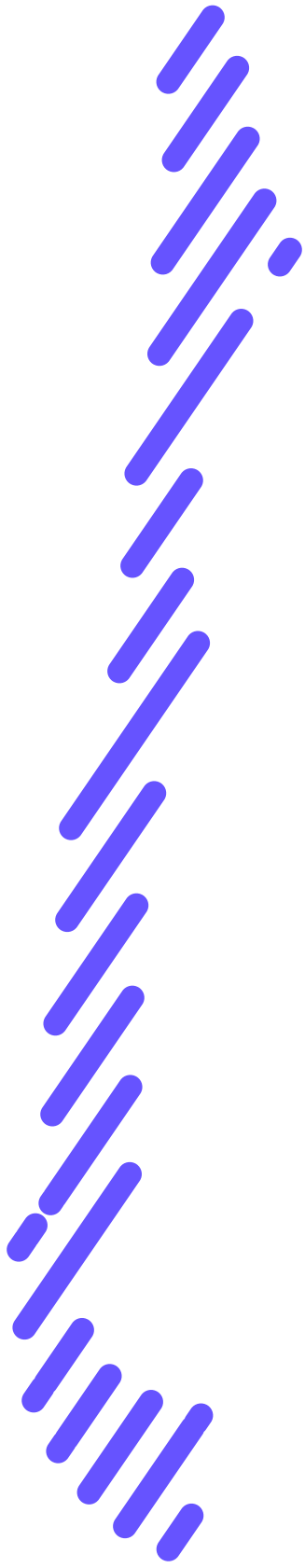
Chile´s Path to Cybersecurity

A Brief View Of Our Reality

November 2023



CHILE´S PATH TO CYBERSECURITY.

A Brief View Of Our Reality

Edited by Michael Heavey, using AI tools
Graphic design by Aníbal Phillippi
Senator Kenneth Pugh Legislative Team
Chile, November 2023.

DIGITAL TRANSFORMATION STRATEGY

CHILE DIGITAL 2035


→COMMITTEE FUTURE CHALLENGES, SCIENCE,
TECHNOLOGY, AND INNOVATION

Senadora/Senator
XIMENA ORDENES N.

Senador/Senator
KENNETH PUGH O.

PROLOGUE

Senator Ximena Ordenes and Senator Kenneth Pugh, members of the **"Challenges of the Future, Science, Technology and Innovation"** Committee, are pleased to present the Cybersecurity Strategy that is part of "CHILE DIGITAL 2035" presented on May 19th, with the support of ECLAC, academia, and organized civil society.

The strategy outlines the main aspects to consider for its development in the next 12 years, committing the efforts of three consecutive governments at the national, regional, and local levels. It is expected to be a planning tool that guides development strategies and the allocation of necessary human, material, and financial resources, where public-private partnership is vital for progress, based on the common denominator in cybersecurity being "Collaboration and Cooperation with Commitment." Cybersecurity is much broader than proper risk management. It is a new culture that requires knowledge of cyber hygiene from an early age, detection of cyber talent, interoperability, new and improved digital identities provided by the State, protection of personal data, and industrial issues such as protecting critical information infrastructures. It even addresses online disinformation campaigns that jeopardize the Rule of Law, Democracy, and Human Rights.

Anything that goes wrong in the digital world can cause physical harm, such as deaths, economic losses, damage to reputation, and even political damage. In the long term, the main objectives of this strategy are based on the Cybersecurity Maturity Model for Nations (CMM) of the Global Cybersecurity Center at the University of Oxford, which establishes five different dimensions. The OAS has used this model as a measurement tool for the nations of Latin America and the Caribbean, with the support of the IDB, in 2016 and 2020. It presents an excellent baseline and evolution that allows measuring the impact of public policies, one of the aspirations of this effort, the first with a solid long-term political commitment.

DIGITAL TRANSFORMATION STRATEGY

Chile Digital 2035, F: Cybersecurity

Cybersecurity Digital transformation cannot progress without an adequate cybersecurity strategy. Chile must, according to its reality, establish policies and means that allow for the protection of its computer and communication assets, as well as its resilience against potential vulnerabilities or failures.

Cybersecurity is a broad concept that encompasses everything from the protection of personal data to the protection of critical information infrastructure. It also includes all activities associated with the protection of systems, networks, programs, devices, and data from unauthorized access or criminal use, as well as the practice of ensuring the confidentiality, integrity, and availability of information. Over the past decade, there has been a growing concern about the importance of cybersecurity and its impact on humanity. Considering the breadth of the concept of cybersecurity, a holistic approach is required, establishing multiple barriers of protection between different systems, networks, programs, and data (País Digital Foundation, 2021).

It is necessary to create an effective culture of hygiene, prevention, and defence against potential digital risks. To assess Chile's current situation in terms of cybersecurity, various international indices can be taken into account. According to the Cybersecurity Index developed by the International Telecommunication Union (ITU, 2020), Chile has a cybersecurity level significantly behind OECD countries and more advanced economies. Chile ranks 74th globally, even falling behind several Latin American countries such as Brazil, Mexico, Uruguay, and the Dominican Republic. This suggests that there is room for improvement. According to the ITU, Chile's strengths in cybersecurity are the robustness of its legal framework and its cooperation mechanisms, while its main weaknesses are technical aspects and its implementation capacity. Another measurement framework is the cybersecurity maturity model of nations from the University of Oxford (CMM), in its dimensions of strategy, culture, training, legal frameworks, and standards, with a range from 0 to 5, representing 5 as the optimum. The model itself is dynamic and adjusts to reflect achievements and advancements between measurements.

Currently, Chile is on average between a level 2 and 3, according to the latest measurement in 2020 conducted by the OAS with support from the IDB. It is worth noting that Chile launched its first National Cybersecurity Policy (PNCS) for the period 2017-2022 in April 2017, with 5 objectives and 43 measures, which has constituted an important advancement in addressing this challenge, and it is currently under review. The Law on Computer Crimes was updated, now Law No. 21,459, and both the new Law on Personal Data Protection, which creates the new "National Data Protection Agency," and the Cybersecurity Framework Law are currently in the legislative process in the Senate. The latter defines governance in the field, creates new organizations, and defines their scope, including the protection of critical information infrastructure and essential operators.

During 2023, a law on interoperability governance will be enacted to decisively advance the digital transformation of the State, as indicated by Law No. 21,180 and its regulations. In terms of awareness and culture regarding cybersecurity, Law No. 21,113 of 2018 declares October as the national cybersecurity month and promotes national cybersecurity exercises. Work is also being done on the creation of a Cybersecurity Institute under the Ministry of Science, Technology, Knowledge, and Innovation. Chile is a signatory to the Budapest Convention, including the 2nd protocol, for the cross-border fight against cybercrime. These efforts have sought to align current regulations with international standards and best practices, such as the relationship between cybersecurity and the treatment of personal data, security standards to be met in regulated industries and by the State, the classification of new computer crimes, the definition of an international policy on cyberspace and cybersecurity, among others. It is essential to have a national political agreement with a long-term vision to commit government efforts to evolve from a cybersecurity strategy to a national cyberspace policy, with a significant cybersecurity component. The legal framework for cybersecurity consists of a Law on computer crimes and a Law on interoperability governance, in addition to regulatory frameworks on "The Protection of Personal Data" and "The Protection of Critical Information Infrastructure" (the scope of cybersecurity). This is based on cybersecurity governance through a National Agency that allows for the coordination of different sectoral information technology security incident response teams (Computer Security Incident Response Team, CSIRT). And have all the necessary information to determine the "attribution" of a cyber attack to the country, and at the same time support the recovery of operability, resilience, and mitigation of the adverse effects of the attacks, generating evidence for their prosecution. This legal framework allows for the creation of the necessary organizations to manage the "National Cybersecurity System" (see Figure 1).

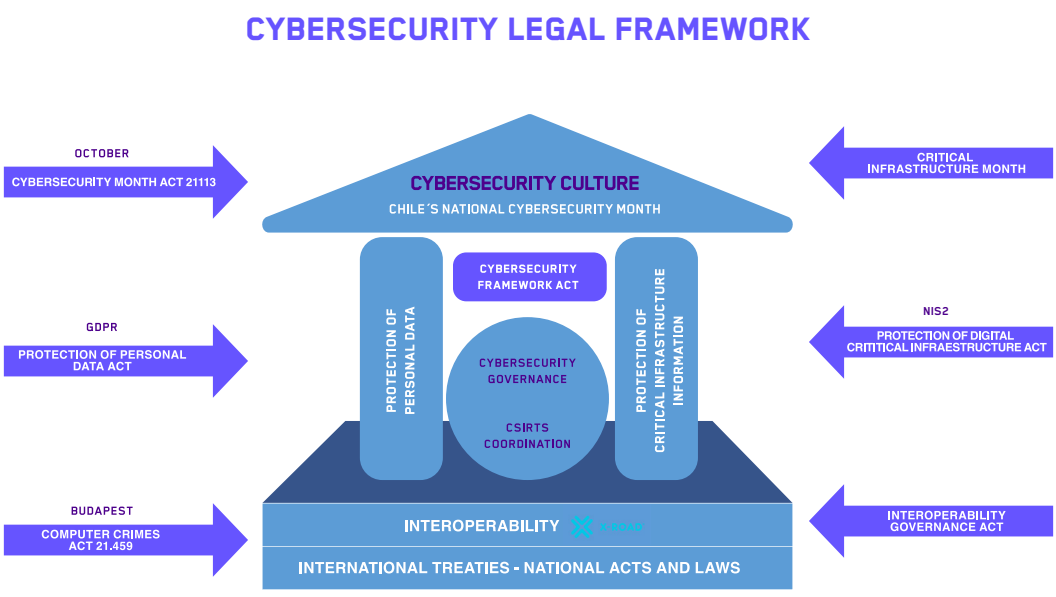
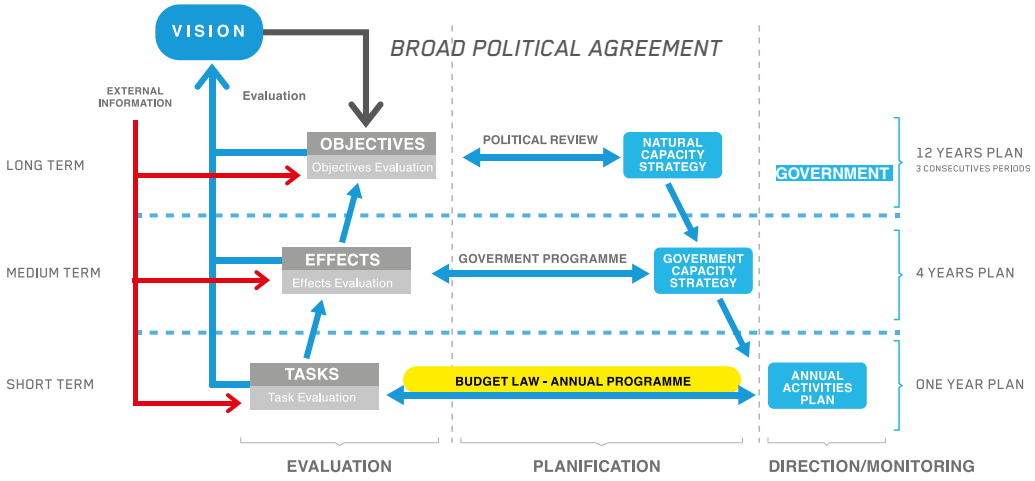


Figure 1 Source: Legislative Team of Senator Kenneth Pugh

For a national cybersecurity strategy by 2035, a three-horizon cybersecurity capability planning model is proposed, considering the long-term (12 years), medium-term (4 years), and short-term (one year). This will allow for the design of a capability planning system by levels. It is proposed to control the progress of the strategy in the long term by monitoring the tasks set each year in the Budget Law.

NATIONAL CAPACITY "PLANNING MODEL"

Figure 3 Cybersecurity Capacity Planning Model



Source: Senator Kenneth Pugh Legislative Team

OBJECTIVE 1 **Establish a dynamic, robust, and resilient national cybersecurity ecosystem**. It is necessary to establish an articulated and dynamic ecosystem vision to address the challenges of cybersecurity, as an emerging and priority area of public policy in a society that is becoming increasingly digital, depending on the internet and the security of its information and the infrastructure that stores, processes, and transports it. The integration of public and private sectors at the highest level and the generation of "digital trust" with new systems of identity and digital address and interoperability, along with robust and redundant networks for the transfer of digital information, and with the necessary backup systems to be highly resilient, are essential. It is fundamental to establish new cybersecurity governance, where the responsibilities and mandates of key actors, both governmental and non-governmental, are clearly defined and determined, as well as the reporting and response systems and the adequate allocation of resources to current and emerging cybersecurity problems and priorities.

LINES OF INTERVENTION

a. Create the National Agency for Cybersecurity and Protection of

Critical Information Infrastructure, being the highest-ranking body in the country in this matter, establishing regulations and oversight in cybersecurity matters. The National CSIRT (Computer Security Incident Response Team) will be part of its responsibility.

b. Develop sector-specific CSIRTs for Essential Operators of Critical Infrastructure.

c. Implement an interoperability system with encryption that allows traceability of information and its integrity, as well as secure cross-border data transfer. An open, free, and federated platform such as X-Road, already installed by the Colombian government and distributed by the Nordic Institute for Interoperability Solutions, is recommended.

d. Evolve to a new Digital Identity system with second-factor authentication and incorporated biometrics.

e. Create a national security accreditation system that defines the classification levels of information, especially sensitive and classified information.

f. Create the National Cybersecurity Operations Center (COC) for crisis management of national impact and determination of attribution of attacks, together with the National Cybersecurity Council.

g. Create the National Agency for Personal Data Protection.

h. Establish the National Cybersecurity Forum.

i. Define the National Strategy against Online Disinformation Campaigns.

j. Strengthen fiber optic networks with redundant links and backups using microwave and satellite technology. Contract secure data storage services within the national territory or with similar protection.

OBJECTIVE 2 A comprehensive national cybersecurity culture

Focused on the generation and availability of programs that raise awareness about cybersecurity throughout the country, focusing on cybersecurity risks and threats and ways to address them. This includes the development of appropriate institutions to promote cybersecurity. It also emphasizes the importance of reporting incidents and integrating cybersecurity into processes in a way that generates trust in citizens' online operations.

LINES OF INTERVENTION

a.Develop cyber hygiene programs in society for minors aged 2 to 12.

b.Develop training programs in digital skills oriented towards cybersecurity throughout the school education.

c. Create programs that mitigate violence on networks from an early age and address cyberbullying situations in minors.

d. Develop digital support programs for older adults to mitigate risks they are exposed to in cyberspace.

e. Carry out national cybersecurity exercises in October according to Law No. 21,113 and develop a comprehensive program to disseminate and update knowledge during that month.

f. Develop activities in November aimed at improving the response capacity of national critical infrastructure to incidents or digital attacks and promoting and updating knowledge of new threats.

g. Create a national culture that allows for the identification and reporting of cybersecurity incidents to the competent national authority. Incident Reporting mechanisms will be established by the National Cybersecurity Agency.

h. Reinforce trust in the use of the network and online services, both public and private.

i. Generate mechanisms to ensure the security of personal information.

j. Establish alternative programs to Military Service for the training of specialists in cyber defence.

OBJECTIVE 3 **Talent Management, capacity development, and cybersecurity industry.** Addresses the availability and implementation of high-quality cybersecurity training and education programs, with training and certification programs for competencies, as well as improving collaboration between the government and the industry to ensure that educational investments meet the cybersecurity education needs in all sectors, based on a governing body with expertise in these matters. R&D+i are relevant topics that should be encouraged to generate a self-sufficient industry that supports the country's cybersecurity management.

INTERVENTION LINES

a. Create the National Cybersecurity Institute (INCIBER) in Valparaíso to coordinate the advanced research network in cybersecurity, cyber talent development, and advanced training of instructors and specialists from different areas, along with the establishment of assessment and accreditation means for competencies, organization

of national exercises, and promotion and dissemination activities of new knowledge in cybersecurity.

b. Implement programs to identify and develop cyber talent from the age of 14.

c. Develop digital skills by providing certified competencies for students of all ages from 18 years old, without requiring previous academic training, using the French methodology of School 42.

d. Improve cybersecurity educational offerings, establishing training and competency accreditation programs according to national and international standards, for technical and university careers.

e. Promote the development of postgraduate scholarships in Cybersecurity, in globally prestigious universities, for doctoral and postdoctoral studies.

f. Promote the inclusion of women in cybersecurity careers to address the existing gender gap.

g. Annually reward outstanding women in Cybersecurity.

h. Annually recognize emerging leaders in Cybersecurity.

i. Encourage the training and retention of cybersecurity specialists to support the State, its services, and economic actors in general.

j. Explore coordination and resources to develop enhanced cybersecurity educational frameworks, with budget and expenditure based on national demand dynamically and with resources from the budget law.

k. Incentivize R&D in cybersecurity by promoting the development of a significant and efficient national industry that projects itself into international markets, with a focus on regional development and a budget indexed to a % of GDP and private contributions.

l. Collaborate in cybersecurity between the civilian sector and defence entities, through dual-use technology projects (civil and military use), along with the availability of adequate annual resources for their implementation.

OBJECTIVE 4 Effective and dynamic legal and regulatory frameworks, protection of rights in cyberspace, and prosecution of cybercrime.

Addressing the various laws and regulations, along with provisions related to cybersecurity, including legal and regulatory requirements and procedures, including legislation on cybercrime and assessment of the impact on human rights. It also considers legislative frameworks related to cybersecurity, including data protection, child protection, consumer protection, and intellectual property, as well as the responsibilities associated with handling, collecting, and storing such information.

INTERVENTION LINES

a. Permanently update the Law on Cybercrime based on the evolution of technology and additional protocols of the Budapest Convention.

b. Enact the new Law on Personal Data Protection and its permanent harmonization with the European General Data Protection Regulation (GDPR).

c. Require Essential Infrastructure Service Operators, as defined, to report cyber incidents to the National Cybersecurity Agency, under established regulations.

d. Enact the Law on Cybersecurity Governance and Protection of Critical Information Infrastructure (Cybersecurity Framework Law in the process as of April 2023), along with new crimes that harm this CI, such as cutting fiber optic cables and damaging digital public infrastructure.

e. Define a mechanism for registering SIM cards to identify their owners.

f. Form new Cybercrime Brigades of the PDI in each region of Chile, specializing in complex investigations and basic training in the establishment of technological crime scenes and digital chain of custody for all police forces.

g. Create the Advanced Cybercrime Investigation Laboratory at the Curauma building of the PDI (Investigative Police) in Valparaíso.

h. Develop specialized Cybercrime Prosecution Offices in the Public Ministry.

i. Train Prosecutors in the direction of investigation and prosecution of cybercrime and form judges in matters of competence for these digital crimes.

j. Generate policies, processes, and legislation for responsible disclosure of security vulnerabilities. Establish a policy or framework for responsible disclosure in public and private sector organizations and the right to legal protection for those who detect and report system vulnerabilities, within defined deadlines or with the consent of the responsible organizations.

k. Establish mechanisms for information exchange on cybercrime between the national public and private sectors, including cooperation with Internet service providers and other technology providers, coordinated by the National Cybersecurity Agency.

l. Identify and audit information assets, critical sectors, and operators regularly, establish cybersecurity requirements through policies and quality standards for supplies and services, and update, maintain, and protect computer systems and equipment.

m. Adopt the Tallinn Manual 2.0 on the Applicable International Law to Cyber Operations.

OBJECTIVE 5 International Cooperation and Regional Leadership in Cybersecurity Ensure the existence and functioning of formal and informal mechanisms that allow cooperation between national and cross-border actors to promote international cybersecurity through agreements aimed at deterring and combating cybercrime and its consequences. International collaboration should pursue effective collaboration in sharing cybersecurity information, incident management, and information handling protocols, and serve as a link for the development of comparable legislation. Likewise, make our country a regional reference for cybersecurity by supporting international collaboration agreements between the government, academia, and the main global cybersecurity references.

INTERVENTION LINES

a) Create a Cybersecurity Capabilities Center for Ibero-America, as a non-governmental organization based on National Universities, associated with the network of research centers supported by the Global Cybersecurity Capabilities Center at the University of Oxford. This will formally relate to the National Cybersecurity Agency, as well as the National Cybersecurity Institute (Inciber).

b) Create a regional international exercise to be executed in Chile by Inciber so that the official teams of the different CSIRTs in the region can personally get to know each other.

c) Establish formal links for exchange and collaboration by national institutions, both in the public and private sectors, and academia, with the main international instances and references in cybersecurity matters, both from friendly governments and international organizations.

d) Participate in the main governing bodies of the Internet, and in those international instances where the State of Chile has been invited, ideally through a Special Ambassador for Cyberspace.

e) Promulgate Chile's International Policy for Cyberspace, where our position regarding the security and neutrality of the network is stated.

f) Establish mechanisms for the exchange of information and evidence on cybercrime between different countries that are signatories to the Budapest Convention.

g) Participate with a national delegation in the Cyberex exercise in Spain, organized by Incibe, in September each year, and in those exercises where a national delegation is invited, such as those organized in Greece by ENISA and the United States.

h) Participate annually in the military exercise Locked Shields in Tallinn, Estonia, at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

GOALS

In this framework, the following is proposed:

*** Creation of the National Institute of Cybersecurity and the Cybersecurity Capability Center of Ibero-America by 2023.**

*** Creation of new national agencies for Personal Data Protection and Cybersecurity and Protection of Critical Information Infrastructure by 2025.**

*** Creation of all sectoral CSIRTs and the National COC by 2030.**

*** Investment of R&D expenditure in Cybersecurity as a percentage of GDP at 0.1% by 2025 and 0.2% by 2030.**

*** Training of 30,000 certified professionals in Cybersecurity by 2035, with at least 30% of them being women.**

*** Achieving a "Cybersecurity Maturity" close to State 5 or "Dynamic" for a nation by 2035, according to the CMM of the University of Oxford, in all Factors with at least State 4 evaluation and externally measured.**

Note: the complete Document "Chile Digital 2035" available at www.forociber.cl

"Chile Digital 2035" was the cornerstone of a Cybersecurity Task Force in 2022".

In 2022, the Challenges of the Future Committee of the Senate invited a selected group of 140 experts from academia, purveyors, lawyers, and other backgrounds to form a Task Force to analyze cybersecurity in Chile and to propose alternatives to improve our reality.

After several meetings and hundreds of man-hours of work, the Task Group work was synthesized in a document named: **"Building Cybersecurity in Chile"**

→BUILDING CYBERSECURITY IN CHILE←

After several meetings and hundreds of man-hours of work, the Task Group work is synthesized in a document named: "Building Cybersecurity in Chile"

This work had an important recognition of the European Union, as is stated in the following:

→PRESENTATION

Cybersecurity is a constant challenge in modern societies, where collaboration is the cornerstone for resilience in cyberspace, where a significant portion of our daily activities take place.

Countries must make substantial efforts to address this matter with a holistic vision and a sense of urgency, working on new legislation and regulations, innovation, education, and professional training. Above all, creating a cybersecurity culture that allows all its citizens to benefit from the Fourth Industrial Revolution in which we are immersed.

Europe has taken necessary steps to consolidate cybersecurity by creating regulations, research and development, institutional frameworks, and governance, both at the member state and community levels. Today, this enables them to have a European Center for Cybersecurity in Bucharest, Romania, and updated powerful regulations known as NIS2, which aim to protect critical infrastructure and entities, as well as the future Cyber Resilience Act, ensuring the security of connected products.

We observe with great interest the steps your country is taking in cybersecurity matters. We recognize the efforts made through the Chilean Senate, which are reflected in this document that undoubtedly contribute to a better understanding, and wider dissemination of cybersecurity culture, and, above all, serve as an important input for your legislation and governance in cybersecurity and digital transformation.

We applaud the efforts of the Chilean academia, civil society, entrepreneurs, and professionals who have worked on this document. We are open to a fruitful and long-lasting relationship with the establishment of the National Cybersecurity Forum, which we hope will be mutually beneficial.

MARGRETHE VESTAGER
Executive Vice President of the European Commission

→EXECUTIVE SUMMARY

The report of the "Chile Digital 2035" Strategy, regarding cybersecurity, states in its opening paragraph:

"It is not possible to advance in digital transformation without an adequate cybersecurity strategy. Chile must, according to its reality, establish policies and means that allow the protection of its computer and communication assets, as well as its resilience against potential vulnerabilities or failures."

Based on this premise, the Cybersecurity Task Force worked by providing inputs for security strategies, with many insights and proposals that allow us to holistically visualize the pains, needs, paths, and opportunities that enable us to mature in cybersecurity as a country.

Facing this requires recognizing some important aspects of the steps we are taking. Chile has a National Cybersecurity Policy for 2017-2022 with 25 objectives and 43 measures, which have been a roadmap to address the cybersecurity challenge. We have a law that designates October as Cybersecurity Month, which has helped raise awareness among Chileans.

We have also made progress in modernizing our regulations through Law No. 21,459, which "Establishes norms on computer crimes, repeals Law No. 19,223, and modifies other legal bodies to adapt them to the Budapest Convention," being an important advancement. Furthermore, work is underway to create a Cybersecurity and Essential and Critical Operators of Information Framework Law, as well as regulations for the protection of personal data.

Moreover, the academic sphere has taken measures to prepare new professionals who are increasingly necessary to meet the requirements of organizations of all sizes. Alongside the creation of undergraduate programs in the field, postgraduate studies in related subjects are also being developed. However, the road is long, and forming habits of cyber-hygiene, detecting talent, and reducing digital literacy gaps are ongoing challenges.

It is interesting to note the internalization of the importance of cybersecurity, with increasing awareness of our enormous dependence on the Internet, information systems, and everything that entails in our daily performance.

Several recent cybersecurity events compromised important IT assets, generating healthy concern and occupation in the field, thus recognizing the tremendous vulnerability we have as a country in cyberspace.

With all of the above, we are building a legal framework for cybersecurity but there is still a long way to go. Through initiatives like this Task Force, the country is reducing gaps and vulnerabilities, maturing our cybersecurity.

The work of the Task Force was subdivided into 7 working tables, which were:

1) **CYBERSECURITY AND PUBLIC POLICIES**
2) **CYBER TALENT DEVELOPMENT**
3) **ADVANCED RESEARCH IN CYBERSECURITY**
4) **EMERGING TECHNOLOGIES**
5) **ESSENTIAL SERVICE OPERATORS**
6) **ONLINE DISINFORMATION**
7) **INTEROPERABILITY AND DIGITAL IDENTITY**

The 7 working groups analyzed the national reality on each topic, following a similar structure:

Introduction, Context, Future Challenges, Proposals, and Conclusions. They provided their respective reports in December 2022, offering important insights and inputs on the future evolution of cybersecurity in our country for the coming years. They reflect inevitable pains, aspirations, and needs ranging from appropriate regulatory frameworks to governance that allows for secure and robust participation of our country in cyberspace.

The working groups conclude, in a similar fashion, on concepts such as the need for a robust policy, further digital transformation of the government, the need for change management, and the necessary creation of appropriate governance, while also promoting education and training in cybersecurity. These topics, developed to a greater or lesser extent depending on each group's subject matter, indicate a significant convergence of what is considered relevant in national cybersecurity.

The work of this team of specialists does not end with the conclusion of the Task Force convened by the committee on Future Challenges but extends to the creation of a "permanent forum," sponsored by the Senate, intended to be an advisory and voluntary body where concerns and initiatives can be channeled to achieve better legislation and updated regulations in this rapidly advancing ecosystem.

Thus, the work of the table concludes with a description of what will be the **"National Cybersecurity Forum."**

A brief of the contents of each chapter is presented:

→Chapter 1: **CYBERSECURITY AND PUBLIC POLICIES**

This chapter details the proposed changes to the National Cybersecurity Policy (PNCS) by a working group of experts in the field. The proposed changes are based on an evaluation of the evolving context since 2017, and the aim is to contribute to the legislative work in its crucial role of legally regulating cybersecurity and support the executive branch and its specialized agencies in formulating the second version of the PNCS.

The proposed changes include the formulation of two new objectives: Promote cybersecurity public policy that favors governance in the field, facilitate the inclusion of sectors, areas, and experts in the subject, and create opportunities for various categories of contributions; and Further promote the digital transformation of the government.

Also outlines the challenges the PNCS faces, such as considering the cybersecurity system as a whole, not as isolated regulations, and providing guidelines and/or recommendations for the private sector regarding what small, medium, and large companies should have in terms of cybersecurity.

Additionally, it outlines the importance of promoting regulatory unification to put an end to the regulatory dispersion of recent years, as well as promoting a cybersecurity industry that meets national needs, particularly concerning strategic requirements and even enabling the exportation and/or integration of these technological developments.

→Chapter 2: **CYBER TALENT DEVELOPMENT**

Creating a culture of cybersecurity is essential for protecting citizens and businesses from cyber threats. To achieve this, it is necessary to develop actions in the short, medium, and long term. Short-term actions include creating a slogan and logo to represent the campaign, as well as creating and disseminating cybersecurity tools for businesses.

Medium-term actions include preparing an information sheet for employees that contains relevant messages for each area of the business, providing a list of easily implementable measures to immediately improve their digital security, surveying teachers at different levels to identify those who would be interested in participating, and establishing awareness stages that address the basic needs of each educational institution.

Long-term actions include establishing a national work plan to be implemented in each region, creating standardized documentation to ensure consistent knowledge delivery at the national level, and having an updated registry of strengths and weaknesses of public officials in various institutions.

Additionally, suggests creating ongoing awareness campaigns tailored to citizens' specific needs to reinforce the creation of a national culture of cybersecurity; also suggests creating a mandatory digital certification for students in schools and high schools, as well as developing accompanying tools to help older adults access information and support for safe internet navigation.

All these proposals are supported by public and private funding

→Chapter 3: **ADVANCED RESEARCH IN CYBERSECURITY**

The need for a National Cybersecurity Strategy to ensure that researchers have access to infrastructure, resources, visibility platforms for their results, and technology transfer opportunities will position the country among the leaders in the R&D industry for cybersecurity by 2035.

Taking the Cybersecurity Maturity Model for Nations (CMM) as a model to consider, the development aims to achieve a "3-Established" level of maturity in R&D for cybersecurity in the short term (4 years), a "4-Strategic" level in the medium term (8 years), and a "5-Dynamic" level in the long term (12 years).

To achieve these levels, it is relevant to identify and consider adequate sources of funding for IAC activities, regional and international actors involved in research, and the creation of testing and prototyping laboratories for R&D projects in cybersecurity, a distributed national laboratory for cybersecurity, and emblematic projects in laboratories that allow leverage between industry, the State, and academia.

Additionally, communities around priority areas of IAC, an observatory unit that identifies emerging problems related to new technologies or threats, and recognition in relevant rankings that Chile climbs into the quadrant of leaders in cybersecurity research and innovation must exist.

→Chapter 4: **EMERGING TECHNOLOGIES**

The proposed methodology for managing innovations based on emerging technologies in the field of cybersecurity is designed to help identify and assess the potential of a specific technology.

It involves reidentifying the problem that the technology aims to address, projecting the advancement of the technology over time, and considering the technical feasibility of implementing solutions based on the technology.

The framework is composed of a methodological analysis that includes identifying the technologies that impact cybersecurity, understanding the state of the art concerning emerging technologies, identifying future challenges and their domains and categories, proposing their application and uses, and analyzing companies that may be working in these fields. 14 categories that will guide the near future of companies dedicated to or involved in cybersecurity include Identity Orchestration, Data Firewalls, Security Creds, Outsourced Security, SaaS Security, Crypto Defence, Security-Infused Networks, Cyber Automation, API Protection, Cyber Insurance, Shift Left Security, Secure Data Sharing, Auto Security, and Post Quantum Cryptography.

These categories are discussed in the context of the challenges that organizations face in terms of financial costs and reputation damage when hackers steal their data or when it becomes publicly leaked.

→Chapter 5: **ESSENTIAL SERVICE OPERATORS**

A summary of a joint effort from professionals from different backgrounds to structure a policy that promotes collaboration between the public and private sectors.

It is an important reference and input for decision-makers, combining multiple perspectives to contribute to national cybersecurity. The policy is based on the Critical Infrastructure Information Act of 2002 (CII Act) which protects voluntarily shared information regarding the security of private and government critical infrastructure.

It establishes uniform procedures for receiving, validating, handling, storing, marking, and using Critical Infrastructure Information (CII) voluntarily submitted to the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS).

The safeguards provided by the PCII Program facilitate the voluntary exchange of information between owners of CII and ESOs and the government. The information sent for PCII protection should be submitted voluntarily, not be available in the public domain, and not be submitted in place of complying with any regulatory requirement.

It serves as a proposal for the establishment of a **National Policy for Critical Infrastructure** which will establish the foundation for facing risks and threats, originating from both the physical and digital worlds, that could compromise our country's operations.

Establish regulations and implementation deadlines for Critical Industry Operators based on identified risk levels (high, medium, low), and enhance cooperation and knowledge exchange in cybersecurity with international parent companies or related companies of Critical Industry Operators.

Develop an annual self-assessment plan for cybersecurity risks based on predefined guidelines, and include Critical Industry Operators in sectorial exercises. Consider exercises involving catastrophic failure scenarios for Critical Industry Operators.

→Chapter 6: **ONLINE DISINFORMATION**

A National Strategy Against Online Disinformation 2035 (ESNACDEL-2035) has been developed with three thematic pillars: institutional framework, education, and defence. For each pillar, initiatives have been established, outlining actions aimed at achieving specific objectives, defining responsibilities, involved actors, as well as an estimated timeframe.

The initiatives are interdependent, complementary, and mutually reinforcing, and they are closely interconnected. The institutional framework pillar focuses on establishing a regulatory framework to regulate behavior on social media platforms, assign/create responsible bodies to address identified threats of disinformation and misinformation and regulate influence.

Measures can be categorized based on their focus: prevention, reaction, and effective engagement among stakeholders.

The strategy aims to generate technology to prevent and respond to the phenomenon effectively, raise public awareness, develop national critical thinking through formal education, and establish a specialized defence entity focused on developing cutting-edge teaching and research to enhance the capacity to respond to the impact of the phenomenon in a

holistic context and generating reactive and proactive capacity through a specialized organization.

This will enhance the ability to respond to the impact of the phenomenon in a comprehensive way and create both proactive and reactive capabilities through a dedicated institution. The achievement of each objective is dependent on resources, especially financial resources, and the suggested timeframe is just a rough estimate.

→Chapter 7: **INTEROPERABILITY AND DIGITAL IDENTITY**

Explores the importance of interoperability and digital identity in Chile today. It begins by introducing the need for secure and reliable information flow in cyberspace, as well as the need for conditions to be established for individuals and institutions to interact with each other.

It then looks at the current regulatory framework for interoperability and digital identity in Chile, which does not have a specific regulation on interoperability but does have Law No. 19.799, which introduced the concept of interoperability and determined obligations and the entity responsible for establishing standards.

The success factor for introducing a successful digital transformation, in which Interoperability and Digital Identity are key, lies in the processes and transformations of the activities and procedures that people apply, so that they can facilitate them without feeling threatened, but rather empowered by the tools that are incorporated.

It is important to establish discipline from the origins of projects involving changes, to establish adaptive competence as a requirement, to manage the acquisition of adaptive competencies, to establish user experience as a hygiene factor, and to plan a set of phases that allow for dimensioning and defining the interventions that are required before, during, and after the completion of projects involving changes, especially interoperability.

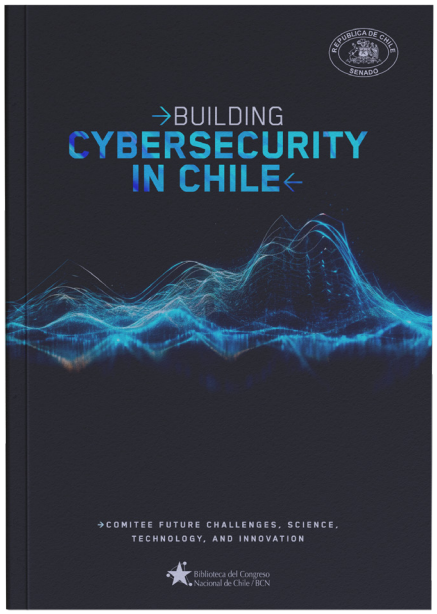
Finally, it looks at the generation of value through interoperability and digital identity, considering technical criteria such as operational governance, formal agreements, and organizational governance.

→Chapter 8: **THE NATIONAL CYBERSECURITY FORUM**

The National Cybersecurity Forum is a voluntary entity, of a public-private nature, that brings together academia, civil society, the State, trade organizations, non-governmental organizations, professional associations, and individuals related to the field of cybersecurity and disruptive technologies, among others, to contribute to a healthy discussion and dissemination of knowledge that becomes a national reference in the field. It will be convened by the President of the Senate and will have a permanent Director appointed by him. Forum members will be grouped into working groups according to their affinity for the topics to be discussed, based on the interests they express when registering. The ultimate goal of the Forum is to contribute to the situational awareness of the main national and international trends, objectives, and regulatory lines of action, and to promote societal changes toward cybersecurity and emerging technological trends in the citizen-state relationship.

***** *The English and Spanish versions of this book are available at:*

www.forociber.cl



THE NATIONAL CYBERSECURITY FORUM

The National Cybersecurity Forum The proposal to create a National Cybersecurity Forum has been considered a relevant initiative and has been embraced by the presidency of the Senate, creating a novel institution that allows for a space of discussion and dissemination of knowledge, with a national perspective.

The recently created institution, with the support of a foundation called the **"Chilean Cybersecurity Alliance,"** will orderly create instances of dialogue, healthy discussion, and the generation of proposals for public policies, so that the Parliament can channel them into laws and regulations that regulate the national cyberspace.

The National Forum, which in many aspects follows the Spanish model that depends on the executive branch, will hold in-person sessions three times a year, in April, July, and October, to present its progress on the topics that are being addressed.

Operationally, the Forum will work based on the formation of virtual working groups, where members, according to their interests and knowledge, guided by a director, will present, discuss, and propose topics that improve the national reality in cyberspace. These mentioned working groups will be formed based on the CMM of the University of Oxford, without prejudice to address specific and punctual topics, such as cyber health, cyber-hygiene, disruptive technologies, and online disinformation, among many others.

With this in mind, the forum was constituted on October 2nd in a special session in the Hall of Honor of the headquarters of the National Congress in Santiago, with the presence of almost 400 guests, which is an important recognition of the project undertaken.

The President of the Senate, Senator Juan Antonio Coloma, highlighted this novel initiative that represents a valuable contribution that brings together academia, civil organizations, and professionals among others, whose common denominator is to work for cybersecurity and digital transformation, pillars for the objective of creating a better country, more modern and inclusive.

On their part, Senators Ximena Ordenes and Kenneth Pugh, at this starting moment, recognized the dedication and efforts that are being made in educational and formative processes from different regions.
It is important to highlight that one of the great achievements of this forum is the explicit recognition that:

"In cybersecurity, we do not compete, we collaborate!"

More details at: **www.forociber.cl**

The next steps of the forum for the April meeting will be to bring together regulatory authorities and those regulated to learn about their vision and experiences, not only at a national level but also internationally. Understanding how different realities are faced in comparison to Chile will allow us to take important steps, recognizing experiences and avoiding the repetition of practices that may have seemed appropriate but are inadvisable due to real circumstances.

To meet the above challenges, a **"Public Policies Summit for Cyberspace"** will be organized every year, under the name of Cyber Policy Summit.

More Details at: **www.cyberpolicysummit.org**

CHILE´S PATH TO CYBERSECURITY

WHAT WE HAVE ACHIEVED SO FAR

National Cybersecurity Policy (PNCS)

We have updated the first version dating back to 2017, addressing issues such as greater dissemination with an emphasis on gender and age diversity. The importance of education and training as relevant pillars for a safer society is recognized. The importance of R&D and innovation, as well as applied research, is also reaffirmed.

The law declared October as Cybersecurity Month

This initiative, approved in 2018, has proven to be a tremendous incentive to promote the dissemination of cybersecurity in the country. In just 5 years, the set awareness objective has been achieved and reflected in publications, seminars, exhibitions, and other activities, which have experienced explosive growth, thus recognizing the importance of the subject matter.

The Law against Cybercrime and Budapest Convention

Our legislation on cybercrime, after many years, was correspondingly updated, assuming the country's adherence to the Budapest Convention and its protocols, which facilitate the cross-border prosecution of such crimes. New offenses and their penalties are specified.

Digital Transformation of the State

The government has set a timetable to gradually force the digital transformation of the State, which has a horizon of 5 years, and considers a deep change in procedures and information management as legislation is created and changes occur.

WHAT ARE WE DOING TODAY?

In our parliament, two very important laws must be concluded before the end of the year:

1) Personal Data Protection Law: which is based on the GDPR and creates a powerful institution for the protection and care of personal data. It establishes a National Data Protection Agency that will be responsible for ensuring strict compliance with the legislation.

2) Cybersecurity Framework Law: It creates the necessary infrastructure for the existence of a National Cybersecurity Agency, which will regulate and supervise cybersecurity, and will also have the National Csirt. It is modeled according to NIS2 and incorporates some interesting new practices from European legislation, such as the Belgian law regarding the reporting of vulnerabilities detected but not exploited by researchers within specific timeframes. It also introduces sanctions and obligations, as well as making some recommended practices in ISO standards mandatory.

Additionally, in parliament, there are discussions about some aspects of Artificial Intelligence, particularly regulatory aspects, but considering its use in the case of it being used to commit a crime.

In our Academy, there is a growing interest in the creation of careers, undergraduate and postgraduate studies, and even professional degrees related to cybersecurity, as well as the accreditation of cybersecurity competencies by internationally recognized entities. This recognizes the lack of trained professionals and the effort to reduce the gap, also generating interesting job opportunities.

CHALLENGES FOR THE NEAR FUTURE

Chile is in the process of digital transformation, and for this, it must generate governance and regulations, taking advantage of international experiences, especially those from Europe.

Digital Identity:

We must progress towards a robust identity that allows us to provide the appropriate certainty that the person accessing government services is who he claims to be. Our country has a well-developed identity registry system, but it must include validation and authentication systems, with personal passwords and biometric characteristics or other means. We aspire to have a robust ID system like the one used in Estonia.

Interoperability:

Chile must establish a definitive model of interoperability, based on the European model of 4 layers, generating an institutionality that promotes its implementation. From the same interoperability, we must move towards a digital address and a universal medical record, which will allow a true revolution in the government's service to its citizens.

Cyberdefense:

Our country must advance in cyberspace, seeking to encourage its defense in the new theater of operations that is cyberspace, working on defense mechanisms, resilience, and recovery, as well as cyberattack strategies. Our development in cyberspace requires applied talent because in this new and decisive scenario, it is the best defense.

Increase police Capacities:

It is important to strengthen police cybersecurity and cybercrime prosecution capacities, especially the PDI, providing new processing capabilities, custody of evidence, and forensic analysis of cybercrimes that address new modalities and actors.

National Digital Transformation Office:

To promote an actual digital transformation that goes beyond the governments in power and their particular interests, Chile must strive for the development of governance that promotes the necessary technological and operational changes, generating regulations and being a facilitator of these changes.

We must evolve from an office under a political ministry to a national institution with long-term objectives that allow for a quick and orderly transition towards a Digital Republic.