as well as for effective coordination and communication among stakeholders during cyber crises.

• Line of Action 3.1. Adopt a Framework for Comprehensive Cybersecurity Risk Management

- Develop a comprehensive cybersecurity risk management framework at the national level, incorporating a gender perspective with an intersectional approach to protect the rights of individuals, based on their diverse needs.
- Establish periodic monitoring and review processes for implementing the comprehensive cybersecurity risk management framework, while adapting it to new threats, vulnerabilities, and trends in cybersecurity.
- Ensure that cybersecurity risk management processes and information security risk management are integrated into the strategic, operational, and budgetary planning processes at public institutions.

• Line of Action 3.2. Strengthen National Capabilities for Monitoring, Detecting, and Responding to Cybersecurity Incidents

- Create and execute a plan to strengthen operational, administrative, human, scientific, and physical infrastructure capabilities for the Computer Security Incident Response Center (CSIRT-CR), to strengthen the same as a national team for cybersecurity incident response.
- Provide a Security Operations Center (SOC) solution to monitor, detect, and respond to cybersecurity incidents at prioritized public institutions.
- Provide prioritized public institutions with technological solutions for threat detection and prevention.
- Create and launch a permanent national Security Operations Center (SOC-CR) that is responsible for preventive, reactive, and proactive cybersecurity risk management at the national level.
- Implement advanced intersectoral alert and response systems for cybersecurity incidents at prioritized public institutions.
- Create and execute a strategy to promote the creation and strengthening of sectoral SOCs.

• Line of Action 3.3. Protect and Defend National Critical Infrastructure and Essential Service Operators

- Define and periodically evaluate the criteria for designating national critical infrastructures, taking into account the human rights protections for individuals, based on their diverse needs.
- Periodically evaluate the designation(s) for critical national infrastructure(s), based on defined criteria.
- Identify, categorize, and update national critical infrastructures and essential service operators.
- Promote development of cybersecurity risk assessments on national critical infrastructures, in conjunction with essential service operators.
- Coordinate national cybersecurity exercises and drills to test preparedness for the operators of national critical infrastructures and essential services.

• Line of Action 3.4. Strengthen the Processing of Information Related to Cybersecurity Incidents

- Create a National Cybersecurity Incident Registry, emphasizing reporting for cybersecurity incidents at national critical infrastructures.
- Establish efficient mechanisms to ensure the proper processing, management, storage, sharing, and information exchange regarding cybersecurity incidents among multiple stakeholders, including the application of industry-recommended standards and participation in regional and international networks, such as the OAS/CICTE's CSIRT Americas Network.
- Create and implement a notification mechanism for law enforcement authorities.
- Create and implement a notification mechanism for individuals and/or organizations affected by cybersecurity incidents.
- Disseminate timely and reliable information regarding cybersecurity risks affecting Costa Rican society, highlighting those that are due to gender and other intersectionalities.

PILLAR 4

ENHANCE THE CAPABILITIES OF THE CYBERSECURITY ECOSYSTEM

MORE CYBER-PREPARED

Costa Rica will develop a skilled cybersecurity workforce through education, training, and formation programs, promoting cybersecurity awareness among the public and fostering a culture of responsible and secure online behavior. Similarly, it will promote research and development in cybersecurity to encourage innovation, enhance capabilities, and stay ahead of evolving cyber threats. This pillar emphasizes the importance of developing human capital and public engagement, and bridging the gender gap in the workforce, as well as the development of cutting-edge technologies, tools, and methodologies to strengthen national cybersecurity defenses.

• Line of Action 4.1. Improve and Expand Cyber Capabilities and Skills, at All Levels

- Develop and implement a national cybersecurity education and training plan across all levels of the Costa Rican educational system, promoting a curriculum that includes cybersecurity content and promotes diversity, gender equality, and social inclusion.
- Formulate and implement a national cybersecurity workforce development strategy, to address labor market needs and cybersecurity trends, as well as to promote diversity, gender equality, and social inclusion.
- Develop and execute capacity-building and cybersecurity skill programs for professionals and senior officials at public institutions.
- Develop and execute capacity-building and cybersecurity skill programs for professionals and executives in private organizations, with an emphasis on MSMEs (Micro, Small, and Medium-sized Enterprises).
- Develop and execute capacity-building and cybersecurity skill programs for professionals who oversee the protection of national critical infrastructures and essential service operators.
- Develop and execute capacity-building and cybersecurity skill programs for professionals at competent law enforcement authorities, including a victim-sensitive approach for online crimes, such as cyberbullying, online gender-based violence, and the online sexual abuse and exploitation of minors.
- Develop and execute capacity-building and cybersecurity skill programs for the general Costa Rican public, recognizing the differentiated and intersectional security needs of individuals and communities.

• Line of Action 4.2. Promote a Responsible Civic Culture of Cybersecurity

- Develop national awareness campaigns on comprehensive cybersecurity risk management, based on best practices and aimed at various stakeholders, with a gender focus and an intersectional perspective.
- Develop online tools and resources, such as tutorials, videos, and guides, to aid the Costa Rican public in acquiring and strengthening their cybersecurity skills.
- Create and implement an awareness program on cyber hygiene practices and the responsible use of technology for the general population, and particularly for children and adolescents.
- Disseminate information regarding the state of cybercrime at the national level, breaking down data based on the victim's profile, to inform and create specific strategies to address the challenges those profiles face.

• Line of Action 4.3. Promote Research, Development, and Innovation

- Establish and implement a program to boost intersectoral innovation and technological developments in cybersecurity, especially in the field of protection and resilience for national critical infrastructures.

- Conduct research studies on the safe development and adoption of new, emerging, and disruptive technologies, along with their impact on cybersecurity.

- Create and implement a plan to encourage the creation of new businesses, in partnership with business incubators and accelerators.

- Promote gender and intersectionality-based research and development in cybersecurity, to protect the individuals most vulnerable to specific types of cyberattacks.

PILLAR 5

COOPERATE IN THE DIGITAL ENVIRONMENT

MORE CYBER-INTEGRATED

Costa Rica will increase its national and international cooperation, collaboration, and information exchange on cybersecurity matters. This pillar emphasizes participation in international initiatives, alliances, and forums to address cross-border cyber threats and promote global cybersecurity standards.

• Line of Action 5.1. Strengthen Cybersecurity Cooperation, Collaboration, and Assistance Among Multiple Stakeholders at a National Level

- Promote the establishment of intergovernmental and intersectoral cooperation, collaboration, and assistance initiatives.
- Strengthen public sector alliances with the private sector, civil organizations, and academia.
- Establish specific cooperation mechanisms with operators of national critical infrastructures and essential service operators.

• Line of Action 5.2. Maximize the Benefits of managing International Cyber Cooperation

- Appoint within the Ministry of Foreign Affairs and Worship organizational responsibilities for foreign cyber affairs (a cyber ambassador or another dedicated office) and regularly report on country representation, the negotiation of international acts, the management of international cooperation and cyber-diplomacy at the policy/strategy level.
- Promote the establishment of relevant bilateral and/or multilateral international cooperation agreements and conventions on cybersecurity and the fight against cybercrime.
- Strengthen the participation of CSIRT-CR in regional and international incident response networks, such as the OAS/CICTE's CSIRTS Americas Network.
- Promote alliances with institutions from other branches of public power, especially with those governing bodies that act as a central authority or contact points within the country for various international cooperation conventions and treaties on cybersecurity and the fight against cybercrime.
- Establish cooperation mechanisms in the investigation and prosecution of cybercrimes with international security and justice agencies and/or organizations.
- Participate in joint and collaborative operations to dismantle cybercriminal networks and protect cybercrime victims.
- Participate in the discussion and development of international regulations addressing cybersecurity challenges and promoting a stable, secure, and trustworthy cyberspace, by understanding the impact of malicious cyber operations on vulnerable groups.
- Promote consideration of various gender and diversity aspects, as well as the active and effective participation of women in international debates on international security issues related to responsible governmental behavior in cyberspace, as well as the incorporation of the cyber component into state efforts to implement the United Nations Security Council Resolution 1325 on "Women, Peace, and Security."

5. PUBLIC INTERVENTIONS

Costa Rica will continue to advance its development and will utilize optimization opportunities to reinforce its strategy in combating cyberattacks, thereby fostering a stable and secure society and economy, by defining key areas for implementing its 2023-2027 National Cybersecurity Strategy.

Through the methodical execution of specific actions, Costa Rica aspires to maintain its leadership in ICT research and development, in addition to being a benchmark in training professionals specialized in cybersecurity and computer science. At the national level, cybersecurity can only be implemented through a multifaceted and diverse approach, thus ensuring simultaneous development of key areas to strengthen the country's cyber resilience.

Costa Rica, aware that cyber threats are a present reality and not a future risk, will allocate the necessary governmental resources to guarantee this strategy's success. Moreover, it will establish alliances with all relevant stakeholders to advance its objectives and goals. The government will promote a cybersecurity culture in the public sector and will encourage the allocation of resources for this purpose.

Below you will the public interventions, with regard to the strategic framework of the 2023-2027 National Cybersecurity Strategy.

Strategic Objective 1. Strengthen Cybersecurity Governance

Line of Action 1.1. Consolidate the National Cybersecurity Coordination Body

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
1	Roadmap to restructure the MICITT	Establish and launch a roadmap to restructure the MICITT, by consolidating and centralizing cybersecurity efforts and activities at the national level.	Implemented the roadmap to restructure the MICITT	0	Indicator goal for the period: 1 Indicator goal per year: 2024: 1 2025: 0 2026: 0 2027: 0	Entities' own resources	MICITT Support from MH and other Ministries	Financial Economic Operational Technological
2	National cybersecurity coordination body	Strengthen the national coordination body to direct the implementation of the 2023-2027 National Cybersecurity Strategy and carry out continuous monitoring, thus equipping it with legal and technical tools that allow it to perform its functions most effectively.	Number of new technical tools in operation at the National Cybersecurity Coordination Body	0	Indicator goal for the period: 8 Indicator goal per year: 2024: 2 2025: 2 2026: 2 2027: 2	Entities' own resources	MICITT Support from MH and other Ministries	Financial Operational Technological
3	Human resources for national cybersecurity coordination	Ensure that the national coordination body has a specialized, qualified, and technical team dedicated to cybersecurity actions that promote gender equality and diversity.	Number of people working at the national coordination body	4	Indicator goal for the period: 21 Indicator goal per year: 2024: 21 2025: 0 2026: 0 2027: 0	Entities' own resources	MICITT Support from MH, MCM, INAMU and other Ministries	Financial Operational

Strategic Objective 1. Strengthen Cybersecurity Governance

Line of Action 1.2. Establish a Whole-Society Cybersecurity Governance Framework

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
4	National Cybersecurity Governance Framework	Design and launch a national cybersecurity governance framework, promoting participation from multiple stakeholders, including national authorities and civil society organizations, and defend people's rights based on their diverse needs.	Administrative act to create the national cybersecurity governance framework	0	Indicator goal for the period: 1 Indicator goal per year. 2024: 1 2025: 0 2026: 0 2027: 0	International cooperation and entities' own resources	MICITT Support from CNSL, CISTE, MCM, INAMU, MREC and all Ministries	Political Financial Economic Operational Social
5	Cybersecurity strategic planning body	Renew the highest intergovernmental and intersectoral strategic planning body to guide cybersecurity management within the country, to promote gender equality and diversity.					MICITT Support from MP, MSP, MIDEPLAN, DIS, OIJ, UEI, SUTEL, MCM, INAMU, MREC	
6	Cybersecurity tactical planning body	Create tactical planning bodies to advise on the implementation of established and prioritized actions, taking into account cooperation with technological leaders and experts in the field.					MICITT Support from MP, MSP, MIDEPLAN, DIS, OIJ, UEI, SUTEL, MREC	
7	Dynamic coordination and collaboration mechanisms	Create and launch dynamic coordination, collaboration, and intergovernmental and intersectoral information exchange mechanisms that link multiple stakeholders.	Number of created and implemented intergovernmental and intersectoral coordination, collaboration, and information exchange mechanisms	0	Indicator goal for the period: 4 Indicator goal per year. 2024: 1 2025: 1 2026: 1 2027: 1	Entities' own resources	MICITT Support from MP, MREC and MIDEPLAN	Operative Social
8	Institutional liaison figures	Create a liaison figure (a person responsible for cybersecurity) at public institutions, in local governments, and in other organizations at the operational level.	Percentage of public organizations with cybersecurity liaison figures	0%	Indicator goal for the period: 100% Indicator goal per year. 2024: 25% 2025: 25% 2026: 25% 2027: 25%	Entities' own resources	MICITT Support from all public organizations	Financial Operative

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
9	Communication strategies, protocols, and mechanisms	Develop strategies, protocols, and communication mechanisms that promote participation from all stakeholders, especially from academia and the private sector, and that account for execution of the action plan.	Number of created and implemented communication mechanisms	0	Indicator goal for the period: 4 Indicator goal per year: 2024: 1 2025: 1 2026: 1 2027: 1	Entities' own resources	MICITT Support from MP, MREC and MIDEPLAN	Financial Operational Social
10	Monitoring and control mechanisms	Establish mechanisms for monitoring and controlling key performance indicators and comprehensive cybersecurity risk management, including indicators that contribute to measuring gender impact with an intersectional perspective.	Number of reports on compliance with key performance indicators and comprehensive cybersecurity risk management	0	Indicator goal for the period: 4 Indicator goal per year: 2024: 1 2025: 1 2026: 1 2027: 1	Entities' own resources	MICITT Support from MP, MCM, INAMU MREC and MIDEPLAN	Financial Operational Social
11	Socioeconomic impact assessments	Conduct socio-economic impact assessments regarding implementation of the 2023-2027 National Cybersecurity Strategy.	Number of socioeconomic impact evaluations regarding the implementation of the 2023-2027 National Cybersecurity Strategy	0	Indicator goal for the period: 1 Indicator goal per year: 2024: 0 2025: 0 2026: 0 2027: 1	Entities' own resources	MICITT Support from MP, MCM, INAMU, MREC and MIDEPLAN	Financial Operational Social

Strategic Objective 1. Strengthen Cybersecurity Governance
Line of Action 1.3. Efficiently Allocate Resources for the Implementation of Cybersecurity Initiatives

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
12	Roadmap for the transition to end the state of emergency	Establish and launch a roadmap for the transition to end the state of emergency declared by Executive Decree No. 43542-MP-MICITT of 2022	Implemented the roadmap for the transition to end the state of emergency	0	Indicator goal for the period: 1 Indicator goal per year: 2024: 1 2025: 0 2026: 0 2027: 0	Entities' own resources	MICITT Support from MH, CNE, MIDEPLAN, CGR, MREC	Geopolitical Political Financial Economic Operational Technological Emergent Social

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
13	Investment plan for cybersecurity initiatives	Develop an investment plan that ensures the availability and allocation of sufficient resources at public institutions, to carry out cybersecurity initiatives	Investment plan to allocate resources at public institutions, to carry out cybersecurity initiatives	0	Indicator goal for the period: 1 Indicator goal per year: 2024: 1 2025: 0 2026: 0 2027: 0	Entities' own resources	MICITT Support from MH, MREC and all public institutions	Financial Economic Operational Technological
14	Cybersecurity human resources at public institutions	Strengthen the capacity of public institutions by ensuring suitable human resources, promoting gender equality and diversity, and creating specialized cybersecurity job profiles.	Percentage of public institutions with human resources specifically dedicated to cybersecurity	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 25% 2025: 25% 2026: 25% 2027: 25%	Entities' own resources	MICITT Support from MCM, MREC, INAMU and all public institutions	Financial Operational Social
15	Annual budget at public institutions	Encourage public institutions to guarantee financial resources by annually budgeting those necessary for comprehensive cybersecurity risk management.	Percentage of public institutions aware of the importance of integrating into the budget the resources necessary to carry out cybersecurity initiatives	0%	Indicator goal for the period: 80% Indicator goal per year: 2024: 30% 2025: 30% 2026: 20% 2027: 0%	Entities' own resources	MICITT Support from all public institutions	Financial Operational Technological
16	Acquisition and purchase processes of technological resources at public institutions	Establish efficient processes for the acquisition and purchase of technological resources in public institutions, to ensure comprehensive cybersecurity risk management	Percentage of public institutions implementing processes to acquire and purchase technological resources for the comprehensive management of cybersecurity risks	0%	Indicator goal for the period: 80% Indicator goal per year: 2024: 0% 2025: 10% 2026: 30% 2027: 40%	Entities' own resources	MICITT Support from all public institutions	Financial Operational Technological

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
17	Private investment stimulus program	Promote the design of incentives for private sector investment in financing cybersecurity projects.	Number of programs implemented to stimulate private sector investment	0	Indicator goal for the period: 1 Indicator goal per year: 2024: 0 2025: 1 2026: 0 2027: 0	Entities' own resources	MICITT Support from MH, MEIC, MIDEPLAN, MREC	Financial Operational Technological

Strategic Objective 2. Adapting the Cyber Legal Framework

Line of Action 2.1. Strengthen the Cyber Legal and Regulatory Framework

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
18	Procedures for legislative initiatives or projects	Support the Legislative Assembly in processing initiatives or projects to adjust, adapt, and/or harmonize the legal framework, as related to cybersecurity.	Percentage of procedures for legislative initiatives or projects supported per year	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 100% 2025: 100% 2026: 100% 2027: 100%	Entities' own resources	MICITT MP support	Geopolitical Political Financial Economic Social
19	Processing initiatives or regulatory projects	Assist sectoral regulators in processing initiatives or projects to adapt, adjust, and/or harmonize the regulatory framework, as related to cybersecurity, as well as in exercising supervision and verification of compliance with sectoral regulatory framework provisions, as related to cybersecurity.	Percentage of regulatory initiatives or projects supported per year	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 100% 2025: 100% 2026: 100% 2027: 100%	Entities' own resources	MICITT Support from sector regulators	Financial Economic Operational
20	Review the cyber legal and regulatory framework	Thoroughly review and update the cyber legal and regulatory framework, emphasizing legal protections against gender-based cyber threats from an intersectional perspective, to prevent, sanction, and eradicate the gender violence that is facilitated by digital technologies.	Number of revisions to the cyber legal and regulatory framework	0	Indicator goal for the period: 2 Indicator goal per year: 2024: 0 2025: 1 2026: 0 2027: 1	Entities' own resources	MICITT Support from MCM, INAMU, DIS and UEI	Operational

Strategic Objective 2. Adapting the Cyber Legal Framework

Line of Action 2.2. Strengthen the Technical Regulatory Framework Related to Comprehensive Cybersecurity Risk Management

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
21	Regulatory mark of the CSIRT-CR	Update the regulatory framework to strengthen administrative and technical processes for the Computer Security Incident Response Center (CSIRT-CR).	Number of administrative acts (decrees, resolutions, or others) strengthening the CSIRT-CR	0	Indicator goal for the period: 2 Indicator goal per year: 2024: 1 2025: 1 2026: 0 2027: 0	International cooperation	MICITT	Financial Economic Operational Technological Emergent Social
22	Standards, protocols and technical procedures: Guides and Plan	Establish standards, protocols, and technical procedures for the prevention, containment, resolution, and response to national cybersecurity incidents, including: • Guidelines to evaluate inter-institutional ICT security programs. • Contingency plans for ICT security in the public sector. • Guidelines to reduce the impact and likelihood of ransomware and data extortion incidents in public and private organizations, including best international practices to prepare, prevent, and mitigate these incidents.	Number of established standards, protocols, and technical procedures	0	Indicator goal for the period: 10 Indicator goal per year: 2024: 3 2025: 3 2026: 2 2027: 2	International cooperation	MICITT	Operational Technological
23	Regulatory framework for the protection of national critical infrastructures and essential service operators	Develop a regulatory framework to protect national critical infrastructures and essential service operators, adopting international standards and norms, including: • A national protocol for the management of and response to cyber crises and emergencies. • Contingency and recovery plans for national critical infrastructures and essential services. • A manual for conducting national cybersecurity exercises and drills.	Number of technical standards specifically related to national critical infrastructure and established essential service operators	0	Indicator goal for the period: 6 Indicator goal per year: 2024: 2 2025: 2 2026: 1 2027: 1	International cooperation	MICITT	Operational Technological

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
24	Compliance supervision mechanisms	Promote compliance with the technical regulatory framework, as related to comprehensive cybersecurity risk management.	Percentage of public institutions complying with the technical regulatory framework, as related to comprehensive cybersecurity risk management	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 25% 2025: 25% 2026: 25% 2027: 25%	Entities' own resources	MICITT Support from sectoral regulators SUTEL	Operational

Strategic Objective 3. Strengthen Infrastructure Protection and National Cyber Resilience

Line of Action 3.1. Adopt a Framework for Comprehensive Cybersecurity Risk Management

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
25	Comprehensive Cybersecurity Risk Management Framework	Develop a comprehensive cybersecurity risk management framework at the national level, incorporating a gender perspective with an intersectional approach to protect the rights of individuals, based on their diverse needs.	Developed a comprehensive cybersecurity risk management framework	0	Indicator goal for the period: 1 Indicator goal per year: 2024: 0 2025: 0 2026: 1 2027: 0	International cooperation	MICITT Support from MIDEPLAN, MCM, INAMU	Operational Technological Social
26	Monitoring processes and periodic review of the implementation of the comprehensive risk management framework	Establish periodic monitoring and review processes for implementing the comprehensive cybersecurity risk management framework, while adapting it to new threats, vulnerabilities, and trends in cybersecurity.	Percentage of public institutions implementing the comprehensive cybersecurity risk management framework	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 0% 2025: 0% 2026: 50% 2027: 50%	Entities' own resources	MICITT Support from MIDEPLAN and OIJ	Operational Technological
27	Integration of cybersecurity risk management into institutional processes	Ensure that cybersecurity risk management processes and information security risk management are integrated into the strategic, operational, and budgetary planning processes at public institutions.	Process of integrating cybersecurity risk management into institutional processes	0	Indicator goal for the period: 1 Indicator goal per year: 2024: 2025: 0 2026: 0 2027: 1	Entities' own resources	MICITT MIDEPLAN support	Operational Technological

Strategic Objective 3. Strengthen Infrastructure Protection and National Cyber Resilience

Line of Action 3.2. Strengthen National Capabilities for Monitoring, Detecting, and Responding to Cybersecurity Incidents

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
28	CSRT-CR Capacity Building Plan	Create and execute a plan to strengthen operational, administrative, human, scientific, and physical infrastructure capabilities for the Computer Security Incident Response Center (CSIRT-CR), to strengthen the same as a national team for cybersecurity incident response.	CSIRT-CR capacity strengthening plan Implemented	0	Indicator goal for the period: 1 Indicator goal per year: 2024: 0 2025: 1 2026: 0 2027: 0	International cooperation	MICITT	Financial Economic Operational Technological
29	Security Operations Center (SOC) Solution	Provide a Security Operations Center (SOC) solution to monitor, detect, and respond to cybersecurity incidents at prioritized public institutions.	Percentage of progress regarding the implementation of the Security Operations Center (SOC) solution	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 100% 2025: 0% 2026: 0% 2027: 0%	International cooperation	MICITT Support from prioritized public institutions	Financial Operational Technological
30	Prioritized public institutions	Provide prioritized public institutions with technological solutions for threat detection and prevention.	Percentage of prioritized public institutions connected to the Security Operations Center (SOC) solution	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 100% 2025: 0% 2026: 0% 2027: 0%	International cooperation	MICITT Support from prioritized public institutions	Financial Operational Technological
31	Permanent National Security Operations Center (SOC-CR)	Create and launch a permanent national Security Operations Center (SOC-CR) that is responsible for preventive, reactive, and proactive cybersecurity risk management at the national level.	Percentage of progress in the implementation and launch of the permanent national Security Operations Center (SOC-CR)	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 30% 2025: 70% 2026: 0% 2027: 0%	International cooperation	MICITT Support from prioritized public institutions	Financial Operational Technological

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
32	Advanced intersectoral alert and response systems	Implement advanced intersectoral alert and response systems for cybersecurity incidents at prioritized public institutions.	Percentage of prioritized public institutions with implemented advanced intersectoral alert and response systems	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 70% 2025: 30% 2026: 0% 2027: 0%	International cooperation	MICITT Support from prioritized public institutions	Financial Operational Technological
33	Strategy to promote sectoral SOC	Create and execute a strategy to promote the creation and strengthening of sectoral SOCs.	Number of new sectors with SOCs that were created and launched	0	Indicator goal for the period: 3 Indicator goal per year: 2024: 1 2025: 1 2026: 1 2027: 0	International cooperation	MICITT Support from prioritized public institutions	Financial Operational Technological

Strategic Objective 3. Strengthen Infrastructure Protection and National Cyber Resilience

Line of Action 3.3. Protect and Defend National Critical Infrastructure and Essential Service Operators

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
34	Criteria for designating national critical infrastructures	Define and periodically evaluate the criteria for designating national critical infrastructures, taking into account the human rights protections for individuals, based on their diverse needs.	Technical document on the criteria to designate national critical infrastructures and essential services prepared	0%	Indicator goal for the period: 1 Indicator goal per year: 2024: 1 2025: 0 2026: 0 2027: 0	International cooperation	MICITT Support from MCM, INAMU and all operators that exercise control over national critical infrastructures and provide essential services	Operational Technological

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
35	Identification of national critical infrastructure operators that provide essential services	Periodically evaluate the designation of national critical infrastructures based on defined technical criteria.	Number of evaluations to designate national critical infrastructure and essential services carried out	0	Indicator goal for the period: 3 Indicator goal per year: 2024: 0 2025: 1 2026: 1 2027: 1	International cooperation	MICITT Support of all operators that exercise control over national critical infrastructure and provide essential services	Operational Technological
36	Catalog of national critical infrastructures	Identify, categorize, and update national critical infrastructures and essential service operators.	Number of updates to the catalog of national critical infrastructures and essential service operators carried out	0	Indicator goal for the period: 3 Indicator goal per year: 2024: 0 2025: 1 2026: 1 2027: 1	International cooperation	MICITT Support of all operators that exercise control over national critical infrastructure and provide essential services	Operational Technological
37	National Critical Infrastructure Cybersecurity Risk Assessments	Promote the development of cybersecurity risk assessments on national critical infrastructures, in conjunction with essential service operators.	Percentage of cybersecurity risk assessments carried out for national critical infrastructures and essential services	0%	Indicator goal for the period: 80% Indicator goal per year: 2024: 0% 2025: 20% 2026: 30% 2027: 30%	International cooperation	MICITT Support of all operators that exercise control over national critical infrastructure and provide essential services	Operational Technological
38	National cybersecurity exercises and drills	Coordinate national cybersecurity exercises and drills to test preparedness for the operators of national critical infrastructures and essential services.	Number of executed national cybersecurity exercises and drills	1	Indicator goal for the period: 8 Indicator goal per year: 2024: 2 2025: 2 2026: 2 2027: 2	International cooperation	MICITT Support of all operators that exercise control over national critical infrastructure and provide essential services	Financial Operational Technological

Strategic Objective 3. Strengthen Infrastructure Protection and National Cyber Resilience
Line of Action 3.4. Strengthen the Processing of Information Related to Cybersecurity Incidents

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
39	National Registry of Cybersecurity Incidents	Create a National Cybersecurity Incident Registry, emphasizing reporting for cybersecurity incidents at national critical infrastructures.	Percentage of public institutions that report cybersecurity incidents to the National Registry	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 10% 2025: 20% 2026: 30% 2027: 40%	International cooperation	MICITT Support from all public institutions	Operational Technological
40	Efficient mechanisms for the processing of cybersecurity incident information	Establish efficient mechanisms to ensure the proper processing, management, storage, sharing, and information exchange regarding cybersecurity incidents among multiple stakeholders, including the application of industry-recommended standards and participation in regional and international networks, such as the OAS/CICTE's CSIRT Americas Network.	Percentage of public institutions using mechanisms to process information on cybersecurity incidents	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 0% 2025: 20% 2026: 40% 2027: 40%	Entities' own resources	MICITT Support from all public institutions	Operational Technological
41	Notification mechanism to competent law enforcement authorities	Create and implement a notification mechanism for law enforcement authorities.	Percentage of public institutions using the mechanism to notify competent law enforcement authorities	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 0% 2025: 20% 2026: 40% 2027: 40%	Entities' own resources	MICITT Support from all public institutions	Operational Technological
42	Notification mechanism for affected individuals or organizations	Create and implement a notification mechanism for individuals and/or organizations affected by cybersecurity incidents.	Percentage of public institutions using the notification mechanism for affected individuals or organizations	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 0% 2025: 20% 2026: 40% 2027: 40%	Entities' own resources	MICITT Support from all public institutions	Operational Technological

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
43	Cybersecurity risk information disclosure mechanism	Disseminate timely and reliable information regarding cybersecurity risks affecting Costa Rican society, highlighting those that are due to gender and other intersectionalities.	Number of reports disclosed on cybersecurity risks that affect Costa Rican society	0	Indicator goal for the period: 8 Indicator goal per year: 2024: 2 2025: 2 2026: 2 2027: 2	Entities' own resources	MICITT Support from MCM, INAMU	Operational Technological Social

Strategic Objective 4. Strengthen the Capabilities of the Cybersecurity Ecosystem

Line of Action 4.1. Improve and Expand Cyber Capabilities and Skills, at All Levels, based on a Human-Centric and Gender-Based Approach with an Intersectional Perspective

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
44	National cybersecurity education and training plan	Develop and implement a national cybersecurity education and training plan across all levels of the Costa Rican educational system, promoting a curriculum that includes cybersecurity content and promotes diversity, gender equality, and social inclusion.	Developed a national cybersecurity education and training plan	0	Indicator goal for the period: 1 Indicator goal per year: 2024: 1 2025: 0 2026: 0 2027: 0	International cooperation	MEP Support from MICITT, MCM, INAMU, MNA, MDHIS, MCJ, INA, Academia	Financial Economic Operational Social
45	National Cybersecurity Workforce Development Strategy	Formulate and implement a national cybersecurity workforce development strategy, to address labor market needs and cybersecurity trends, as well as to promote diversity, gender equality, and social inclusion.	Formulated Cybersecurity Workforce Development Strategy	0	Indicator goal for the period: 1 Indicator goal per year: 2024: 1 2025: 0 2026: 0 2027: 0	International cooperation	MICITT Support from MICITT, MCM, INAMU, MNA, MDHIS, MCJ, INA, Academia	Financial Economic Operational Social
46	Training programs for the public sector	Develop and execute capacity-building and cybersecurity skill programs for professionals and senior officials at public institutions.	Percentage of people at public institutions trained in cybersecurity (including in the metrics that promote diversity, gender equality, and social inclusion)	0%	Indicator goal for the period: 50% Indicator goal per year: 2024: 10% 2025: 10% 2026: 15% 2027: 15%	Entities' own resources	MICITT Support from MEP, INA, Academia and all public institutions	Operational Social

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
47	Training programs for the private sector	Develop and execute capacity-building and cybersecurity skill programs for professionals and executives in private organizations, with an emphasis on MSMEs (Micro, Small, and Medium-sized Enterprises).	Number of people in private organizations trained in cybersecurity (including in the metrics that promote diversity, gender equality, and social inclusion)	0	Indicator goal for the period: 2,000 Indicator goal per year: 2024: 200 2025: 300 2026: 500 2027: 1,000	Entities' own resources	MICITT Support from MEP, INA, Academia	Operational Social
48	Training programs for national critical infrastructures	Develop and execute capacity-building and cybersecurity skill programs for professionals who oversee the protection of national critical infrastructures and essential service operators.	Percentage of professionals who protect national critical infrastructures and trained essential service operators (including the metrics that promote diversity, gender equality, and social inclusion)	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 20% 2025: 25% 2026: 25% 2027: 30%	Entities' own resources	MICITT Support for MEP and all operators that exercise control over national critical infrastructures and provide essential services	Operational Technological
49	Training programs for the law enforcement sector	Develop and execute capacity-building and cybersecurity skill programs for professionals, as given by competent law enforcement authorities, and to include a victim-sensitive approach for online crimes, such as cyberbullying, online gender-based violence, and the online sexual abuse and exploitation of minors.	Percentage of professionals at competent law enforcement authorities (including in the metrics that promote diversity, gender equality, and social inclusion)	0%	Indicator goal for the period: 70% Indicator goal per year: 2024: 10% 2025: 20% 2026: 20% 2027: 20%	Entities' own resources	MICITT Support MEP, MCM, INAMU and all law enforcement authorities	Operational Technological

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
50	Citizen training programs	Develop and execute capacity-building and cybersecurity skill programs for the general Costa Rican public, recognizing the differentiated and intersectional security needs of individuals and communities.	Number of people who participate in spaces to strengthen cybersecurity (including the metrics that promote diversity, gender equality, and social inclusion)	4.429	Indicator goal for the period: 31.000 Indicator goal per year: 2024: 5,693 2025: 6,959 2026: 8,857 2027: 9,491	Entities' own resources	MICITT Support from MEP, MTSS, MCM, INAMU, MNA, MDHIS, MCJ	Operational Social

Strategic Objective 4. Strengthen the Capabilities of the Cybersecurity Ecosystem

Line of Action 4.2. Promote a Responsible Civic Culture of Cybersecurity

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
51	National awareness campaigns	Develop national awareness campaigns on comprehensive cybersecurity risk management, based on best practices and aimed at various stakeholders, with a gender focus and an intersectional perspective.	Number of executed national awareness campaigns on comprehensive cybersecurity risk management	1	Indicator goal for the period: 4 Indicator goal per year: 2024: 1 2025: 1 2026: 1 2027: 1	International cooperation	MICITT Support from MEP, MTSS, MCM, INAMU, MNA, MDHIS, MCJ, INA, Academia	Operational Social
52	Online awareness tools and resources	Develop online tools and resources, such as tutorials, videos, and guides, to aid the Costa Rican public in acquiring and strengthening their cybersecurity skills.	Number of people using online tools and resources to acquire and strengthen cybersecurity skills (including the metrics that promote diversity, gender equality, and social inclusion)	0	Indicator goal for the period: 7,000 Indicator goal per year: 2024: 1,000 2025: 1,500 2026: 2,000 2027: 2,500	International cooperation	MICITT Support from MEP, MTSS, MCM, INAMU, MNA, MDHIS, MCJ	Operational Social

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
53	Awareness program on cyber hygiene and responsible use of technologies	Create and implement an awareness program on cyber hygiene practices and the responsible use of technology for the general population, and particularly for children and adolescents.	Number of executed national awareness campaigns on cyber hygiene practices and the responsible use of technology	0	Indicator goal for the period: 4 Indicator goal per year: 2024: 1 2025: 1 2026: 1 2027: 1	Entities' own resources	MICITT Support from MEP, MTSS, MCM, INAMU, MNA, MDHIS, MCJ, INA, Academia	Operational Social
54	Disclosure mechanisms on the status of cybercrime	Disseminate information regarding the state of cybercrime at the national level, breaking down data based on the victim's profile, to inform and create specific strategies to address the challenges those profiles face.	Number of published reports on the state of cybercrime at the national level	0	Indicator goal for the period: 8 Indicator goal per year: 2024: 2 2025: 2 2026: 2 2027: 2	Entities' own resources	MICITT Support from OIJ, MCM and INAMU	Operational Social

Strategic Objective 4. Strengthen the Capabilities of the Cybersecurity Ecosystem
Line of Action 4.3. Promote Research, Development, and Innovation

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
55	Program to promote innovation and technological development	Establish and implement a program to boost intersectoral innovation and technological developments in cybersecurity, especially in the field of protection and resilience for national critical infrastructures.	Number of projects to promote innovation and intersectoral technological development in cybersecurity identified	0	Indicator goal for the period: 6 Indicator goal per year: 2024: 1 2025: 1 2026: 2 2027: 2	Entities' own resources	MICITT Support from MH and all operators that exercise control over national critical infrastructure and provide essential services	Financial Operational Technological

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
56	Research studies in the development and safe adoption of new emerging and disruptive technologies	Conduct research studies on the safe development and adoption of new, emerging, and disruptive technologies, along with their impact on cybersecurity.	Number of research studies on the development and the safe adoption of new emerging and disruptive technologies prepared	0	Indicator goal for the period: 4 Indicator goal per year. 2024: 1 2025: 1 2026: 1 2027: 1	International cooperation	MICITT Support from INA, Academia	Financial Operational Technological Emergent
57	Promotion plan for the creation of new companies	Create and implement a plan to encourage the creation of new businesses, in partnership with business incubators and accelerators.	Number of companies created under the implemented plan to promote the creation of new companies	0	Indicator goal for the period: 20 Indicator goal per year. 2024: 5 2025: 5 2026: 5 2027: 5	Entities' own resources	MICITT Support from MH and MEIC	Financial Operational Technological
58	Studies to promote research and development	Promote gender and intersectionality-based research and development in cybersecurity, to protect the individuals most vulnerable to specific types of cyberattacks.	Number of studies to promote research and development in cybersecurity prepared	0	Indicator goal for the period: 2 Indicator goal per year. 2024: 0 2025: 1 2026: 0 2027: 1	Entities' own resources	MICITT Support from MCM, INAMU, MNA, MDHIS, MCJ	Operational Technological Social

Strategic Objective 5. Cooperate in the Digital Environment

Line of Action 5.1. Strengthen Cybersecurity Cooperation, Collaboration, and Assistance Among Multiple Stakeholders at a National Level

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
59	Intergovernmental and intersectoral cooperation, collaboration and assistance initiatives	Promote the establishment of intergovernmental and intersectoral cooperation, collaboration, and assistance initiatives.	Number of signed initiatives for intergovernmental and intersectoral cooperation, collaboration, and assistance	0	Indicator goal for the period: 6 Indicator goal per year. 2024: 1 2025: 1 2026: 2 2027: 2	Entities' own resources	MICITT Support from public institutions	Operational Technological

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
60	Alliances with the private sector, civil society organizations and academia	Strengthen public sector alliances with the private sector, civil organizations, and academia.	Number of signed alliances with the private sector, civil society organizations, and academia	0	Indicator goal for the period: 4 Indicator goal per year: 2024: 1 2025: 1 2026: 1 2027: 1	Entities' own resources	MICITT Support from MEP, MEIC	Operational Technological
61	Cooperation mechanisms with national critical infrastructure operators	Establish specific cooperation mechanisms with operators of national critical infrastructures and essential service operators.	Percentage of operators that exercise control over national critical infrastructure and provide essential services using the established cooperation mechanism	0%	Indicator goal for the period: 100% Indicator goal per year: 2024: 0% 2025: 20% 2026: 30% 2027: 50%	Entities' own resources	MICITT Support of all operators that exercise control over national critical infrastructure and provide essential services	Operational Technological

Strategic Objective 5. Cooperate in the Digital Environment

Line of Action 5.2. Maximize the Benefits of managing International Cyber Cooperation

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
62	Head of cyber-diplomacy	Appoint within the Ministry of Foreign Affairs and Worship organizational responsibilities for foreign cyber affairs (a cyber ambassador or another dedicated office) and regularly report on country representation, the negotiation of international acts, the management of international cooperation and cyber-diplomacy at the policy/strategy level.	Number of reports on the state of international cooperation at the political/strategic level	0	Indicator goal for the period: 6 Indicator goal per year: 2024: 0 2025: 2 2026: 2 2027: 2	Entities' own resources	MREC Support from MP and MICITT	Geopolitical Political Operational

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
63	Bilateral and/ or multilateral international cooperation conventions and agreements	Promote the establishment of relevant bilateral and/or multilateral international cooperation agreements and conventions on cybersecurity and the fight against cybercrime.	Number of signed bilateral and/ or multilateral international cooperation conventions and agreements	0	Indicator goal for the period: 4 Indicator goal per year: 2024: 1 2025: 1 2026: 1 2027: 1	Entities' own resources	MREC Support from MP, MICITT, OIJ and entities that govern as central authority or contact points in the country for various international cooperation agreements and treaties	Geopolitical Political Operational
64	Strengthening the participation of the CSIRT-CR in international networks	Strengthen the participation of CSIRT-CR in regional and international incident response networks, such as the OAS/ CICTE's CSIRTS Americas Network.	Number of events with regional and international CSIRT networks	0	Indicator goal for the period: 8 Indicator goal per year: 2024: 2 2025: 2 2026: 2 2027: 2	Entities' own resources	MICITT Support from MREC	Operational Technological Emergent
65	Alliances with institutions from other branches of public power regarding international cooperation	Promote alliances with institutions from other branches of public power, especially with those governing bodies that act as a central authority or contact points within the country for various international cooperation conventions and treaties on cybersecurity and the fight against cybercrime.	Number of alliances signed with institutions from other branches of public power that govern as central authorities or contact points in the country for various international cooperation agreements and treaties on cybersecurity and the fight against cybercrime	0	Indicator goal for the period: 8 Indicator goal per year: 2024: 2 2025: 2 2026: 2 2027: 2	Entities' own resources	MICITT Support from MP, MREC and entities that govern as central authority or contact points in the country for various international cooperation agreements and treaties	Political Operational

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
66	Cooperation mechanisms with international security and justice organizations	Establish cooperation mechanisms in the investigation and prosecution of cybercrimes with international security and justice agencies and/or organizations.	Number of established, created, and implemented cooperation mechanisms to investigate and prosecute cybercrimes	0	Indicator goal for the period: 4 Indicator goal per year: 2024: 1 2025: 1 2026: 1 2027: 1	Entities' own resources	MICITT Support from all public institutions	Political Operational
67	Country participation in international operations	Participate in joint and collaborative operations to dismantle cybercriminal networks and protect cybercrime victims.	Number of reports that result in joint and collaborative operations to dismantle cybercriminal networks and to protect victims of cybercrimes	0	Indicator goal for the period: 4 Indicator goal per year: 2024: 1 2025: 1 2026: 1 2027: 1	Entities' own resources	MICITT Support from MP, MREC and OIJ	Geopolitical Operational Technological
68	Country participation in discussion and development of international regulations	Participate in the discussion and development of international regulations addressing cybersecurity challenges and promoting a stable, secure, and trustworthy cyberspace, by understanding the impact of malicious cyber operations on vulnerable groups.	Number of international events attended for the discussion and development of international regulations that address cybersecurity challenges and promote a stable, secure, and reliable cyberspace	0	Indicator goal for the period: 4 Indicator goal per year: 2024: 1 2025: 1 2026: 1 2027: 1	Entities' own resources	MREC Support from MP and MICITT	Geopolitical Political Operational

#	Public Intervention	Objective	Indicator	Base Line	Goal	Required Resources	Responsible	Risks
69	Country participation on responsible behavior of States and implementation of Resolution 1325	Promote consideration of various gender and diversity aspects, as well as the active and effective participation of women in international debates on international security issues related to responsible governmental behavior in cyberspace, as well as the incorporation of the cyber component into state efforts to implement the United Nations Security Council Resolution 1325 on "Women, Peace, and Security."	Number of international events attended on international security issues related to the responsible behavior of States in cyberspace and the incorporation of the cyber component in State efforts to implement Resolution 1325	0	Indicator goal for the period: 4 Indicator goal per year: 2024: 1 2025: 1 2026: 1 2027: 1	Entities' own resources	MREC Support from MP and MICITT	Geopolitical Political Operational

SIGLAS:

MP	Ministry of the Presidency
MREC	Ministry of Foreign Affairs and Worship
MH	Ministry of Finance
MSP	Ministry of Public Security
MJP	Ministry of Justice and Peace
MEP	Ministry of Public Education
MOPT	Ministry of Public Works and Transport
MEIC	Ministry of Economy, Industry and Commerce
MAG	Ministry of Agriculture and Livestock
MS	Ministry of Health
MTSS	Ministry of Labor and Social Security
MCJ	Ministry of Culture and Youth
CNSL	National Online Safety Commission
INAMU	National Institute of Women
SUTEL	Superintendency of Telecommunications
CNE	National Emergency Commission

OIJ	Judicial Investigation Organization – Judicial Branch
MIDEPLAN	Ministry of National Planning and Economic Policy
MINAE	Ministry of Environment and Energy
MIVAH	Ministry of Housing and Human Settlements
MCE	Ministry of Foreign Trade
MICITT	Ministry of Science, Technology and Telecommunications
MT	Ministry of Tourism
MDR	Ministry of Sports and Recreation
MC	Ministry of Communication
MDHIS	Ministry of Human Development and Social Inclusion
MCM	Ministry of the Status of Women
MCSP	Ministry of Coordination with the Private Sector
MNA	Ministry of Children and Adolescents
CISTE	Interinstitutional Council on Terrorism
DIS	Intelligence and Security Directorate
UEI	Special Intervention Unit
CGR	Comptroller General of the Republic

6. MONITORING, EVALUATION, AND RISK MANAGEMENT

Monitoring on the physical and budgetary execution of the proposed actions to achieve the Strategic Objectives will be carried out through an Action Plan. This plan indicates the entities responsible for each action, the execution periods for these actions, the necessary and available resources to carry them out, and the significance of each action in the fulfillment of both the general purpose and the specific objectives under each pillar of the Strategy.

The National Cybersecurity Coordination entity will carry out quarterly activities to monitor and evaluate implementation of the Strategy and will present annual reports to the highest intergovernmental and intersectoral strategic planning entity.

Costa Rica will monitor the various stakeholders, assessing both their cybersecurity maturity level and evaluating capabilities, to ensure continuous improvement, emphasizing the short and medium-term. Additionally, support will be given to develop audits on the processes carried out by public institutions and the development of comparative efficiency exercises based on the collection and analysis of statistically relevant information at the national level, as well as in the preparation of situational reports on the state of cybersecurity.

Lastly, it is also expected that the Strategy will be reviewed and updated every year or as necessary.

The key performance indicators will be monitored and evaluated by the National Cybersecurity Coordination entity on a quarterly basis, and annual reports will be presented to the highest intergovernmental and intersectoral strategic planning entity.

7. SOCIAL AND CITIZEN PARTICIPATION

Construction of the 2023-2027 National Cybersecurity Strategy is based on the analysis of fundamental inputs provided by all the various stakeholders in Costa Rica. These inputs allow for the creation of a proposal that is submitted for consideration through a Public Consultation process. During this process, stakeholders presented their considerations within a reasonable time frame; these were then reviewed and addressed by the national government.

8. DISCLOSURE

In accordance with the provisions of the 2023-2026 National Development and Public Investment Plan (PNDIP) (MIDEPLAN, 2023a), this National Strategy is aimed at both internal audiences (state institutions) and external audiences (all those who have a particular interest in the importance and relevance of cybersecurity).

The tools and mechanisms available via the MICITT (press releases, website, social networks, forums and lectures in various areas, workshops and dialogues, and documentation centers and media, among others) will be used to disseminate the 2023-2027 National Cybersecurity Strategy, in order to facilitate transparency and accountability to the Costa Rican citizenry.

9. GLOSSARY

Below you will find some definitions:

Cluster: These are groups of servers that are managed together and participate in workload management. A cluster can contain nodes or individual application servers.

Computer System or Information System: Any system, device, equipment, network, or isolated asset, or a combination of the same, that is interconnected or related to another, including its software, whose function, or that of any of its elements, is the collection, the storage, use, exchange, dissemination, transmission, elimination or, in general, the processing of information, in the execution of a program.

Confidentiality: Preserve authorized restrictions on access to and disclosure of information, including means to protect personal privacy and restricted, limited, and/or proprietary information.

Critical Information Infrastructure: These are the assets, systems, and networks, whether physical or virtual, whose incapacity or destruction would have a negative effect.

Critical Information Infrastructure Operator: These are all organizations or entities that operate physical or virtual systems, which offer essential services to support basic systems at a social, educational, economic, environmental, and/or political level.

Critical Infrastructure: IT systems and assets, whether physical or virtual, so vital to society that their incapacity or destruction can have a debilitating impact on security, the economy, public health or safety, the environment or any combination of these issues.

Cyber Threats: Refers to any potential malicious attack that seeks to illegally access data, disrupt digital operations, or damage information.

Cyberattack: These are unwanted attempts to steal, expose, alter, disable or destroy information through unauthorized access to computer systems.

Cybercrime: This is a criminal activity that targets a computer, a computer network, or a networked device, or that uses one of these elements.

Cybersecurity: This is the ability to protect or defend the use of cyberspace from cyber-attacks.

Cybersecurity Incident: Digital or physical breach that threatens the privacy, restricted access, integrity, and/or availability of an organization's sensitive or restricted, as well as confidential, information systems or personal data. Incidents range from intentional cyberattacks by hackers or unauthorized users to unintentional security policy violations by authorized legitimate users.

Cybersecurity Incident Management: Action in response to cybersecurity incidents, implementing the necessary controls and mechanisms for their monitoring and identification, as well as the lines of action to follow.

Cybernetics: This is the science that relates the inputs and outputs of a system.

Cyberspace: This is the complex environment resulting from the interaction of people, software, and services on the Internet, via technological devices and the networks connected to them; it does not exist in any physical form.

Cybercrime: This is the illicit act in which Information and Communication Technologies, such as computer, electronic, or technological resources, or the Internet, among others, are used as a means or as an end to carry them out. That is, computers, smartphones, software, etc. are used in the commission of these crimes, such as the falsification of documents through a computer or destruction of information contained in a computer.

Cybersecurity Standards: These are the techniques generally established in published materials that seek to establish best practices to prevent, detect, and respond to cybersecurity threats, to protect the cyber environment of a user or organization in order to reduce risks, including prevention or cyberattack mitigation.

Digital Risks: This is the possibility that a threat or vulnerability escalates to real damage to the company, resulting in a loss or theft of information or a stoppage of its activity as a consequence of the damage caused.

Digital Transformation: Digital transformation is the process of completely replacing manual, traditional, and/or legacy methods of doing business with the latest digital alternatives. This type of reinvention touches on all aspects of a business, not just technology.

Essential Services: Any service, as provided by the State or by private companies, with respect to which the impairment, degradation, denial of service, interception, interruption, non-availability, and/or destruction of its information infrastructure may seriously affect: life or physical integrity of people; the provision of services, being these health, security, energy, water supply, education, or telecommunications; and the normal functioning of road infrastructure and means of transportation, to the general population of users or clients, for those systems necessary for financial, banking, payment methods, and/or transactions that allow the transaction of money or securities; or in general, the normal development and well-being of the population.

Gender: A set of socially constructed values that define the different characteristics (emotional, affective, intellectual, or physical) and behaviors that each society assigns to men or women. Unlike sex, which is determined at birth, gender is learned and can be modified (INAMU, 2018).

Gender Equality: Refers to the existence of a "floor from which women can be recognized as equals and be treated normatively as equals, not in the sense of identity, but in the axiological sense: each person is worth the same as any other." Each woman is worth the same as another woman and each man, while each man is worth the same as each man and each woman. This is the principle of the equal worth of people, which is one of the fundamental universal human rights (MIDEPLAN, 2017a)

Gender Perspective: This allows us to focus, analyze and understand the characteristics that define women and men specifically, as well as their similarities and differences. From this perspective, the vital possibilities of each person are analyzed – the meaning of their lives, their expectations and opportunities, and the complex and diverse social relationships that exist between both genders. (MIDEPLAN, 2017a)

Incident: An event that does or potentially results in adverse consequences or adverse effects that represents a threat to an information system or the information that the system processes, stores, or transmits, and that may require a response action to mitigate the consequences.
Incident Response: Activities that address the direct short-term effects of an incident and can also support short-term recovery.

Information: Organized set of processed data.

Infrastructure: Assets of an essential and indispensable nature, whose operation is essential and does not allow alternative solutions, so its disruption or destruction would have a serious impact on essential services.

Intersectional Perspective: The intersectional perspective identifies a system of diverse and interconnected oppressions, including gender but also including issues such as race, religion, and class, which sometimes creates complex social, economic, and other hierarchies between the people who comprise a society (APC, 2022).

Malware: Malicious software that can renders infected systems useless. Most malware variants destroy data by deleting or wiping files critical to the operating system's ability to run.

Phishing: This is an attempt to steal users' credentials or confidential data, such as credit card numbers. In this case, scammers send users emails or text messages designed to look like they come from a legitimate source, using fake hyperlinks.

Ransomware: This is sophisticated malware that exploits system weaknesses and uses strong encryption to hold data or system functionality hostage.

Regulated Sector: Represents some strategic economic activity for the country, which is subject to the supervision of a regulator or sectoral inspector.

Resilience: The ability of an organization to resist an adverse situation, such as a cybersecurity incident. Business resilience should be accompanied by a contingency and continuity plan to deal with possible crisis situations at the company.

Risk: A measure of the degree to which an entity is threatened by a potential circumstance or event, and typically, a function of the adverse impacts that would arise if the circumstance or event occurred; and the probability of occurrence.

Sector Regulator: Public entity within whose main functions is the regulation and/or supervision of one or more specific regulated sectors.

Security Control: These are protective security mechanisms that range from access to data and systems, to device management and network protections.

Security Operations Center (SOC): A team specifically qualified in cybersecurity and with the necessary tools to conveniently analyze, investigate and support possible corporate cybersecurity events. An SOC can be external or internal, and its goal is to avoid and mitigate possible attacks on the company, constituting what we could call countermeasures against a cyber-attack.

Security Vulnerability: Weakness or failure of a system and that can be exploited for malicious purposes.

Source Code: Set of instructions that a system must follow and that is written by programmers, in one or more programming languages so that it is understandable by people.

Technical Alerts: Their objective is to communicate to a user information regarding the occurrence of events of interest in a computer system.

Vulnerability Scanning: The process of identifying network systems that have known or identified vulnerabilities, such as exploits, flaws, security gaps, insecure access entry points, and/or system configuration errors.

10. BIBLIOGRAPHIC REFERENCES

APC. (2022). *A Framework for Developing Gender-Responsive Cybersecurity Policy - Norms, Standards and Guidelines.* Obtenido de https://www.apc.org/sites/default/files/gender-cybersecurity-policy-norms.pdf

APC. (2023). *What is a gender approach to cybersecurity?* Obtenido de https://www.apc.org/en/pubs/apc-policy-explainer-what-gender-approach-cybersecurity

CEPAL. (2022). *Digitalización de las mujeres en América Latina y el Caribe. Acción urgente para una recuperación transformadora y con igualdad.* Obtenido de https://repositorio.cepal.org/bitstream/handle/11362/47940/4/S2200375_es.pdf

CGR. (2023). *Opiniones y sugestiones: Emergencia Cibernética: obstáculo para la transformación digital y el bienestar social; retroceso para la transparencia y la rendición de cuentas*. Obtenido de https://sites.google.com/cgr.go.cr/rchp/ma2022/dfoe-cap-os-00001-2023?authuser=0

CHATHAM HOUSE. (2023). *Understanding gender and cybersecurity.* Obtenido de https://www.chathamhouse.org/about-us/our-departments/international-security-programme/understanding-gender-and-cybersecurity

CNE. (2022). *Plan General de la Emergencia Ciberataques*. Obtenido de https://www.cne.go.cr/recuperacion/declaratoria/planes/Plan%20General%20de%20la%20Emergencia%20por%20Ciberataques.pdf

e-Governance Academy. (2023). *National Cyber Security Index Project.* Obtenido de https://ncsi.ega.ee/ncsi-index/

FORTINET. (2022). *2022 Cybersecurity Skills Gap - Global Research Report*. Obtenido de https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

FORTINET. (2023). *Fortinet informa que América Latina fue el objetivo de más de 360 mil millones de intentos de ciberataques en 2022.* Obtenido de https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent

GARTNER. (2023). *Top Strategic Cybersecurity Trends for 2023*. Obtenido de https://www.gartner.com/en/articles/top-strategic-cybersecurity-trends-for-2023

GCSCC. (2023). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. Obtenido de https://gcscc.ox.ac.uk/the-cmm

GFCE. (2023). *Gender and Cybersecurity: creating a more inclusive digital world*. Obtenido de https://thegfce.org/initiatives/gender-and-cybersecurity-creating-a-more-inclusive-digital-world/

GPD. (2023). *New Guide to Fostering Inclusive Cyber Norm Processes.* Obtenido de https://www.gp-digital.org/news/gpd-unveils-new-guide-to-fostering-inclusive-cyber-policymaking-processes/

IBM. (2023). *Cost of a Data Breach Report 2023.* Obtenido de https://www.ibm.com/reports/data-breach

INAMU. (2018). *Política nacional para la atención y la prevención de la violencia contra las mujeres de todas las edades Costa Rica 2017-2032.* Obtenido de https://planovicr.org/sites/default/files/documentos/planovi_2017-2032_diagramada_2019_0.pdf

INTERPOL. (2022). *2022 INTERPOL Global Crime Trend Report.* Obtenido de https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf

MCKINSEY. (2023). *Technology Trends Outlook 2023*. Obtenido de https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech#/

MICITT. (2017). *Un acercamiento a la brecha digital de género en Costa Rica.* Obtenido de https://www.micitt.go.cr/wp-content/uploads/2022/04/un-acercamiento-a-la-brecha-digital-de-genero.pdf

MICITT. (2019). *Indice de Brecha Digital IDB 2016-2018*. Obtenido de https://www.micitt.go.cr/wp-content/uploads/2022/04/indice_de_brecha_digital_2016-2018_0.pdf

MICITT. (2021). *Revision de la Estrategia Nacional de Ciberseguridad de Costa Rica 2017*. Obtenido de https://www.micitt.go.cr/wp-content/uploads/2022/05/Revision-de-la-Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-2017.pdf

MICITT. (2023). *Estrategia de Transformación Digital 2023-2027 de Costa Rica*. Obtenido de https://www.micitt.go.cr/wp-content/uploads/2023/06/ETD-2023-2027-CONSULTA-PUBLICA-02-06-2023.pdf

MIDEPLAN. (2016). *Manual de Planificación con Enfoque para Resultados*. Obtenido de https://documentos.mideplan.go.cr/share/s/Tc1cuf30TOWL8_jBSxdI8Q

MIDEPLAN. (2017a). *Política Nacional para la igualdad entre mujeres y hombres en la formación, el empleo y el disfrute de los productos de la Ciencia, la Tecnología, las Telecomunicaciones y la Innovación, 2018-2027.* Obtenido de https://repositorio-snp.mideplan.go.cr/handle/123456789/92

MIDEPLAN. (2017b). *Guía sobre el enfoque de igualdad de género y derechos humanos*. Obtenido de https://documentos.mideplan.go.cr/share/s/UWG8czewS5-A8GJsx8xBCw

MIDEPLAN. (2018a). *Guia de la Teoría de la Intervención*. Obtenido de https://documentos.mideplan.go.cr/share/s/3hKUn5b6Q5mjqaTeZoKQyg

MIDEPLAN. (2018b). *Guía de Indicadores - Orientaciones básicas para su elaboración*. Obtenido de https://documentos.mideplan.go.cr/share/s/Iny9wiulTiy3QZdWrvq0ew

MIDEPLAN. (2023a). *Plan Nacional de Desarrollo y de Inversión Pública 2023-2026.* Obtenido de https://sites.google.com/expedientesmideplan.go.cr/pndip-2023-2026/pagina_principal

MIDEPLAN. (2023b). *Lineamientos para incorporar la Planificación Prospectiva Estratégica en el Sistema Nacional de Planificación (SNP).* Obtenido de https://documentos.mideplan.go.cr/share/s/Lfq4MTVVQkiEKClspayHuw

OEA & BID. (2020). *Observatorio de la Ciberseguridad en America Latina y el Caribe.* Obtenido de https://observatoriociberseguridad.org/#/home

OEA & ONU Mujeres. (2021). *Ciberviolencia y Ciberacoso contra las mujeres y niñas en el marco de la Convención Belem Do Pará*. Obtenido de https://lac.unwomen.org/sites/default/files/2022-11/MUESTRA%20Informe%20Violencia%20en%20linea%202.1%20%282%29_Aprobado%20%28Abril%202022%29_0.pdf

OEA. (2021). *Ciberseguridad de las mujeres durante la pandemia de COVID-19: Experiencias, riesgos y estrategias de autocuidado en la nueva normalidad digital.* Obtenido de https://www.oas.org/es/mesecvi/docs/Ciberseguridad_COVID_esp.pdf

OEA. (2023). *Report on Cybersecurity Workforce Development in an Era of Talent and Skills Shortages*. Obtenido de https://www.oas.org/en/sms/cicte/docs/Report_Cyber_WorkForce_Development_in_an_Era_of_Talent_and_Skills_Shortages.pdf

PARLAMENTO EUROPEO. (2023). *Ciberseguridad: amenanzas principales y emergentes.* Obtenido de https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_es.pdf

SULA BATSU & GPD. (2023). *Normativa a contemplar para un adecuado abordaje desde los derechos humanos de la ciberseguridad en Costa Rica.* Obtenido de https://www.yumpu.com/es/document/read/68368596/normativa-a-contemplar-abordaje-de-derechos-humanos-en-ciberseguridad-en-costa-rica

SUTEL. (2023). *Estadísticas del sector de telecomunicaciones.* Obtenido de https://www.sutel.go.cr/sites/default/files/informe_estadisticas_del_sector_de_telecomunicaciones_costa_rica_2022.pdf

UIT. (2023). *Global Cybersecurity Index (GCI)*. Obtenido de https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

UNIDIR. (2023). *Gender and Disarmament*. Obtenido de https://unidir.org/programmes/gender-and-disarmament

WEF. (2022). *Global Gender Gap Report 2022*. Obtenido de https://www.weforum.org/reports/global-gender-gap-report-2022/

WEF. (2023a). *Global Gender Gap Report 2023*. Obtenido de https://www3.weforum.org/docs/WEF_GGGR_2023.pdf

WEF. (2023b). *Global Cybersecurity Outlook 2023*. Obtenido de https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

Annex 1

Recommendations Regarding Implementation of the 2017-2021 National Cybersecurity Strategy, presented by MICITT with support from OAS & Cyber4Dev

Recommendation from MICITT with support from OAS & Cyber4Dev	Type of Measurements
• Assign responsibilities and a **governance framework** that promotes public-private coordination. • Consider creating a **high-level coordination body** at the governmental level (e.g. a National Cybersecurity Council) • Raise awareness among heads of government entities regarding the potential impact that cybersecurity incidents may have on their operations, in order to **allocate appropriate resources** to address incident response vulnerabilities. • Develop a **communications strategy** that includes planning to inform government departments and agencies, businesses, and civil society regarding relevant initiatives. • Include a high-level **action plan** on how to achieve the desired objectives, as well as **indicators** with which to measure achievements.	Organizational Measures
• Establish a working group specifically to analyze the **legal framework** and gaps that need to be addressed at the national level, and consider the national position of the Costa Rican Government in addressing cybercrime investigation, both within and outside its jurisdiction, especially as it relates to research and cooperation between jurisdictions.	Regulatory Measures
• Take appropriate measures to generate visibility for the **CSIRT-CR** legal mandate, as national coordinator in the management and response to cybersecurity incidents. • Clearly define the **Critical Information Infrastructure** (CII). • Carry out horizontal and vertical mapping based on the intersectoral independence of the Critical Information Infrastructure (CII) of Costa Rica. • Promote coordination between authorities to ensure periodic testing and evaluation of critical infrastructure, **essential services**, and the government network. • Design monitoring mechanisms and provide regular updates to the list of critical infrastructure elements and suppliers. • Establish a common cybersecurity risk assessment methodology, periodic sector risk assessments, a risk repository, a cybersecurity incident registry, and a mandatory report. • Develop specific standards for each industry at the national level and establish awareness campaigns, as well as workshops for their implementation. • Address cyber **crisis management**, contingency planning and disaster recovery, and cybersecurity exercises. • Periodic Risk Analysis and Threat Panorama reports for both the public and private sectors. • Develop **large-scale cybersecurity incident management plans** as part of national emergency planning.	Technical Measures
• Increase and strengthen the cybersecurity **workforce**. • Develop and include basic **cybersecurity education programs** for each educational level. • Map cybersecurity courses and centralize access to information regarding **academic professionalization offers**, and promote this resource at the national level. • Develop, nationalize, and make visible national **awareness** campaigns for the public sector and the general public, especially for vulnerable population groups.	Capacity Strengthening Measures
• Carry out cooperation agreements with academia and the technical community.	Cooperation Measures

Source: Own elaboration (2023) from (MICITT, 2021)

Annex 2

Recommendations Regarding the Declaration of a State of Emergency in 2022, presented by the Comptroller General of the Republic

CGR Recommendation	Type of Measurements
• Modernize the cybersecurity **governance model** to consolidate a coordinating body that effectively supervises and manages information security measures and practices, and to develop a collective capacity that involves public institutions, civil society, the private sector, international organizations, and other stakeholders. • Do not eliminate or reduce investments in cybersecurity that are made from the Republic's Budget and seek to enable contingency financial resources that allow for an effective response to possible cyberattacks that materialize in the future.	**Organizational Measures**
• Review, modernize, and adapt the regulatory framework to manage the risks associated with information security, considering cybersecurity and the definition of minimum standards for practices at public institutions.	**Regulatory Measures**
• Prioritize the security of **critical infrastructure** by precisely defining what the national critical infrastructure is, at the levels of both the public and private sectors, as well as defining what are the essential protection mechanisms that are required, so that the involved institutions can establish the corresponding roadmap. • Strengthen **risk management** to identify and prioritize critical assets, critical infrastructure, and periodic cybersecurity risk assessment. Also, allocate resources and efforts to protect those who present a higher level of risk, thus maximizing the return on investment in terms of economic and social benefits.	**Technical Measures**
• Strengthen the cybersecurity culture by developing staff **awareness** regarding the relevance of cybersecurity in the management and custody of information and the continuity of services.	**Capacity Strengthening Measures**
• Adopt a **collaborative** approach, in which spaces are created for joint learning, awareness around good practices, sharing successful experiences, and developing an articulated ecosystem in accordance with the needs of the institutions.	**Cooperation Measures**

Source: Own elaboration (2023) from (CGR, 2023)

MINISTERIO DE CIENCIA,
INNOVACIÓN, TECNOLOGÍA
Y TELECOMUNICACIONES

GOBIERNO
DE COSTA RICA

COSTA RICAN
NATIONAL CYBERSECURITY STRATEGY 2023 - 2027