NATIONAL CYBERSECURITY POLICY

2023-2028

CICS Interministerial Committee on Cybersecurity

Gobierno de Chile

gob.cl

NATIONAL CYBERSECURITY POLICY

2023-2028

CICS Interministerial Committee on Cybersecurity

Gobierno de Chile

gob.cl

NATIONAL CYBERSECURITY POLICY

2023-2028

TABLE OF CONTENTS

Over the last ten years, Chile has successfully positioned itself in several international rankings on digital competitiveness, which prove us to be a country whose digital transformation process has accelerated.

In the same period, our country began a planning process to address the risks associated with the massive use of information and communications technologies, which gave rise to the National Cybersecurity Policy for the years 2017 to 2022 that guided cybersecurity actions during three consecutive governments. In terms of cybersecurity, Chile has a true State policy.

On this occasion, I have the honor of introducing to you the new National Cybersecurity Policy for the 2023-2028 period. It is an instrument with a comprehensive approach, which provides continuity to the efforts that we have been developing over the last decade to safeguard our digital assets, protect the rights of our citizens and strengthen the resilience of our institutions in the face of growing cyber threats.

Just like the previous one, this policy is the product of multisector collaboration between the public sector, the private sector, the academia and the civil society, because cybersecurity is best guaranteed through a joint effort in which our entire society participates. The policy promotes collaboration and coordination to take advantage of the experience of different sectors with a view to preventing cybersecurity risks.

To face the challenges and new threats to people's security, the new National Cybersecurity Policy establishes a roadmap for public and private action that requires actions in the medium term and is composed of five strategic goals: having a resilient infrastructure, ensuring the protection of people's rights, fostering a culture of cybersecurity, promoting national and international coordination and fostering industry and scientific research.

Additionally, four transversal dimensions have been incorporated on this occasion, whose purpose is to ensure that the five goals are achieved with a focus on protecting and promoting the rights of individuals and their families on the Internet. The current policy incorporated dimensions of gender equality; protection of children and adolescents; protection of the elderly and environmental protection.

With this new National Cybersecurity Policy we hope to move forward with strong steps in the construction of a safe digital space for everyone.

For the implementation of the policy, an action plan is established consisting of a set of short-term measures, covering a period of two years instead of five, as the case was with the previous policy, which will permit us to review progress, evaluate the need for improvements and amend those actions that have been poorly implemented. Therefore, the action plan will be published separately from the Policy.

With this new National Cybersecurity Policy we hope to move forward with strong steps in the construction of a safe digital space for everyone.

Gabriel Boric Font
President of the Republic

A few days after publication in the Official Gazette of the 2023-2028 National Cybersecurity Policy, which sets the strategic goals of the State of Chile on this matter for the coming years, the National Congress unanimously passed the framework bill on cybersecurity that creates the National Cybersecurity Agency. Thus, Chile becomes the first country in Latin America and the Caribbean to have a general law and a national public institutional framework on cybersecurity, which helps increase maturity levels in such an essential area of people's lives.

Digital security has also become a challenge for the government, society, companies and, also, for people. Incidents and cyberattacks that have affected both public and private sector organizations, and even individuals, have increased considerably - both in number and sophistication.

Therefore, having a new political cybersecurity planning instrument is key for our country and now it is for us as a society to advance its correct implementation, as a State policy, as so committed in our Government Program. Such was the case in the second government of President Michelle Bachelet, where the first cybersecurity policy was established, the implementation of which was maintained during the government of President Sebastián Piñera, including the presentation of the framework bill on cybersecurity.

We have assumed digital security as a priority challenge of the government of President Gabriel Boric Font, placing strong emphasis on improving our technological infrastructure and promoting the protection of people's rights in cyberspace.

For this, with the creation of the National Cybersecurity Agency we will be able to focus efforts on protecting the normal operation of such sensitive areas as the electrical sector, transportation or telecommunications, where the effects of a cyberattack might affect people's daily lives.

Because we are convinced that when we adopt measures to protect digital security, we are not only protecting computers. We are protecting people and society as a whole. As many have argued, cybersecurity has ceased to be a technical issue and has become a State duty, which even allows us to better confront transnational organized crime.

Because we are convinced that when we take steps to protect digital security, we are not only protecting computers, we are also protecting people and society as a whole.

Having both this new National Cybersecurity Policy, as well as the recently approved Framework Law on Cybersecurity, will allow us to advance much more strongly in building a safe digital space so that people can exercise their rights and carry out their activities normally and safely.

Manuel Monsalve Benavides
Under Secretary of the Interior


01
INTRODUCTION

1.Introduction

Information and communication technologies (ICTs) play a fundamental role in the daily activities and well-being of people, in the generation of wealth for countries, the provision of basic services for societies, and in nations' security and sovereignty. Both the quantity and variety of uses that we give to ICTs, and the number of people with access to them, have increased rapidly in the past 20 years, creating new opportunities for social development and economic growth. However, technology is intrinsically vulnerable. Most of ICTs were not designed with information security in mind, thus allowing various actors to be able to harm people and organizations through these technologies.

In April 2017, then-President Michelle Bachelet launched Chile's first National Cybersecurity Policy, which contained five public policy objectives on cybersecurity, including a series of 41 measures to be implemented between 2018 and 2022. The Policy was confirmed by the government of President Sebastián Piñera, showing progress in the design of the institutional framework and the strengthening of the regulatory framework, and allowing the country to advance decisively in the challenges we face. Challenges have diversified and become more complex, and the global scenario is experiencing accelerated changes, making it necessary to swiftly strengthen the same areas of protection considered in the first policy, and to grow new capacities to adapt to circumstances different from those that were foreseen five years ago.

President Gabriel Boric's administration has continued the process of implementing the National Cybersecurity Policy including the discussion of the draft framework law on cybersecurity, placing special emphasis on the protection and defense of people's rights, gender equality, and the deepening of democracy. Efforts have been made to provide protection to those groups that are mostly affected by digital violence and cybercrimes, taking into consideration that cyberspace threats do not impact everyone equally, with the main victims being women, girls, children, adolescents, older people and sex/gender dissidents.

To increase our level of maturity in cybersecurity, we need to have a free, open, secure and resilient cyberspace, as stated in the first National Cybersecurity Policy, which constituted a State policy and, as such, must be renewed.

This Policy is the result of the participation of a number of actors from the public and private world, who, through public hearings, expressed their concerns and views regarding the issues and challenges that digital life entails. Civil society played a fundamental role in its preparation through two citizen consultations, one before and the after its drafting. For its preparation, the recommendations of the International Telecommunication Union (ITU)[1] were followed, the experience of similar and more advanced countries was reviewed, various international publications[2] were consulted, and an evaluation of the implementation process of the measures of the first Policy was carried out. This second policy represents both a continuation of the efforts of the first and a readaptation of the focus for the coming years as a result of the review of the changes that have taken place since then.

1.1. Why do we need a National Cybersecurity Policy

This century will probably see more changes than the entire history of humanity, both as regards to cultural life and in political and economic terms. Global warming accelerates climate change, accentuating extreme weather and increasing the frequency and duration of events such as droughts, floods, tornadoes, and wildfires. The availability of water has decreased, which affects agriculture and decreases our ability to produce food.[3] All these changes are already affecting our country, and they are expected to accelerate during this century.

The SARS CoV-2 (COVID-19) pandemic has produced, as of April 2023, just over 6.8 million deaths worldwide[4] and more than 52,000 confirmed deaths in our country.[5] In addition to the enormous social cost in terms of public health, the pandemic accelerated multiple digital transformation processes. Productivity in most societies has been significantly diminished for several years, thus contributing to an emerging or already declared economic recession in dozens of countries. As with the 1918 global flu epidemic, the effects of the current pandemic will take many years to pass.

Lastly, the political and economic instability that the war in Eastern Europe has generated puts us in a scenario that we have not seen since the Second World War. Before the conflict, Ukraine produced 10% of the world's wheat, 15% of its corn, and 13% of its barley.[6] Grain shortage generated price increases for several months, and has contributed to the increase in inflation in many economies.

All of the above is relevant to our country, but what relationship does this have with cybersecurity?

Cybersecurity is not an end in itself. Cybersecurity is a condition that, if it exists, allows full use of the Internet and the web, tools that enable and promote human activities. All our efforts to face challenges such as climate change and the COVID-19 pandemic, and to restore peace and political and economic stability globally, can be facilitated or hindered by the presence or absence of the communication tools provided through computer networks and systems.

In December 2003, the World Summit on the Information Society, established under the auspices of the United Nations (UN), published a declaration of principles of the Information Society, after long negotiations with private and public organizations and representatives of the civil society of all participating countries.[7] In point 4 of the declaration it is affirmed that ***"everyone has the right to freedom of opinion and expression; that this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Communication is a fundamental social process, a basic human need and the foundation of all social organization."***[8] It is the fulfillment of this basic human need and fundamental human right, that we make possible through cybersecurity. Today, every State has the duty to create the conditions to allow each person to exercise this right.

Twenty years later, in January 2023, the ***World Economic Forum*** published a report[9] introducing a series of cybersecurity issues as seen from the perspective of experts and business leaders around the world, highlighting the following:

- Global geopolitical instability has convinced leaders and experts alike of the importance of managing cybersecurity risks. 91% of study participants believe that a catastrophic cybersecurity incident is relatively likely within the next two years.

- 43% of leaders believe that their organization is likely to be attacked via cyberspace within the next two years.

- Concerns about cybersecurity and personal data protection are increasingly influencing how and where businesses operate. The level of cybersecurity that each country is capable of securing is being considered by investors to make decisions about where to invest.

- The nature of threats in cyberspace is changing. Both business leaders and cybersecurity experts believe that attackers are concentrating on damaging business processes and undermining the reputation of organizations.

Our economy, most part of international trade, our leisure activities, mass media, social and political interactions, and the keeping and dissemination of our culture, they all depend heavily on access to the Internet and to the media and applications enabled by it. That is why the first version of the National Cybersecurity Policy (2017-2022) set the goal for 2022 ***to have a free, open, secure, and resilient cyberspace; for the same reason,*** the new National Cybersecurity Policy (2023-2028) will pursue the same objective.

1.2. Cybersecurity Challenges in our Country

Chile has a medium level of maturity in cybersecurity on the international stage. In the 2020[10] Global Cybersecurity Index, Chile was ranked 74th worldwide, and 7th in the Americas (below the United States, Canada, Brazil, Mexico, Uruguay, and the Dominican Republic). In this index, Chile stands out for its progress in legal measures, organizational measures and cooperation; however, it runs behind in technical measures.

Regarding the National Cybersecurity Index[11], developed by Estonia and continuously updated, Chile is in 53rd place among 175 countries, and in 6th place in Latin America and the Caribbean, below the Dominican Republic, Argentina, Paraguay, Peru and Uruguay. In this ranking, which consists of 12 different areas, Chile stands out in the development of cybersecurity policies; fight against cybercrime, and military operations; but it runs behind in protection of essential services; protection of digital services, crisis management and protection of personal data.

The main problems we face today in terms of cybersecurity in our country are:

1. **Insufficient resilience of our organizations and infrastructure.**
   Recent security breaches in the country confirm the need to strengthen the protection of our network infrastructure and systems while improving the training and preparation of public officials, as well as all the people in organizations that may require it. For this purpose, it is necessary to monitor our cyberspace effectively, especially the network infrastructure of the public sector, essential services and operators of vital importance.

2. **The lack of culture of organizations and people regarding the importance of cybersecurity.**
   This, together with the lack of knowledge, means that both organizations and individuals do not take sufficient protection measures in cyberspace. Therefore, the State challenge is to provide basic literacy in cybersecurity and generate awareness of its importance in each person, from second childhood to the elderly, both in primary and secondary education, as well as in private organizations, the public sector, and the civil society. To address this challenge, the State will take particular care of the most remote territories.

3. **The lack of cybersecurity specialists.**
   Estimations reveal that Chile is lacking around 28,000 cybersecurity specialists to serve the needs of both the public and private sectors[12], and that careers specifically related to cybersecurity only have 10% of

women, a figure that is consistent with the 15% of participation of women in cybersecurity jobs available in the country. The absence of women in the labor world and in computer science-related careers, both in technical training centers and in universities and professional institutes, finds its explanation in different social conditions that discourage their participation, and not in a lack of interest of women in this area. The State needs to create the conditions to reduce these gaps, encouraging a greater number of people to choose to study careers related to cybersecurity, and promoting an increase in female participation in this sector, especially considering that women represent 52.4%. of the Chilean population.

4. **The lack of sophistication of our demand for cybersecurity.**
   It is estimated that the cybersecurity industry in our country has annual sales of around $350 million dollars, which represents 0.11% of Chile's GDP[13]. Cybersecurity is an economic area that is intensive in capacities, which, in the future, could represent a growing part of our gross domestic product, help to position our country in the Latin American scenario, and even strengthen confidence in our economy, as seen from abroad. However, for this to happen, it is necessary to have a broader and more sophisticated demand.

5. **The increase in cyberspace crimes.**
   According to the national urban citizen security survey, the rate of reporting cybercrime has increased progressively in recent years from 6.6% in 2017 to 10.1% in 2021.[14] This type of crime puts people's security and trust in cyberspace at risk while being a phenomenon that must be addressed from a preventive and punitive perspective.

Our country is undoubtedly affected by global trends, but it also has specific problems. There are groups of attackers that have been highly active in Latin America, claiming responsibility for large data leaks that occurred in 2022 and 2023. The number of incidents that are recorded in the State Connectivity Network (the data network that provides connectivity to an important part of the public sector) confirms that one of the key concerns in the coming months must be the strengthening of public infrastructure, as well as the education and training of public officials, as well as a strengthening of essential services and operators of vital importance.

1.3. Five Objectives of the National Cybersecurity Policy

To face the above problems and challenges, the new National Cybersecurity Policy includes five fundamental objectives:

1. **Resilient Infrastructure:**
   The country will have a robust and resilient information infrastructure, prepared to resist and recover from cybersecurity incidents and socio-environmental disasters, from a risk management perspective.

2. **People's Rights:**
   The State will protect and promote the protection of people's rights on the Internet, through strengthening the existing institutional framework in terms of cybersecurity, and including the generation, adoption, and promotion of the required mechanisms and technological tools for each person to be able to integrate into society and develop and express themselves fully.

3. **Cybersecurity Culture:**
   Chile will develop a culture of cybersecurity around education, best practices, responsibility in the management of digital technologies, and promotion and safeguarding of people's rights.

4. **National and International Coordination:**
   The State will develop public governance to coordinate the necessary actions in cybersecurity. Public and private organizations will jointly create instances of cooperation, with the purpose of communicating and disseminating their cybersecurity activities, avoiding duplication of work and loss of resources, and making efficient efforts in this area. In the international arena, the State will coordinate with countries, organizations, institutions, and other international actors, to allow our country to better deal with malicious activities and incidents in cyberspace.

5. **Promotion of the industry and scientific research:**
   The country will promote the development of a cybersecurity industry that protects people and organizations and that serves its strategic objectives. To this end, it will promote the focus of applied scientific research on cybersecurity issues, according to the country's needs.

The choice of the above objectives is not random: It is possible to establish a relationship between them and the dimensions defined in at least two international cybersecurity models[15].

Additionally, the policy includes some crosscutting dimensions seeking to safeguard and promote the protection of the rights of individuals and their families on the Internet:

1. **Gender equality:**
   All initiatives will give priority to women, both to increase their security in the digital environment -since they are the main victims of digital violence, and to improve their inclusion, through positive actions aimed at correcting the inequities existing in our society, where despite representing more than 50% of the Chilean population, their participation in cybersecurity jobs existing in the country barely reaches 15%.

2. **Protection of children:**
   All initiatives must consider preferential protection for children and adolescents.

3. **Protection of the elderly:**
   All initiatives must consider preferential protection for the elderly.

4. **Protection of the environment:**
   All initiatives must minimize their negative impact on the environment.

As in the first version, an Action Plan will form part of this policy including a set of short-term measures to implement it. Nevertheless, unlike the previous version, the plan will be published separately from the Policy as it covers a period of only two years, while the Policy is a long-term instrument. The purpose of this change is allowing progress to be reviewed, changes and improvements proposed, and make timely amendments, if necessary, during the implementation of the Policy rather than just at the end of its term. Each measure will have an institution responsible for leading the efforts to deliver its implementation, and will periodically report the progress achieved, or the lack thereof, to the Inter-Ministerial Committee on Cybersecurity. Each measure will be associated with clear and measurable results, and achievement deadlines.

The Inter-Ministerial Committee on Cybersecurity will suggest alternatives for monitoring and implementing the Policy, including providing advice about compliance with its measures to achieve the public policy objectives contained in this document.

The government may use a wide range of political, economic, strategic, and social measures to achieve the implementation of the measures, while creating the conditions to bring about a cybersecurity ecosystem in the country, in accordance with the policies outlined in this document.

The State will progressively encourage applied research and development to cybersecurity, fostering private investment in the area, in conjunction with higher education institutions and national research centers. Applied scientific research is an unavoidable and necessary duty of the State to generate knowledge that allows increasing the efficiency of productive factors, generating added value over the mere extraction of raw materials, and providing services that give the country advantages in the international commercial arena. Cybersecurity research is a required condition to generate a cybersecurity ecosystem in our country and comply with the public policy objectives contained in this document.

1.4. Relationship with other National Objectives

• Cyberdefense Policy

Our country has a current Cyberdefense Policy, published in March 2018 through Decree No. 3, 2017, of the Ministry of National Defense. Two priorities are established in this document:

1. International cooperation:
Chile will collaborate with other countries, and promote transparency, and trust measures in fora such as the UN, the OAS, Unasur, and other organizations, in coordination with the Ministry of Foreign Affairs.

2. Capacity building:
The National Defense sector will develop career strands in each branch of the Armed Forces; it will create a Joint Cyberdefense Command, including the creation of a Defense Information Security Incident Response Center (National Defense's CSIRT).

It is worth mentioning that cyberdefense is essential for the achievement of national cybersecurity objectives; therefore, efforts should be made to strengthen the country's capacities to face cyberthreats that may threaten the country's security and put national sovereignty at risk.

Additionally, the Policy sets out a principle of equivalence: Chile may consider massive cyberattacks on its inhabitants, its infrastructure or its interests as an armed attack, within the framework of Article 51 of the United Nations Charter. This principle places the Internet communications infrastructure at the same level as the infrastructure considered strategic and vital for the country, such as the transport network and the network of health centers, among others. This Policy is consistent with the Cyberdefense Policy, and specifies public policy objectives that are in full accordance with the objectives and priorities of that planning instrument, particularly with regard to the objective of National and International Coordination.

Likewise, the National Defense sector will carry out the organic reorganization required for the fulfillment of its roles in cyberspace.

• National Artificial Intelligence Policy

Our country also has a National Artificial Intelligence Policy in place published in November 2021 through Decree No. 20 of the Ministry of Science, Technology, Knowledge and Innovation. Four crosscutting principles are set out in this paper: Artificial Intelligence (or AI) focused on the well-being of people, AI for sustainable development, inclusive AI, and globalized and evolving AI. The Policy also establishes three axes:

1. **Enabling factors,** such as talent development, technological infrastructure, and the promotion and encouragement of the massive use of data for decision-making.

2. **Development and adoption,** which includes basic and applied research, technology transfer, innovation, entrepreneur-ship, improvement of public

services, and technology-based economic development, among others.

3. **Ethics, regulatory aspects and socioeconomic effects,** where a broad and heterogeneous set of topics and areas of discussion and reflection are considered, including cybersecurity, cyberdefense, gender, etc.

This policy is fully consistent with the objectives and strands set out in the National Artificial Intelligence Policy, particularly regarding the first strand related to the training and development of talents, and capacity building and awareness of people; the second strand on applied research, technology transfer, entrepreneurship and improvement of public services; and the third strand relative to the promotion of safe technological systems and strengthening of the institutional framework in cybersecurity.

• The National Policy against Organized Crime

Lastly, our country has a National Policy against Organized Crime, published in December 2022, with the purpose of reducing the criminal activity of criminal organizations that operate in Chile, through the planned and coordinated action of State institutions. This policy has three fundamental objectives: dismantling gangs and criminal organizations, implementing specific measures to control various crimes, and strengthening inter-institutional coordination through the consolidation of a public security ecosystem. The second objective above explicitly mentions cybercrime as one of the forms of crime to be fought against.

Measures proposed by the previous Policy included the preparation of a new National Cybersecurity Policy for 2023-2028, the processing of a draft framework law on Cybersecurity and Critical Infrastructure, and the development of prevention strategies and digital education.

This Policy is fully consistent with the National Policy against Organized Crime, specifically with regards to the prevention of the perpetration of computer crimes, the generation of a culture of cybersecurity in our country, and the coordination between government institutions and private entities, where one motivation is the exchange of information and collaboration to better prevent and fight cybercrime.


02
OBJECTIVES

2. Public Policy Objectives 2023-2028

2.1. Resilient Infrastructure

The country will have a robust and resilient information infrastructure, prepared to resist and recover from cybersecurity incidents and socio-environmental disasters under a risk management perspective. For this, it is necessary to advance in the strengthening of the physical and logical technical elements of our cyberspace, including our growing network of devices connected to the Internet (Internet-of-Things, or IoT).

To achieve this objective, it will be necessary to:

1. Promote the processing of the framework bill on cybersecurity and critical information infrastructure, which creates the National Cybersecurity Agency, which operates as the governing body for cybersecurity in Chile, with regulatory, supervisory and sanctioning powers, which helps increase the level of institutional maturity in cybersecurity, both in the public and private sectors.

2. Create the National Computer Security Incident Response Team (National CSIRT), to meet the needs and requirements for protection and recovery from incidents in the public and private sectors affecting organizations considered to be of vital importance.

3. Strengthen resilience of our essential services against cybersecurity incidents. Public and private institutions operating services considered vital must improve their level of maturity in cybersecurity and their ability to overcome breaches and attacks. The State will deliver basic recommendations and guidelines allowing institutions to protect themselves against the most frequent or high-impact attacks.

4. Strengthen the physical resilience of the network in Chile. In coordination with the private sector, the State, in accordance with the provisions of the relevant legal and regulatory bodies, will promote the prioritization of the connection of previously unconnected places, or where there is no redundancy of connections with at least two other places.

5. Strengthen network information analysis in national cyberspace, through investment in applied scientific research to be carried in collaboration with the academic sector and domestic industry, to place Chile at the forefront in Latin America in the generation of knowledge and development of cybersecurity technology.

2.2. People's Rights

Cybersecurity culture, including the generation, adoption, and promotion of proper mechanisms and technological tools so that each person can integrate into society and fully develop and express themselves, granting special protection to women, girls, boys, adolescents, older adults, and sex/gender dissidence. All people should be able to use the Internet to communicate, work, study, and develop personally, within their family, and socially in an environment of equity, inclusion, justice, and protection of diversity.

To achieve this objective, it will be necessary to:

1. Strengthen the regulatory framework on cybersecurity and personal data protection, through the approval and implementation of the cybersecurity framework law and the law on personal data protection.

2. Generate training instances for the development of habits and basic digital security measures by all public officials, allowing them to protect citizen's information entrusted to them and that they manage through networks and computer systems.

3. Prevent the perpetration of cybercrimes, with emphasis on those affecting women,

girls, boys and adolescents, the elderly and sex/gender dissidents, due to their greater vulnerability in cyberspace.

4. Identify and correct inequities in the access to and use of cyberspace caused by the lack of knowledge of digital security by people and social groups in situations of greater vulnerability to incidents.

2.3. Cybersecurity Culture

Chile will develop a cybersecurity culture around education, best practices, responsibility in the management of digital technologies, and the promotion and safeguarding of people's rights. The protection of society is directly related to the ability of each person to protect themselves. It is necessary to generate notions and practices of cyber hygiene within the population, so that each person is capable of taking care of their digital identity and information on their own.

To achieve this objective, it will be necessary to:

1. Design and implement a national awareness plan about cybersecurity and privacy, so that all people using a computer or smartphone, regardless of the country's region where they are located, may acquire notions and practices of cyber hygiene. This program will focus especially on women, girls, boys, adolescents, older adults and sex/gender dissidents, on people who live outside the Metropolitan Region, and on other groups that could be at a disadvantage compared to the rest of society in terms of knowledge about cybersecurity; and in micro and small businesses.

2. Generate and implement a main plan for the introduction and improvement of education in cyber hygiene and cybersecurity for the primary education system, humanist-scientific secondary education and technical-professional secondary education. In particular, this plan will consider evaluating the generation of specialties for technical-professional secondary education and the incorporation of cyber hygiene and cybersecurity subjects to related specialties throughout the country.

3. Promote a culture of risk assessment and management, both within public and private organizations, which allows us to prepare for incidents and disasters that can seriously affect the people of our country, their well-being, their health, rights, and identity, as well as their assets or the possibility to fully develop themselves through the Internet.

4. Promote applied scientific research in cybersecurity, to solve problems that our country will have in the coming years as a result of the intensive use and implementation of technologies with unsuspected applications. Our country cannot simply be a passive consumer of technologies developed abroad, it being the responsibility of the State to generate the conditions to solve complex technical problems calling for scientific research, and that arise from the needs and protection requirements of our people and organizations.

2.4. National and International Coordination

In order to make efficient and effective use of available resources, coordinated and focused action towards the achievement of public policy objectives is essential. Public and private organizations will promote instances of cooperation with the rest of the public sector and industry, and with the future national cybersecurity authority, with special emphasis on the communication and dissemination of efforts made in cybersecurity, in order to avoid duplication of work and waste of resources. In the international aspect, the State will

coordinate and work with countries, organizations, institutions and other international actors, to allow our country to better deal with malicious activities and incidents in cyberspace, thus contributing to strengthening its regional leadership in the field of cybersecurity.

To achieve this objective, it will be necessary to:

1. Generate opportunities of collaboration and cooperation between public and private organizations in various fields, including education, infrastructure, protection of rights, promotion of the industry and other areas related to cybersecurity that may be of interest to the country, with the purpose of promoting the initiatives under development and coordinating them appropriately.

2. Develop cooperation relationships with cybersecurity institutions from leading countries in the field aimed to learn about their experiences and bring relevant experience to the implementation of cybersecurity initiatives or projects. To this purpose, an international cooperation strategy will be developed where specific priorities and lines of action are established.

3. Increase participation in multilateral fora, particularly within the United Nations and the Organization of American States, as well as in multi-stakeholder initiatives. Likewise, work and collaboration within the framework of the Budapest Convention will be promoted.

4. Actively promote cyberdiplomacy, encouraging discussion at a regional and global level regarding the application of standards, international law, and confidence-building measures in cyberspace, and the development of bilateral agreements fostering cooperation in cybersecurity, and respect for human rights in cyberspace.

5. Coordinate international policy on cybersecurity. The Ministry of Foreign Affairs will be responsible for this coordination with the other ministries and government agencies.

2.5. Promotion of the Industry and Scientific Research

The country will promote the development of a cybersecurity industry protecting people and organizations and serving its strategic objectives. This promotion will be implemented through incentives and funds aimed at the offer of cybersecurity services and products, as well as through the generation of a more sophisticated demand in cybersecurity, so that our industry can better protect people and organizations, while serving better the country's interests

To achieve this objective, it will be necessary to:

1. Focus applied research on cybersecurity issues and needs in both the public and private sectors. To this end, the creation of institutes for applied scientific research and technology transfer in the field will be promoted by fostering cybersecurity as a preferred area by the national academic sector, and connecting the needs of organizations and the public sector with existing scientific knowledge.

2. Create incentives for technological entrepreneurship in cybersecurity, driven by the needs of our country's private and public organizations, and particularly by the Information Security Incident Response Centers (CSIRTs), supported by research groups in universities and research centers. These incentives will not be restricted to the economic sphere; they will be broad and will focus especially on regions other than the Metropolitan Region.

3. Review the mechanisms for contracting cybersecurity services by the State, making them more efficient and expeditious, giving preference to the contracting of cybersecurity services offered by the local industry.

4. Promote the products and services of local cybersecurity companies nationally and abroad, through public funds and public-private alliances, and generate economic and tax incentives for existing companies to be able to expand their service offerings in cybersecurity and offer them preferentially to the State.

5. Promote the integration and inclusion of gender mainstreaming in the development of the cybersecurity ecosystem in our country, generating positive action measures that allow increasing the number of women in managerial and technical roles in cybersecurity.

NATIONAL CYBERSECURITY POLICY

2023-2028


03
CONCLUSIONS

3. Country's Governance in the Field of Cybersecurity

3.1. Regulatory Framework

Our country has a broad set of legal and regulatory regulations that are directly or indirectly related to cybersecurity. Within these, our own Political Constitution of the Republic stands out at the national level (articles 8, 19, 24, 39 and following) and laws such as Law No. 20,285, on access to public information; Law No. 19,628, on the protection of private life; Law No. 21,180 on the digital transformation of the State; Law No. 21,113 that declares the month of October as the national cybersecurity month; Law No. 21,459 creating regulations on computer crimes, repealing Law No. 19,223 and modifying other legal bodies in order to adapt them to the Budapest Convention; Law No. 21,521 promoting financial competition and inclusion through innovation and technology in the provision of financial services, the FINTEC Law; Law No. 19,799, on digital documents, digital signature and certification services of said signature; Law No. 19,974, on the State Intelligence System and the creation pf the National Intelligence Agency; and Law No. 18,168, the general telecommunications law, among other legal bodies.

Additionally, we the following regulations are also in place: Decree No. 83 of 2004, issued by the Ministry of the General Secretariat of the Presidency, passing a technical regulation for state administration bodies on the security and confidentiality of digital documents; Decree No. 1,299 of 2004, issued by the Ministry of the Interior and Public Security, establishing new rules that regulate the State Connectivity Network administered by the Ministry of the Interior and setting the procedures, requirements and technological standards for the incorporation into said network of public institutions; Decree No. 1 of 2015, issued by the Ministry of the General Secretariat of the Presidency, passing technical regulations on systems and websites of State's administration bodies; Decree No. 533 of 2015, which creates the Inter-Ministerial Committee on Cybersecurity, as amended by Decree No. 579 of 2020, both issued by the Ministry of the Interior and Public Security; Decree No. 273 of 2022, issued by the Ministry of the Interior and Public Security, which establishes the obligation to report cybersecurity incidents; Decree No. 14 of 2014, issued by the Ministry of Economy, Development and Tourism, amending Decree No. 181 of 2002, which approves the regulations of Law No. 19,799 on digital documents, digital signature and the certification of said signature, and repealing the relevant decrees; Decree No. 24 of 2019, issued by the Ministry of Economy, Development and Tourism, passing the technical standard for the provision of the advanced digital signature certification service; etc.

In turn, there are sectoral regulations such as Exempt Resolution No. 1,381 of August 10, 2020, issued the Undersecretariat of Telecommunications, passing a technical standard on general cybersecurity fundamentals for the design, installation and operation of networks and systems used for the provision of telecommunication services; Exempt Resolution No. 785 of November 3, 2021, issued by the Undersecretariat of Assistance Networks, passing an Information Security and Cybersecurity Instruction for the health sector; from the Superintendency of Casinos and Games, whose Circular gives instructions regarding the cybersecurity guidelines that operating companies and gaming casino concessionaires must observe; the Superintendency of Pensions creating a Management Model for Information Security and Cybersecurity; general regulation No. 454 dated May 18th, 2021, issued by the Financial Market Commission, setting out instructions on the management of Operational Risk and Cybersecurity, as well as the periodic performance of self-assessments in both matters in insurance companies and reinsurers; Guidance No. 32 dated December 5th, 2018 regarding ChileCompra, which approves Recommendations for contracting cloud services, among other texts.

Lastly, at the international level, there is the Budapest Convention and the ISO/IEC 27000 series of standards that have been published by the National Institute for Standardization (INN).

3.2. Current and Future Institutionality

The current institutional framework in terms of cybersecurity is under the lead of various agencies and entities. This makes it necessary to strategically coordinate the different efforts, their roles and duties, and the establishment of common practices and technical criteria, with the aim of improving efficiency and effectiveness in the field of cybersecurity.

It is of public knowledge that our country has been affected by a series of cybersecurity incidents and attacks in recent years. This, added to a regulatory and institutional dispersion, has generated the urgent need to legislate in this regard. Thus, with the recognition of cybersecurity as a cross-cutting means for the protection of people, their rights, patrimony and individual security, the government of President Gabriel Boric has promoted the Draft Framework Law on Cybersecurity (Bulletin No. 14,847-06), introduced during the administration of President Sebastián Piñera.

Said project offers a comprehensive response to the issues and challenges that cybersecurity imposes, and is consistent with the digital transformation process being carried out by our country, which scope of application is the entire public and private sector, with cybersecurity obligations differentiated by risk and size. A reflection of that is the obligation to set out the essential services and identify the operators of vital importance. Regarding the institutional framework, it creates the National Cybersecurity Agency, the Multisectoral Council on Cybersecurity, a National CSIRT and the National Defense CSIRT, ensuring its coordination with other Sectoral CSIRTs that may be created.

Lastly, the bill proposes to establish specific obligations in terms of cybersecurity for the public and private sectors, incorporating the dimension of education, training, best practices and cyber hygiene. In addition, following the best and most current international practices, it seeks to support vulnerability research by granting legal protection to ethical hacking, and promote the notification of cybersecurity incidents.

If the bill is approved, Chile will have a regulatory framework and a cutting-edge national cybersecurity authority at a regional and global level.

Notes and license

1. Guide to Developing a National Cybersecurity Strategy, 2nd edition 2021.

2. Such as the guides and manuals of the NATO Cooperative Cyber Defense Center of Excellence; ENISA's National Cyber Security Strategies; the Oxford University Cybersecurity Capabilities Maturity Model for Nations; and the Global Cybersecurity Index of the International Telecommunication Union.

3. IPCC, 2022: Summary for Policymakers [H.-O. Pörtner, D.C. Roberts, E.S. Poloczanska, K. Mintenbeck, M. Tignor, A. Alegría, M. Craig, S. Langsdorf, S. Löschke, V. Möller, A. Okem (eds.)]. In: Climate Change 2022: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change [H.-O. Pörtner, D.C. Roberts, M. Tignor, E.S. Poloczanska, K. Mintenbeck, A. Alegría, M. Craig, S. Langsdorf, S. Löschke, V. Möller, A. Okem, B. Rama (eds.)]. Cambridge University Press, Cambridge, UK and New York, NY, USA, pp. 3–33, doi:10.1017/9781009325844.001.

4. *https://www.worldometers.info/coronavirus/*

5. *https://www.gob.cl/pasoapaso/cifrasoficiales/*

6. *https://www.dw.com/en/five-facts-on-grain-and-the-war-in-ukraine/a-62601467*

7. *https://en.wikipedia.org/wiki/Right_to_Internet_access*

8. *https://www.itu.int/net/wsis/docs/geneva/official/dop.html*

9. Global Cybersecurity Outlook 2023, Insight Report, January 2023. World Economic Forum. In collaboration with Accenture. See *https://www.weforum.org/reports/global-cybersecurity-outlook-2023/.*

10. The Global Cybersecurity Index, of the International Telecommunication Union, is a ranking measuring "the level of commitment" of the 193 ITU member countries using five pillars: legal, technical, organizational, training and cooperation.
See *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx*

11. National Cybersecurity Index (NCSI). See *https://ncsi.ega.ee*

12. Brief study #2: Estimation of the gap of cybersecurity experts in Chile. National Cybersecurity Coordination, January 2023. Available at *https://bit.ly/cnc-eb02*

13. Brief study #1: RFI of the cybersecurity industry in Chile. National Cybersecurity Coordination, December 2022. Available at *https://bit.ly/cnc-eb01*

14. *https://www.ine.gob.cl/estadisticas/sociales/seguridad-publica-y-justicia/seguridad-ciudadana*

15. The Cybersecurity Capacity Maturity Model (CMM) from the Global Center for Cybersecurity Capacity at the University of Oxford (*https://gcscc.ox.ac.uk/the-cmm*), and also the Global Cybersecurity Index (ICG) published by the International Telecommunication Union in 2020 (*https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-S.pdf*)

The National Cybersecurity Policy was approved by H.E. the President of the Republic, pursuant to Supreme Decree No. 164, dated June 16th, 2023, and published in the Official Gazette of December 4th, 2023.

The official Spanish text of the Policy is available at the following link:
https://www.diariooficial.interior.gob.cl/publicaciones/2023/12/04/43717/01/2415658.pdf

The National Cybersecurity Policy 2023-2028 was prepared by the Interministerial Committee on Cybersecurity, in compliance with a mandate set out by Supreme Decree No. 533, of 2015 and was passed in the session held on May 25th, 2023. Its permanent members were:

1. Manuel Monsalve Benavides, Under-Secretary of the Interior
2. Macarena Lobos Palacios, Under-Secretary General of the Presidency
3. Heidi Berner Herrera, Under-Secretary of Finance
4. Victor Jeame Barrueto, Under-Secretary of Defense
5. Gloria de la Fuente González, Under-Secretary of Foreign Affairs
6. Jaime Gajardo Falcón, Under-Secretary of Justice
7. Claudio Araya San Martín, Under-Secretary of Telecommunications
8. Montserrat Castro Hermosilla, Under-Secretary (A) of Economy and Smaller Businesses
9. Willy Kracht Gajardo, Under-Secretary of Mining
10. Luis Felipe Ramos Barrera, Under-Secretary of Energy
11. Carolina Gainza Cortés, Under-Secretary of Science, Technology, Knowledge and Innovation
12. Luis Marcó Rodríguez, Director of the National Intelligence Agency

The Interministerial Committee on Cybersecurity was chaired by Daniel Álvarez Valenzuela.

The delegated representatives were:

1. José Inostroza Lara, Under-Secretariat General of the Presidency
2. Claudio Reyes Barrientos, Under-Secretariat of Finance
3. Pablo Sierra Hormazabal and Juan Pablo Cortés Albornoz, Under-Secretariat of Defense
4. Felipe Cousiño Donoso, Pablo Castro Hermosilla and Magdalena Durán Reyes, Under-Secretariat of Foreign Affairs
5. Gabriel Monsalve León, Under-Secretariat of Justice
6. Enoc Araya Castillo, Under-Secretariat of Telecommunications
7. Joan Romero Ubiergo, Under-Secretariat of Energy
8. Constanza Alarcón Cuevas, National Intelligence Agency
9. Nicky Arenberg Nissin, Under-Secretariat of Economy and Smaller Businesses
10. Daniela Vera Puga and Gonzalo Arenas Sepúlveda, Under-Secretariat of Science, Technology, Knowledge and Innovation

The Advisory Commission of the Interministerial Cybersecurity Committee was led by Ingrid Inda Camino. The Executive Secretary of the Committee was headed by Michelle Bordachar Benoit and the Executive Secretary team was made up of Alejandra Ayala Díaz, Cristian Bravo Lillo, Bárbara Schneider Schiehl and Hernán Espinoza Medina.

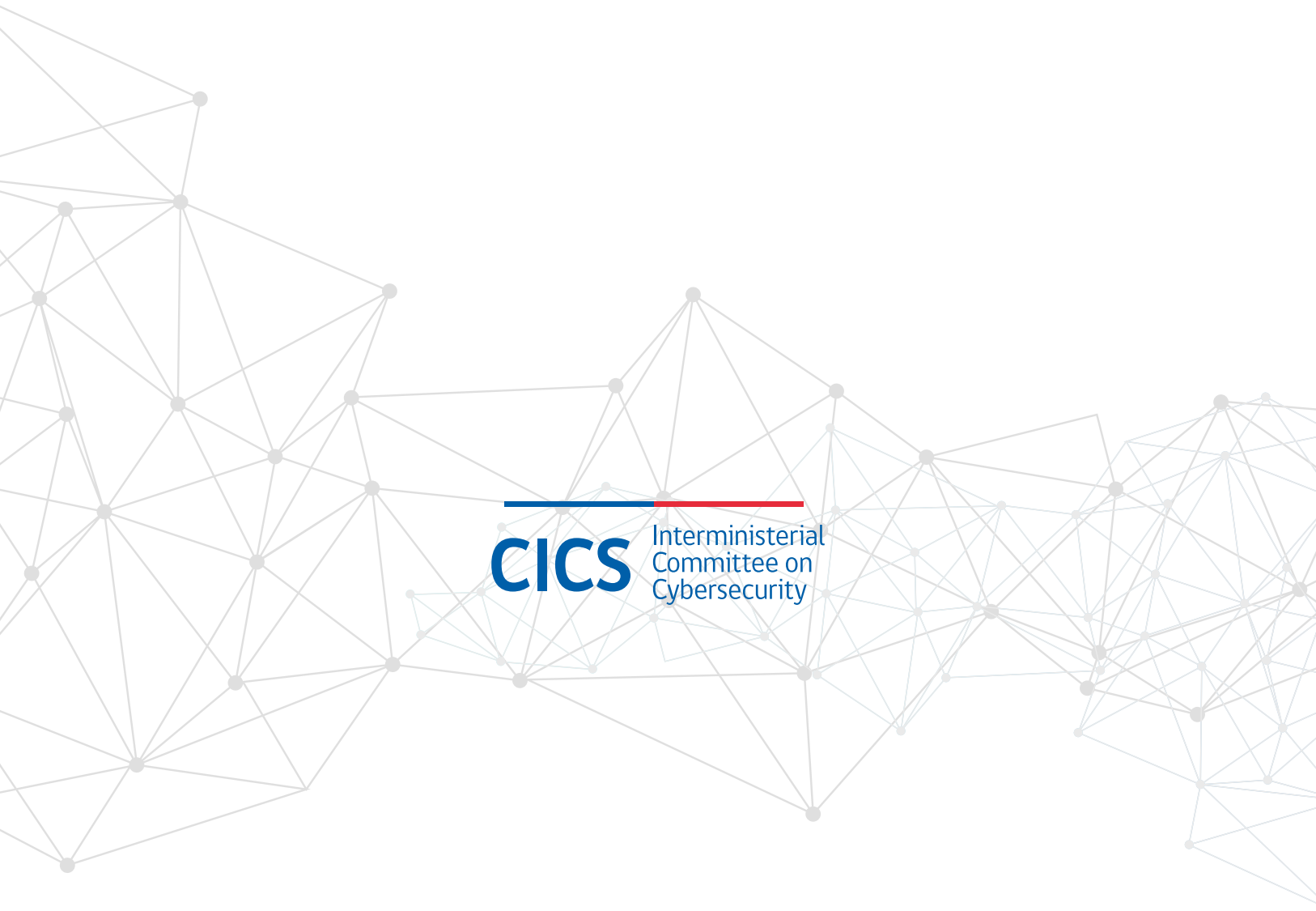
Representatives of the following organizations participated in the public meetings:

- Academia Politécnica Militar (Military Polytechnic Academy)
- Alianza Chilena de Ciberseguridad (Chilean Cybersecurity Alliance)
- Asociación Chilena de Tecnologías de la Información (Chilean Association of Information Technologies)
- Asociación Nacional de Informáticos Municipales (National Association of Municipal Computer Scientists)
- Centro Nacional en Sistemas de Información en Salud (CENS) (National Center for Health Information Systems (CENS))
- ChileTelco
- CODELCO
- Consultora en Género Paz Peña (Gender Consultant Paz Peña)
- Derechos Digitales (Digital Rights)
- ENAP
- Fundación País Digital (Digital Country Foundation)
- Fundación Soshisi (Soshisi Foundation)
- Fundación Soymás (Soymás Foundation)
- Fundación Whilolab (Whilolab Foundation)
- Hackada
- Instituto Milenio Fundamentos de los Datos (Millennium Institute of Data Fundamentals)
- NIC Chile
- Observatorio ALMA (ALMA Observatory)
- Red de Mujeres de Alta Dirección (Network of Senior Management Women)
- Universidad Andrés Bello (Andres Bello University)
- Universidad de Chile, Departamento de Ciencias de la Computación (University of Chile, Computer Sciences Department)

Two public consultations, including the participation of over 1,000 people, were held on March 3rd and May 8th, 2023.

Design and layout: Fredy Castillo V. / Interior Government Division / Under-Secretariat of the Interior.

Year 2024, Santiago. Metropolitan Region. Chile.



CICS Interministerial Committee on Cybersecurity

Subsecretaría del Interior — Gobierno de Chile

Subsecretaría de Defensa — Gobierno de Chile

Subsecretaría de Relaciones Exteriores — Gobierno de Chile

Subsecretaría de Justicia — Gobierno de Chile

Subsecretaría General de la Presidencia — Gobierno de Chile

Subsecretaría de Telecomunicaciones — Gobierno de Chile

Subsecretaría de Economía — Gobierno de Chile

Subsecretaría de Hacienda — Gobierno de Chile

Subsecretaría de Minería — Gobierno de Chile

Subsecretaría de Energía — Gobierno de Chile

Subsecretaría de Ciencia, Tecnología, Conocimiento e Innovación — Gobierno de Chile

Agencia Nacional de Inteligencia — Gobierno de Chile

NATIONAL CYBERSECURITY POLICY

2023-2028

CICS Interministerial Committee on Cybersecurity

Gobierno de Chile

gob.cl