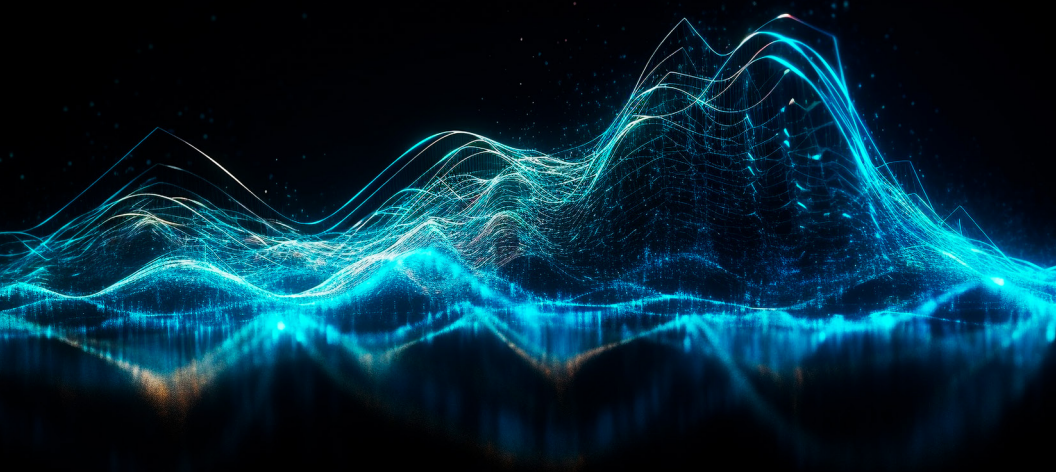
REPÚBLICA DE CHILE
SENADO

→BUILDING CYBERSECURITY IN CHILE←



→COMITEE FUTURE CHALLENGES, SCIENCE, TECHNOLOGY, AND INNOVATION

Biblioteca del Congreso Nacional de Chile / BCN

Michael J. Heavey
Editor-in-Chief

Tania Yovanovic, Raimundo Roberts, Carolina Muñoz, Pascal de Smet d´Olbecke
Assistant Editors

Carolina Sancho, Pelayo Covarrubias, Xavier Bonnaire, Tania Yovanovic, Romina Torres, Pedro Pablo Pinacho, Rodrigo Alfaro, Luz Cardona, Eduardo Morales, Igor Carrasco, Jorge Gatica, Felix Staicu, Francisco Méndez, Carla Illanes, Julio Cámara, Kenneth Pugh
Editors

Aníbal J. Phillippi
Graphic Design

Building Cybersecurity in Chile - Cybersecurity Task Force of the Future Challenges, Science, Technology, and Innovation Committee, 2022. Michael J. Heavey, Editor-in-Chief, Valparaiso, Chile, Ediciones Biblioteca del Congreso Nacional de Chile 2023, 211 pages.

Senate-Chile Future
Challenges, Science, Technology, and Innovation Committee - Senate Chile Cybersecurity Task Force 2022

DISCLAIMER: This english version of " Construyendo la Ciberseguridad en Chile" was translated from spanish by the Editor in Chief, helped by AI tools such as DeepL, Grammarly, ChatBot, and others".

SECOND EDITION NOVEMBER 2023

PREFACE

The work carried out by the Cybersecurity Task Force marks a milestone in collaboration to address an issue that affects all of us in the world of the Fourth Industrial Revolution and demands our best efforts to have a safer country in cyberspace.

Multiple challenges have been analyzed, resulting in important proposals that should serve as a powerful guide to advance in cybersecurity and emerging technologies that impact our society, and will undoubtedly bring about enormous economic, social, and above all, human changes.

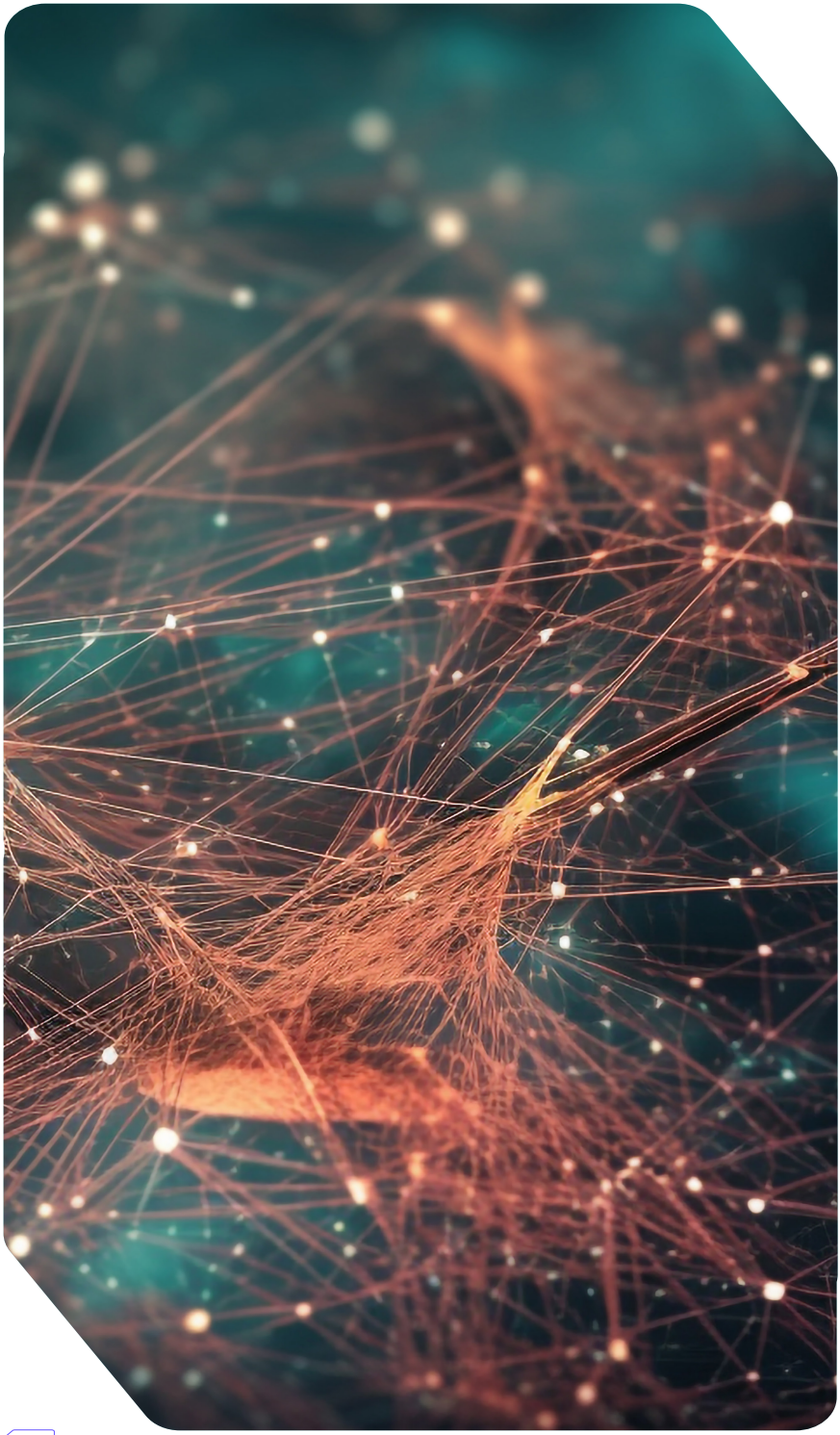
The Senate of the Republic has embraced many initiatives through the Future Challenges Committee, which have served as the basis for new legislation. This has been made possible through the support of specialists and academics who have generously contributed their time and expertise to highlight topics that have an impact on the country's development.

Cybersecurity has undoubtedly become a reality that was not even discussed a few decades ago. It has now become a cornerstone of the nation's future, rapidly moving towards the digital transformation of our society. Therefore, we must advance in developing the capabilities to navigate scenarios that will test our institutions and their resilience, and consequently, our democracy and way of life.

Considering the above and the recommendations of this report, we will promote the creation of the "National Cybersecurity Forum" from the Senate, following the experience of other nations with similar initiatives. This important step will formalize the institution's constant interest in the impact of emerging and influential technologies, always aiming for the future well-being of the nation.

The Forum will be a permanent platform to convene the collaboration of the best experts, specialists, and knowledgeable individuals, not only from academia but also from the industry and civil society organizations, enabling us to work on this subject with the necessary foresight.

JUAN ANTONIO COLOMA CORREA
PRESIDENT OF THE SENATE OF THE REPUBLIC OF CHILE



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

→COMMITTEE FUTURE CHALLENGES, SCIENCE, TECHNOLOGY, AND INNOVATION

PROLOGUE

Senator
XIMENA ORDENES N.

Senator
KENNETH PUGH O.

The achievement that was reached in 2021 under the auspices of the Senate's committee on Transportation and Telecommunications, resulting in the Chile Digital 2035 document, was made possible by the participation of the Association of Telecommunications Companies, along with Cepal, academia, and civil society. This allowed for the proposal of a roadmap for the country's digital transformation over a 12-year horizon.

One of the important topics addressed in that document is the inclusion of cybersecurity. In 2022, as members of the Committee on Future Challenges, we decided to promote cybersecurity as a significant aspect of our vision for the future, considering its high and growing impact on society.

In line with this, we proposed and sponsored the creation of a Cybersecurity Task Force, aiming to convene a broad range of professionals from academia, industry, civil organizations, the Armed Forces, law enforcement, as well as many experienced professionals in these fields.

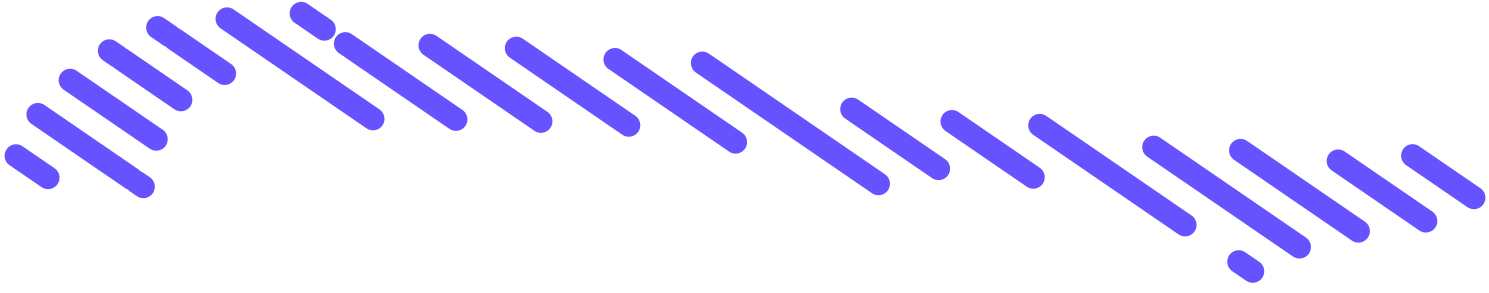
The purpose was to build upon the progress already made and propose new alternatives and paths to be taken by both the executive and legislative branches, providing a strong boost to national cybersecurity development.

We greatly appreciate the more than 140 professionals who accepted the challenge to work and dedicate their time. Their collective effort amounts to several thousand hours of work, aimed at discussing the ways to create a society that is more familiar with cybersecurity, more resilient, and more innovative. We aim to leverage our capabilities and talents to the best of our abilities while recognizing our failures and shortcomings.

The Cybersecurity Task Force addressed various areas, working on multiple fronts, and the findings and conclusions are presented in the following chapters.

After this magnificent exercise, we are certain of the need for a formal and consultative body that convenes specialists, academics, business leaders, civil society members, and others in a permanent forum, under the auspices of the Senate. This forum would allow for the channeling, presentation, discussion, and debate of these matters, enriching legislative and regulatory work with the necessary agility and depth, enabling us to maintain a leading position in cybersecurity.

This document will serve as a guiding light for the development of cybersecurity in Chile, based on the principle of necessary collaboration among all, as no one is immune to vulnerabilities that can be maliciously exploited.



INTRODUCTION

"The Committee "Challenges of the Future, Science, Technology, and Innovation," in addition to carrying out its legislative work, has established itself as a platform for generating foresight and addressing topics beyond political contingency, but with a future-oriented perspective. From this Committee, topics have emerged that will certainly influence the future of the nation, and they are condensed in the book "Chile Has a Future, from its Territories," published this year, which contains the initiatives addressed from its creation until the year 2021.

The creation of the Cybersecurity Task Force within this Committee was an initiative promoted by Senator Ximena Órdenes and Senator Kenneth Pugh, to raise awareness about cybersecurity issues already raised in the report of the Chile Digital Strategy 2035 conducted under the auspices of the Senate Committee on Transport and Communications. Its purpose is to develop these matters in a framework of broad collaboration.

The task force formally started on July 7, 2022, in a special session of the Committee on Future Challenges (chaired by Senator Francisco Chahuán), which convened 140 specialists from academia, industry, public services, police, armed forces, civil organizations, and other professionals focused on issues related to cybersecurity, digital transformation, and public policies. They accepted the invitation to participate and contribute their time and effort.

The work presented here involved a personal commitment through countless meetings and thousands of work hours, readings, and conversations with the sole purpose of contributing to this initiative while dedicating personal and professional time. This work adheres to the guiding principle that governs those of us in the field:

¡In cybersecurity, we don't compete, we collaborate!

Thanks to all who participated in this great project.

MICHAEL J. HEAVEY
Civil Electronic Engineer
Cybersecurity Task Force Coordinator
Committee on Future Challenges, Science, Technology, and Innovation
Valparaíso, April 2023.

TASK FORCE ORGANIZATION

The work was mainly conducted virtually, taking advantage of the benefits of technology. Between July and December, this important task was carried out, which is condensed into the following chapters and will serve as a guide and inspiration for the processes of organization, governance, regulations, and legislation that the country needs to project itself into the future as a true Cybersecure Digital Republic.

Based on the Cybersecurity chapter of the document 'Chile 2035,' the task force was organized into 7 subcommittees, each led by a chair and a co-chair:

→01

Cybersecurity and Public Policies, led by **Dr. Carolina Sancho** and **Pelayo Covarrubias, MA.**


→02

Cyber Talent Development, led by **Dr. Xavier Bonaire,** and **Tania Yovanovic.**


→03

Advanced Research in Cybersecurity, led by **Dr. Romina Torres** and **Dr. Pedro Pablo Pinacho.**


→04

Emerging Technologies, led by **Dr. Rodrigo Alfaro** and **Dra. Luz Cardona, MA.**


→05

Essential Services Operators,
led by **Ing. Eduardo Morales** and
Igor Carrasco, MA.


→06

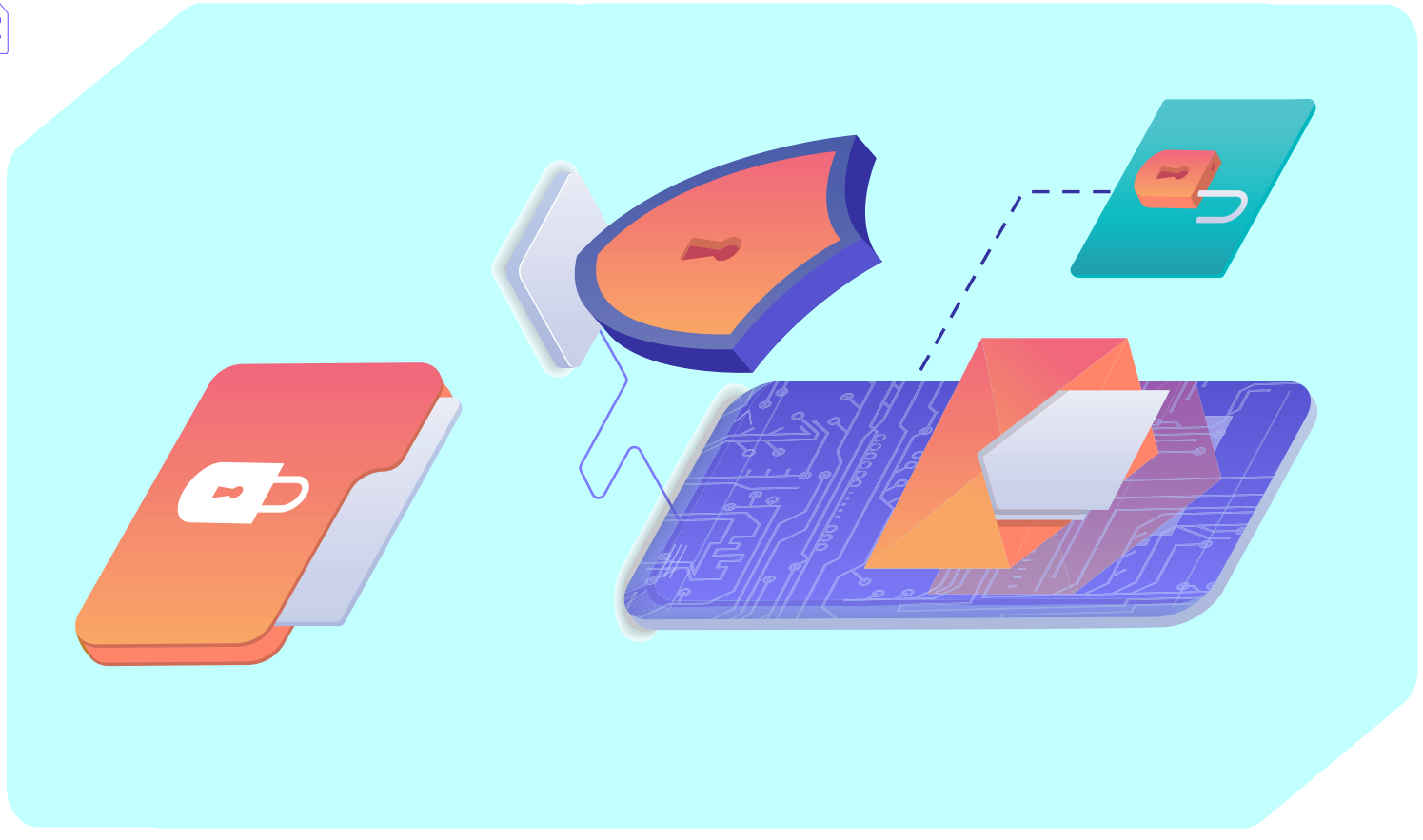
Online Disinformation, led by
Dr. Jorge Gatica and **Félix Staicu, MSc.**


→07

Interoperability and Digital Identity,
led by **Francisco Méndez, MA.,**
and **Carla Illanes, MA.**


→08

National Cybersecurity Forum



INVITED TO THE CYBERSECURITY TASK FORCE

→Alberto Jara
→Alejandro Hevia
→Alex Pessó
→Alexandra Barros
→Alfie Antonio Ulloa
→Alfredo Diaz
→Amalia Pizarro
→Andrea Obaid
→Andres Barrientos
→Andrés Pumarino
→Benjamín Blanco
→Berioska Contreras
→Carlos Bustos
→Carlos Fuentes
→Carlos Lobos
→Carlos Manzano
→Carlos Montoya
→Carlos Parker
→Carmina Hernandez
→Catherine Narváez
→César Galindo
→César Pallavicini
→Christian Sifaqui
→Claudia Inostroza
→Claudia Negri
→Claudio Álvarez
→Claudio Galleguillos
→Claudio Reyes
→Cristián Rojas
→Danic Maldonado
→Daniel Álvarez
→Daniel Seco
→Daniel Velásquez
→Daniela Rusowsky
→Diego Philippi
→Edison Escobar
→Eduardo Costoya
→Felipe Rodríguez
→Fernanda Mattar
→Fernando Mejías
→Fernando Muñoz
→Francisco Correa
→Francisco Garcia
→Freddy Macho
→Gabriel Bergel
→Gonzalo Díaz de Valdés
→Guillermo Carey
→Guillermo Garcia
→Héctor González
→Helvecia Castro
→Hernan Espinoza
→Igal Neiman
→Ingrid Inda
→Italo Foppiano
→Jaime Astorquiza
→Jaime Caiceo
→Javier Ramírez
→Jessica Matus
→Jorge Arredondo
→Jorge Astudillo
→Jorge Flores
→Jorge Rojas
→José Fuentealba
→Jose Luis Perez
→Juan Carlos Ramirez
→Juan Huechucura
→Juan Ignacio Nicolossi
→Juan Lopizic
→Juan Pablo Gonzalez
→Julio Lopez
→Karin Quiroga
→Kristian Araoz
→Lidia Herrera
→Loreto Bravo
→Luis Silva
→Marcelo Wong
→Marco Zuniga
→Maria Francisca Yañez
→María José Escobar
→Mario Troncoso
→Marisel Cabeza
→Mauricio Cantergiani
→Mauricio Romo
→Maurizio Mattoli
→Michelle Bordachar
→Miguel Cisterna
→Miguel Solís
→Mirko Koscina
→Monica Retamal
→Pablo Itaim
→Paola Arellano
→Patricia Diaz
→Patricio Leyton
→Patricio Ovalle
→Paula Pinto
→Paulina Silva
→Pedro Huichalaf
→Pedro José Novoa
→Peter Waher
→Puppy Rojas
→Raúl Arrieta
→Renato Bustamante
→Ricardo Andrade
→Ricardo Dorado
→Ricardo Monreal
→Ricardo Seguel
→Ricardo Soto
→Ricardo Vásquez
→Rocío Ortiz
→Rodrigo Bustamante
→Rodrigo Díaz
→Rodrigo Pérez
→Rodrigo San Martin
→Romina Garrido
→Ruth Garrido
→Sebastian Berrios
→Sebastián Carey
→Sebastián Izquierdo
→Sebastián Vargas
→Sergio Leiva
→Taryn Revesz
→Thierry de Saint Pierre
→Victoria Hurtado
→Ximena Cisternas
→Ximena Sepulveda
→Yerka Yukich
→Pamela Calisto
→Cristian Rojas
→Paz Suarez
→Carolina Muñoz
→Felipe Rodríguez
→María Paz Ilabaca

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.

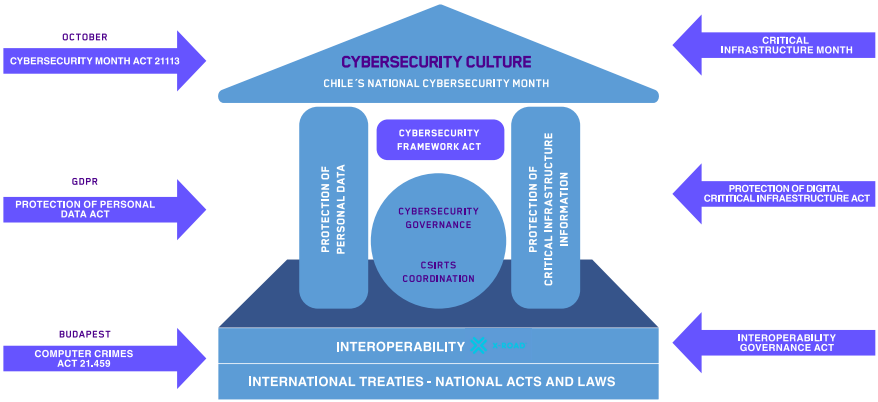
Moreover, the academic sphere has taken measures to prepare new professionals who are increasingly necessary to meet the requirements of organizations of all sizes. Alongside the creation of undergraduate programs in the field, postgraduate studies in related subjects are also being developed. However, 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.

Cybersecurity Legal Framework:



Source: Legislative Team of Senator Kenneth Pugh

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."

INDEX

*Chapter 1_*

Cybersecurity and Public Policies

PARTICIPANTS IN THE ELABORATION OF THIS TEXT:

- Coordinating team of the working group "Cybersecurity and Public Policy": Carolina Sancho and Pelayo Covarrubias.

- Technical Working Committee of the working group "Cybersecurity and Public Policy" convened by the Committee: Sebastián Izquierdo, Marisel Cabeza, María Francisca Yañez, Alberto Jara, Jessica Matus, Paola Arellano, Paulina Silva, Romina Garrido, Carmina Hernández, Hernán Espinoza, Daniel Álvarez, Jaime Astorquiza, Íngrid Inda, Pedro Huichalaf, Catherine Narváez, Juan Pablo González, Edison Escobar, Michel Souza, Michelle Bordachar, and Claudia Inostroza.

1. INTRODUCTION

"The digital transformation of our society through Information and Communication Technologies is an undeniable reality. Alongside it, cybersecurity, a concept that was non-existent a few decades ago, is a matter of constant concern where the State must take a leadership and regulatory role through coordinating and normative actions.

The increasing automation, robotization, and digitalization have brought considerable benefits but have also generated new challenges, from which our country is not exempt. On the contrary, we are lagging behind leading Western countries and the OECD. For this reason, it is necessary to progress in terms of improving and establishing a legal and regulatory framework that ensures a more robust and resilient development in cyberspace, providing the appropriate tools to have adequate cybersecurity according to international standards.

Important steps have been taken, starting with the establishment of our first National Cybersecurity Policy 2017-2022 (PNCS), which has raised awareness and sensitized the community about cybersecurity. Additionally, it has led to an increasing number of legislative initiatives on topics such as cybercrime and data protection, alongside the creation of public bodies and entities like the "Government CSIRT" and soon the National Cybersecurity Agency.

Within the framework of this constant and growing challenge of cybersecurity, twenty-two professionals, including lawyers, entrepreneurs, engineers, journalists, and others, were called upon to form a working group called **"Cybersecurity and Public Policies."** From June 30, 2022, to January 5, 2023, and through more than 5 plenary meetings and many hours of work, they analyzed and proposed changes to the regulatory framework. In this chapter, they present various proposals to be considered by legislators to enhance how we address the topic of cybersecurity from a public policy perspective, strengthening our position in this field, especially in legislation.

2. CONTEXT

Our Parliament has played an irreplaceable role in regulating issues related to cybersecurity, which has resulted in the update of laws. For example, in the case of cybercrime and the progress made from Law No. 19,223/1993 to Law No. 21,459/2022, as a commitment of Chile upon joining the Budapest Convention on Cybercrime. Additionally, efforts are being made to establish a specialized institution in this field, namely, a National Cybersecurity Agency.

The executive branch holds a key role in cybersecurity as the primary responsible party for responding to public issues through public policies. These policies include, among other measures, the promotion of regulations relating to critical infrastructure, critical information infrastructure, personal data protection, business continuity plans, and more.

Developing a cybersecurity public policy involves not only the public sector. The private sector, owning a significant amount of critical infrastructure associated with cyberspace, as well as the academic community, which identifies emerging problems, dilemmas, and challenges, are stakeholders that need to be actively considered in addressing cybersecurity issues and the dangers that exist in the use of cyberspace.

Furthermore, but no less important, civil society, represented by individual citizens and organized entities contributing input and demands, plays a role in the formulation of policies. The executive branch must consider these inputs and demands within the framework of a democratic political system where participation and inclusion are guiding principles in its interaction with citizens.

3. FUTURE CHALLENGES

Identifying the challenges to consider in the Chilean case regarding cybersecurity from a public policy perspective has been a complex task, given the diverse nature of these matters and their integration for a better understanding and assessment of the required efforts. To facilitate their systematization, they are developed based on the objectives outlined in the National Cybersecurity Policy 2017-2022 (PNCS).

3.1 PNCS OBJECTIVE 1: "The country will have a robust and resilient information infrastructure prepared to withstand and recover from cybersecurity incidents, from a risk management perspective."

Challenge(s):

Establish a Cybersecurity Framework Law that includes:
Strengthening risk management and business continuity plans to ensure the protection of components that may be attacked or exposed, affecting the operational continuity of services.
Implementing international standards in this field to provide confidence and security for both public and private institutions operating in cyberspace.

Encouraging multidisciplinary work that reconciles specialized and comprehensive actions, avoiding a solely technical approach. Approval of this law would enable the establishment of a cybersecurity architecture, its functioning, and its interaction with other entities or actors involved in the management of this governmental agency.

Establish the necessary institutional framework that allows interaction among the CSIRTs (Computer Security Incident Response Teams) from different sectors, both public and private. This would enhance and strengthen timely coordination among them in incident response or prevention, especially in certain particularly critical sectors.

Place special emphasis on the element of culture or awareness as a key aspect to drive changes within organizations (Change Management). Successfully addressing this challenge would bring clarity in terms of attributions and competencies for regulating, coordinating, overseeing, and enforcing sanctions when cybersecurity incidents occur.

It would also provide a conceptualization of what is meant by a regulated sector, its defining characteristics, and who would be considered obligated subjects.

Note: *As of the date of this report (April 2023), the Cybersecurity Framework Law, Bill 14.847-06, is undergoing its initial constitutional process. Its proposed changes are being reviewed by the Joint Committees on Security and Defense of the Senate. This draft legislation incorporates a significant proportion of the issues described in this section.*

3.2 PNCS OBJECTIVE 2: "The state will safeguard people's rights in cyberspace.

Challenge(s):

Consider the cybersecurity system as a whole, not as isolated regulations. The necessary certainty for regulated markets, individuals, companies, and public entities comes hand in hand with the simultaneous and homogeneous progress of various initiatives that establish "the rules of the game" in this regard.

Advancing in the law on cybercrimes, for example, will require adjustments to companies' crime prevention models implemented under Law 20.393. These adjustments practically entail moving towards comprehensive data governance models, especially for personal and sensitive data, to establish effective control systems for safeguarding them. Implementation of this law requires guidelines included in personal data protection laws (minimum standards) and, depending on the regulated sector, the Cybersecurity Framework Law also demands precise obligations for obligated subjects (e.g., the public sector and institutions declared as critical or vital operators).

Given that the right to cybersecurity is an enabling condition for the exercise of other rights, special attention should be given to ensuring that cybersecurity policies, laws, and practices are aimed at defending and promoting the right to privacy in line with the commitments undertaken by the State of Chile in various international human rights treaties, such as Article 12 of the Universal Declaration of Human Rights, Article 17 of the ICCPR, Article 16 of the Convention on the Rights of the Child, Article 5 of the American Declaration of the Rights and Duties of Man, and Article 11.2 of the American Convention on Human Rights.

Facilitate access for all individuals to enjoy their fundamental rights and freedoms in the digital environment. To achieve this, it is necessary to create the necessary conditions for eliminating situations of discrimination, abuse, and violence that predominantly affect certain segments of the population. In formulating programs, projects, and actions aimed at protecting cybersecurity, priority should be given to the protection of those in disadvantaged situations, especially women, children, adolescents, the elderly, and people with disabilities.

3.3 PNCS OBJECTIVE 3: Chile will develop a cybersecurity culture towards education, best practices, and responsibility in the handling of digital technologies.

Challenge(s):

Promoting a cybersecurity culture that contributes to addressing contingencies in both the public and private sectors, safeguarding people's security in cyberspace.

Cybersecurity education is the cornerstone of secure digital transformation processes, where all citizens are potential users and should consider this from early school ages throughout their lives, recognizing the constant change.

Consider the promotion of cyber-hygiene or digital hygiene to create habits and best practices in the use of computer systems and mobile devices among the entire population, especially in public institutions and educational environments.

Promoting collaboration and public-private partnerships to facilitate a better exchange of information and knowledge in cybersecurity matters, while also fostering the creation of knowledge associated with these topics. Collaborating in cybersecurity does not hinder competition in the markets.

Incorporating an age-focused approach to cybersecurity, taking into account that interests, measures, and levels of security to promote may vary depending on age.

3.4 PNCS OBJECTIVE 4: "The country will establish cooperation relationships in cybersecurity with other actors and actively participate in international forums and discussions.

Challenges

Advance in the formulation and enactment of an international cyberspace policy.

Evaluate the need for continuous adaptation of existing institutions to address the challenges of being immersed in this ecosystem, as well as protecting assets related to information systems, processing, data, and networks. Working towards a holistic vision of integration into cyberspace, recognizing and adopting international standards.

Effectively promoting, systematizing, and monitoring cooperation agreements signed or to be signed by the executive branch in cybersecurity matters to identify opportunities and limitations for their use when necessary.

3.5 PNCS OBJECTIVE 5: "The country will promote the development of a cybersecurity industry that serves its strategic objectives."

Challenge(s):

Promoting regulatory unification to put an end to the regulatory dispersion of recent years, where several different standards exist for the industry.

Providing guidelines and/or recommendations for the private sector regarding what small, medium, and large companies should have in terms of cybersecurity, such as prevention and detection systems.

Promoting a cybersecurity industry that meets national needs, particularly concerning strategic requirements and even enabling the exportation and/or integration of these technological developments.

4. PROPOSALS

There is a proposal to formulate new objectives, which are as follows:

4.1 NEW OBJECTIVE A: "Promote cybersecurity public policy that favors governance in the field, facilitating the inclusion of sectors, areas, and experts in the subject, and creating opportunities for various categories of contributions."

Their inclusion would allow for:

- Having an enabling requirement for digital transformation, safeguarding information, and protecting personal data, ultimately serves the exercise of rights and people's lives in the digital world.

- Promoting and strengthening public-private convergence, coordination, and articulation, is a necessary but insufficient condition for the management of preventive alerts and cybersecurity incidents.

- Considering a public institutional model guided by principles of coordination, particularly with the private sector on an ongoing basis. By improving communication, coordination, and collaboration between various institutions, organizations, and both public and private companies, nationally and internationally, the timely detection and containment of cyberspace incidents are facilitated. Additionally, the participation of academia is important to incorporate international trends in these matters and existing knowledge on a particular subject, among other benefits.

- To implement an institution similar to the Future Committee of the Senate, a "National Cybersecurity Forum" sponsored by it, can be created. This forum would serve as a consultative, prospective, and proactive entity for cybersecurity legislation.

- Promoting cybersecurity governance, including permanent coordination between public institutions and the private sector to ensure cybersecurity, prevention measures, clearly defined roles within the organization, an authority with robust competencies, an increase in specialized professionals, talent retention policies, annual budget allocation considering requirements and contingencies, and continuous training for public officials with involvement from the private sector and academia.

4.2 NEW OBJECTIVE B: Further promote the digital transformation of the government

Their inclusion would allow for:

- Facilitating the implementation of the Digital Transformation Law, which also requires enabling foundational requirements that must comply with the same regulations (Framework Law on Cybersecurity, as all government services are considered essential/critical). Additionally, it is necessary to update the Personal Data Protection Law and Supreme Decree No. 83/2005, which sets the technical standards for the security and confidentiality of electronic documents within government agencies.

- Establishing a governance law for interoperability within the government, which regulates how information can be shared within the government without the need for continuous requests (Principle of "once-only" submission).

- Implementing change management policies within the government to facilitate the use of information, setting rules and regulations on accessing information and data, and privacy approaches that include data anonymization, among others.

- Strengthening digital identity processes to ensure that only authorized individuals have access to information through proper identification, authentication, and validation.

- Enhancing electronic signatures and their universal application.

- Implementing the use of a universal digital domicile, where individuals can receive notifications and maintain their informational relationship with the government.

- Advancing the development of a universal medical record.

4.3 NEW OBJECTIVE C Promoting a National Public Policy on Cybersecurity with a multisectoral approach."

Their inclusion would allow for:

-Including these measures would enable:

-Facilitating the involvement of stakeholders, including civil society organizations, in a holistic and sustained manner to achieve better-informed and evidence-based public policy outcomes.

-Formulating policies through intensive public-private dialogue involving representatives from public services, trade unions, civil society, as well as national and international academics and experts.

-Ensuring that the draft of the second version of the National Public Policy on Cybersecurity (PNCS) undergoes a public consultation process, similar to the current first version. Including these measures would also:

4.4 NEW OBJECTIVE D: Promoting a National Public Policy on Cybersecurity with a gender and social impact approach."

Including these measures would enable

- Take into special consideration that certain forms of digital violence are predominantly directed against women, requiring special monitoring. For example, identifying Gendertrolling, which refers to a type of user particularly averse to women expressing their opinions; Cyberharassment, which involves intentionally causing substantial emotional distress to the victim through persistent online expressions, forming part of a pattern rather than isolated incidents; Cyberstalking, which refers to online harassment that involves a course of action rather than a single incident:

- Continuation of physical harassment through digital means, which includes the repeated monitoring of a person through the internet or other electronic mediums (such as surveillance cameras, electronic listening devices, computer software, mobile applications, and GPS devices), including behaviors such as sending unwanted communications, making sexual advances or requests, threats of violence, and monitoring or tracking the victim's location, daily activities, and/or communications.Creepshot: Refers to a photo taken by a man of a woman or girl in public without her consent. The photos often focus on the victim's buttocks, legs, or cleavage. Cyberflashing: Sending obscene photographs to a woman without her consent to tease, intimidate, or make her uncomfortable.

- Encouraging research that addresses the impact of using cyberspace in everyday life from a holistic approach, incorporating different academic disciplines such as psychology, sociology, political science, international relations, law, economics, and education, among others. This research should particularly consider how frequent use of digital media affects the personal and social relationships of citizens. Additionally, it should examine the effects of social media and other mediums on the creation and dissemination of false information (fake news), misinformation, or manipulated information aimed at distorting the presented facts (disinformation). This research should stimulate the development of citizens' ability to discern between such cases and trustworthy and reliable information.

- Giving special attention and monitoring to this issue, promoting official and publicly available statistics that reflect the evolution of this situation.

4.5 NEW OBJECTIVE E: Promoting a National Public Policy on Cybersecurity with an Age Approach."

Its inclusion would allow:

Considering measures to be implemented according to the characteristics of each stage of people's lives, taking into account that each stage has different levels of knowledge, exposure to technology, interests, responsibility, and challenges. This approach should be cross-cutting throughout the policy framework. Consideration should also be given to the context of vulnerable groups, such as elderly individuals, who may require physical locations to address their virtual needs.

5. CONCLUSIONS

The text you've provided outlines the proposed suggestions and considerations of cybersecurity experts. It highlights current challenges derived from the objectives set in the existing National Cybersecurity Policy (PNCS) and suggests proposals based on an evaluation of the evolving context since 2017. 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.

Given the identified challenges, efforts should focus on strengthening cybersecurity through a risk management perspective. Protection of individuals' rights in cyberspace, promoting a culture of safe practices, and increasing cybersecurity expertise through enhanced training programs are necessary steps. Additionally, advancing Chile's international cyber policy and aligning industry operations with international cybersecurity standards while fostering national technological development that can be exported should be prioritized.

Looking ahead to future proposals, a governance-focused approach should be adopted in the public cybersecurity policy to encourage interagency coordination and inclusivity. Gender and social impact considerations should be integral to the updated cybersecurity policy, acknowledging the different situations faced by individuals, particularly women, in cyberspace. The need for training and inclusion of women in technological advancements and development should be emphasized. Moreover, considering citizens of different age groups and tailoring measures accordingly is crucial to ensure effective cybersecurity initiatives that cater to their specific needs.

*Chapter 2_*

Developing Cyber Talent

PARTICIPANTS IN THE ELABORATION OF THIS TEXT::

- Coordinating team of the working group "Developing Cyber Talent": Xavier Bonaire and Tania
Yovanovic

- Technical Working Committee of the working group "Developing Cyber Talent" convened by the Committee: Ximena Sepúlveda, Martin Seguel, Rodrigo San Martin, Alexandra Barros, Sebastian Vargas, Lidia Herrera, and Claudia Jaña.

1. INTRODUCTION

Cyberspace is a creation entirely made by human beings; it is the result of a collective creation that expands at an astonishing pace, constantly demanding new contributions and advances in knowledge. Cyberspace demands new talents, which should be identified from an early age, provided with the necessary resources for their development and education, and ultimately placed in the job market.

The demand is enormous, and this deficit has been recognized in European countries, which can easily be extrapolated to our national reality. Consequently, we are facing a reality that requires constant attention, with new strategies and actions aimed at developing our cyber talent and making it available to meet the needs of our country.

Throughout more than 20 working meetings, including plenary sessions and working groups, held between June 22 and November 30, 2022, a team composed of professionals from various backgrounds, including lawyers, engineers, journalists, entrepreneurs, and academics, achieved the results reflected in this chapter.

2. CONTEXT IN CHILE

Cybersecurity is a concerning issue in Chile, both in the realm of government agencies and private companies. The numerous recent events involving attacks on institutions and companies that are part of the country's critical infrastructure reflect the lack of a general cybersecurity culture in Chile, and in some cases, a lack of concern for the topic.

The publicly evidenced cybersecurity crises during 2022 indicate a lack of preparedness in the country, not only regarding the use of appropriate technology but also how these crises are managed, sometimes inadequately.

Common sense leads us to think that cybersecurity is essentially a technical problem, where the focus is on using the right technology, in the right place, and at the right time. However, cybersecurity is primarily a human matter.

Humans play a role throughout the cybersecurity chain, from designing secure systems and programs (software) to implementing technologies such as firewalls or attack detection and prevention systems, incident response and forensic analysis, to crisis management involving communication and other associated actions.

In this context, the development of cyber talent in Chile should be part of a comprehensive plan to improve national cybersecurity. The country's deficit in cybersecurity specialists presents a significant challenge for government agencies and companies to hire professionals in this field. Developing cyber talent is, therefore, a priority to enhance the overall level of the country's cybersecurity.

3. CYBERSECURITY RANKING

The assessment of a country's cybersecurity state is crucial to identify and address any potential weaknesses and develop appropriate policies and actions to mitigate them. Several global studies estimate the state of cybersecurity for countries. Generally, the results obtained can vary slightly between different classifications due to the non-uniformity of the criteria used in each evaluation. It's important to note that each classification may have its unique criteria and methodologies, leading to slight variations in results.

The most recognized cybersecurity classifications by the community are:

1. International Telecommunication Union (ITU) Cybersecurity Index: ITU, a United Nations (UN) agency, issues a classification every two years for all member countries. The study is based on data provided by member countries and evaluates cybersecurity based on five pillars:

• Legal Measures: Assesses a country's current state based on existing legal measures and regulations, including laws on cybercrime, data protection, and regulation of critical infrastructure.

2. National Cybersecurity Index (NCI) by e-Governance Academy in Estonia.

3.1 ITU - Cybersecurity Index

The ITU (International Telecommunication Union), a UN (United Nations) agency, publishes a cybersecurity ranking of all countries that are part of the organization every two years. The study is based on data provided by member countries and focuses on five pillars of cybersecurity:

• Legal Measures: Measures the current state of a country based on existing legal measures and regulations, including laws on cybercrime, data protection laws, and regulation of critical infrastructure

• Technical Measures: This pillar assesses a country's current state based on the implementation of technical measures through national and regional agencies. It includes the presence of an active CERT/CSIRT at both the national and sectoral levels, as well as mechanisms for protection and reporting in cases of child abuse.

• Organizational Measures: This pillar measures the strategies and organization at the national level for implementing cybersecurity. It includes the existence of national cybersecurity policies, cybersecurity agencies, and initiatives to combat online child harassment.

• Development Capacity: This pillar measures a country's state in terms of cybersecurity awareness campaigns, cybersecurity exercises, education, and development capacity. It includes the presence of Research and Innovation programs in cybersecurity, as well as an established cybersecurity industry.

• Cooperation: This pillar assesses the existence of cooperation programs between agencies, between private and state-owned companies, and with other countries. It includes public-private agreements and bilateral or multilateral agreements with other countries.

Monaco	72.57	69
Uzbekistan	71.11	70
Jordan	70.96	71
Uganda	69.98	72
Zambia	68.88	73
Chile	68.83	74
Côte d'Ivoire	67.82	75
Costa Rica	67.45	76
Bulgaria	67.38	77
Ukraine	65.93	78

Figure 1 ITU Ranking Chile 2021 - Score Breakdown

Country Name	Overall Score	Regional Rank
United States of America**	100	1
Canada**	97.67	2
Brazil	96.6	3
Mexico	81.68	4
Uruguay	75.15	5
Dominican Rep.	75.07	6
Chile	68.83	7
Costa Rica	67.45	8
Colombia	63.72	9
Cuba	58.76	10

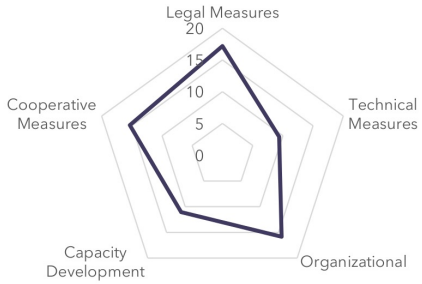
Figure 2 ITU Regional Ranking 2021

Based on the results obtained from these five indicators, ITU generates a classification score ranging from 0 to 100 for each country.

In the 2021 classification, Chile ranks 74th globally with a score of 68.83, as shown in Figure 1. While it is quite distant from the top 10 countries in the ranking. Nevertheless, there has been progressing since the previous 2019 report.

At the regional level, Chile ranks seventh, with a better evaluation than Colombia, Peru, Argentina, and Paraguay, but behind Brazil, Mexico, Uruguay, and the Dominican Republic, as shown in Figure 2. These classifications provide valuable insights into a country's cybersecurity efforts, allowing for analysis and comparison both globally and regionally.

Chile



Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
68.83	17.20	9.39	15.84	11.07	15.33

Source: ITU Global Cybersecurity Index v4, 2020

Figure 3 - ITU Ranking Chile 2021 - Score Breakdown

Figure 3 represents the scores obtained by Chile in the five indicators of the ITU Cybersecurity Index in 2020. Chile demonstrates the best results in the Legal Measures and Organizational Measures indicators. This can be attributed to the country's progress in creating new laws in the field of cybersecurity, such as the most recent legislation on cybercrime.

However, in the Technical Measures and Development Capacity indicators, the country shows a significant lag. The Development Capacity indicator includes Chile's ability to develop cybersecurity talent, specifically the capacity for cybersecurity education in the country.

3.2 NCSI RANKING – National Cyber Security Index

The NCSI ranking is the second internationally recognized classification in cybersecurity. It is published by the e-Governance Academy, which was founded in 2002. The e-Governance Academy is a non-profit foundation aligned with the Government of Estonia, the Open Society Institute (OSI), and the United Nations Development Programme (UNDP).

NCSI national cyber security index

50. Chile 59.74

Population	18.2 million
Area (km²)	756.1 thousand
GDP per capita ($)	25.4 thousand

50th	National Cyber Security Index	60 %
74th	Global Cybersecurity Index	69 %
56th	ICT Development Index	66 %
44th	Networked Readiness Index	57 %

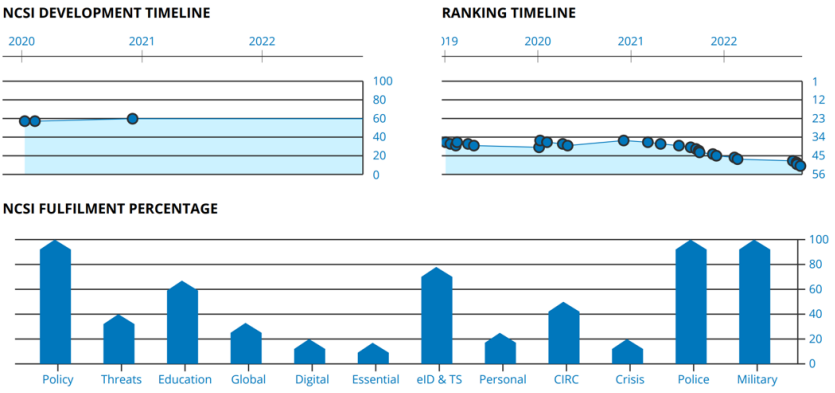


Figure 4 NCSI Ranking Chile 2022

The above figure highlights Chile's drop of 13 positions in the NCSI ranking between 2019 and November 2022. This decline in ranking is primarily attributed to several factors:

1. Chile faced numerous cybersecurity crises during this period, particularly in recent months, involving state organizations. The score also reflects a lack of proper management of cybersecurity crises at both the state and private levels due to a shortage of qualified professionals in this field.

2. There is a significant deficit of cybersecurity personnel in Chile, which is directly related to the country's talent development and education in cybersecurity. This deficit spans early education, higher education, and continuous education.

3. There is a lack of appropriate regulations for the handling of personal data, leading to a high rate of data breaches.

Although great progress can be noted in the legal aspects of cybersecurity in recent years, especially with the new law No. 21449 regarding cybercrime, the NCSI ranking, like that of the ITU, shows the country's deficiencies in cybersecurity.

4. CHALLENGES

To address these challenges, Chile has set certain objectives in its "Chile Digital 2035" Digital Transformation Strategy, which we have named: **"Developing Cyber Talent":**

OBJECTIVE 2 Building a comprehensive national cybersecurity culture

·Developing cyber hygiene programs for children aged 2 to 12.

·Implementing cybersecurity-focused digital skills training throughout the schooling years.

·Creating programs to mitigate online violence from an early age and combat cyberbullying among minors.

·Providing digital support programs for senior citizens to mitigate risks they face in cyberspace.

OBJECTIVE 3 Talent management, capacity development, and cybersecurity industry growth

·Executing programs to identify and develop cyber talents from the age of 14.

·Delivering certified digital skills and competencies training for individuals of all ages starting from 18, regardless of prior academic background, using the French methodology of School 42.

·Improving cybersecurity education offerings by establishing training programs and accreditation of competencies aligned with national and international standards for technical and university-level careers.

·Promoting the development of cybersecurity postgraduate scholarships at globally renowned universities for doctoral and postdoctoral studies.

·Encouraging the inclusion of women in cybersecurity careers to address the existing gender gap.

·Recognizing outstanding women in cybersecurity through annual awards.

·Annually recognize outstanding emerging leaders in cybersecurity.

·Encourage the training and retention of cybersecurity specialists to support the government, its services, and the general economic actors.

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

Based on these objectives, four aspects are proposed for development, which are detailed below.

Education in Primary and Secondary Schools

·Early education in cybersecurity.

·Integration of cybersecurity-focused digital skills training throughout the schooling years.

·Programs aimed at mitigating online violence and cyberbullying among minors.

·Initiatives for identifying and developing cyber talents from the age of 14.

Higher Education

Greater educational offer in cybersecurity.

* Accreditation of competencies through international standards.
* Available for technical and university careers.

Degree-granting programs and courses.

* Undergraduate programs (Engineering, Technical, Professional).
* Master's, Doctorate, and Post-Doctorate.

·Digital skills and competency certification for students over 18 years old, without any previous academic requirements (following the model of École 42 in France).

·Encouragement of postgraduate scholarships in cybersecurity at prestigious universities.

·Training and inclusion of women in cybersecurity careers to address the existing gender gap.

Continuing Education

· Public awareness campaigns and community engagement targeting the general public.

· Training programs and support for senior citizens.

· Offering diplomas and certifications.

· Providing training for businesses and government organizations.

· Facilitating career transitions and retraining.

· Developing alternative programs to Military Service for training Cyberdefense specialists.

Cross-Cutting Themes

These themes contribute to the overall development of cybersecurity talent.

· Establishment of the National Institute of Cybersecurity (INCIBER):

* Raising awareness.
* Accreditation of competencies.
* Organizing national cybersecurity exercises

· Annual recognition of outstanding women in cybersecurity.

· Recognition of emerging and notable leaders in cybersecurity.

· Collaboration in cybersecurity efforts between the civilian sector and defense entities.

* Supporting dual-use technology projects (civilian and military).
* Allocation of adequate resources for implementation.

5. DEVELOPMENT AND PROPOSALS

One of the factors explaining the low level of cybersecurity in Chile is the lack of early education in this field, especially the absence of teaching good cybersecurity practices in schools (cyber hygiene).

Recent publications, such as the World Economic Forum article, highlight the need to teach cybersecurity at an early stage for two reasons:

1. Children use technology devices (such as smartphones, tablets, computers, gaming consoles, etc.) at an increasingly early age, exposing them to cybersecurity risks and cognitive risks (as seen in the OECD report).

2. Children and teenagers are targets of various types of cyber-attacks.

In this context, it is necessary to advance early cybersecurity education in Chile to create national awareness in this field. Therefore, 7 proposals are being developed for this cycle:

Proposal 1 - Include cybersecurity as a subject in the curriculum for primary and secondary education.

It is necessary to include cybersecurity as a separate subject in elementary and secondary education to create early awareness among children. The objective is to teach good cybersecurity practices in the use of mobile devices, social networks, basic credential management (username + password), and the risks associated with exposing personal data.

Short-term actions

* Conducting talks in schools and/or universities to train teachers on good cybersecurity practices.
FINANCING: PUBLIC/PRIVATE

* Running awareness campaigns through the Ministry of Education in the media to sensitize children and parents about good cybersecurity practices.
FINANCING: PUBLIC

* Modify the pedagogy program to include cybersecurity training for future teachers.

FINANCING: PUBLIC

Medium-term actions

* Determine the scope and depth of the topics to be applied at each level, as well as the implementation requirements for each educational institution within the proposal's scope. Look at tangible examples from countries that lead in this area, such as Spain.

FINANCING: PUBLIC/PRIVATE.

Long-term actions

*Include cybersecurity in the science program for primary and secondary education teachers.

*Define subjects by level created/updated according to the proposal on the curricula.

FINANCING: PUBLIC/PRIVATE

EXPECTED IMPACTS

· Raise awareness among school teachers about cybersecurity topics.

· Raise awareness among children about good cybersecurity practices.

· Raise awareness among parents about good cybersecurity practices.

· Provide training to teachers as part of their pedagogy degree curriculum.

· Activate the development/modification of selected subjects based on national-level needs by level.

· Implement an updated training structure in schools throughout the country.

Proposal 2 - National Culture of Cybersecurity in Educational Institutions.

Generate a National Culture of Cybersecurity among parents, guardians, teachers, and students.

Short-term actions

*Generate a National Culture of Cybersecurity among parents, guardians, teachers, and students at different educational levels, from primary to secondary education.
FINANCING: PUBLIC

Medium-term actions

*Raise awareness among teachers in schools and high schools regarding cybersecurity topics.
FINANCING: PUBLIC

Long-term actions

*Training of monitors to lead the update to teachers, parents, and guardians. Identify leaders from educational sectors who will serve as guides for the project, ensuring that they keep the responsible individuals of each level of action updated and informed, thus keeping the topic of cybersecurity alive and up-to-date.

FINANCING: PUBLIC

EXPECTED IMPACTS

·Familiarize users with the risks and benefits of handling cybersecurity topics, such as secure accounts, password management, etc.

·Promote continuous knowledge updates in cybersecurity within different educational entities.

·Create a well-prepared teaching staff in this field to support students and parents in understanding the issues and finding solutions.

·Foster a participatory community with up-to-date knowledge on the subject.

Proposal 3 - Establish Training and Update Alliances

Connecting the education sector with training entities and recognized experiences at the national level.

Short-term actions

*Recognize national training entities focused on promoting the development of talent for the digital world, to support Chile's transition into the digital era.
FINANCING: PUBLIC

Medium-term actions

*The state should actively participate in these alliances, playing a role in endorsing the relationships formed, to strengthen the partnership and address training needs.

FINANCING: PUBLIC/PRIVATE

Long-term actions

*Create opportunities for constant updates through events, competitions, and activities conducted at each educational level.

FINANCING: PUBLIC/PRIVATE

EXPECTED IMPACTS

· High-quality partnerships that benefit educational change and improvement in the field of cybersecurity.

· Promote the participation of different sectors to achieve the necessary alliance for our students.

· Foster education-industry interaction to promote cybersecurity education for students of different ages in primary and secondary education.

Proposal 4 - Design Continuous Training Programs for Teachers

Designing continuous training programs for teachers, both practicing, recent graduates, and Pedagogy students. Educating the future teachers of the country and incorporating cybersecurity into their curriculum ensuring continuous updating and integration of cybersecurity topics, contributes to the development of a national cybersecurity culture.

Short-term actions

*Survey teachers at different levels to identify those who would be interested in participating in this proposal. This will create a registry of teachers who can be part of this action.

FINANCING: PUBLIC/PRIVATE

Medium-term actions

*Based on the registry mentioned above, establish awareness stages that address the basic needs of each educational institution at the primary and/or secondary level.

FINANCING: PUBLIC/PRIVATE

*Develop standardized documentation to ensure consistent knowledge delivery at the national level, eliminating any ambiguity in the subject matter.

FINANCING: PUBLIC/PRIVATE

Long-term actions

*Establish a national work plan to be implemented in each region, either through in-person courses or using available technologies. Initially, this plan would be guided by expert professionals and take examples from other countries, such as Spain. This example aligns closely with our background and circumstances.

FINANCING: PUBLIC/PRIVATE

EXPECTED IMPACTS

· Enable the country to have a workforce of education professionals who incorporate necessary cybersecurity actions into their teaching practices, ensuring that young minds adopt cybersecurity practices and hygiene required to thrive in the digital world.

Proposal 5 - Formulate a Cybersecurity Certification Program

Formulate a program to accredit competencies and certifications in cybersecurity for elementary and secondary school teachers. This program will ensure a standard of quality in knowledge delivery and validate the level of knowledge among teachers, ensuring they meet the minimum qualifications required to participate in this digital literacy process and bridge the digital gap.

Short-term actions

*Identify institutions/organizations that can help cover the population of teachers regionally and nationally.

FINANCING: PUBLIC/PRIVATE

Medium-term actions

*Create workshops for teacher preparation and leveling, focusing on basic technology and cyber hygiene. These workshops can be conducted in person or virtually.

FINANCING: PUBLIC/PRIVATE

Long-term actions

*Develop a national certification plan supported by proven and secure tools for establishing contacts and measuring knowledge. This will optimize the learning time for professionals.

FINANCING: PUBLIC/PRIVATE

EXPECTED IMPACTS

· Accredited and certified teachers with unified knowledge and language.

· Updated digital cyber hygiene practices. Collaboration between public and private sectors.

· Activation of agreements with Higher Education Institutions (HEIs), technology companies, government agencies, NGOs, among others.

Proposal 6 - Design of Training Programs and Campaigns

Design training programs and campaigns for parents and guardians with best practices in cybersecurity (involving Higher Education Institutions, Schools, the Investigations Police, and the Ministry of Education). Design update campaigns for active teachers. Promote the technological knowledge that parents, guardians, and active teachers working with this technologized generation need today.

Short-term actions

*Identify the number of educational institutions that need to update their teachers on cybersecurity topics.

*Determine the number of educational institutions where these campaigns should be implemented to define the scope of this proposal. Create a regional action map.

FINANCING: PUBLIC/PRIVATE

Medium-term actions

*Define the core topics that need further exploration based on the information gathered in the previous point.

FINANCING: PUBLIC/PRIVATE

Long-term actions

* Implement necessary changes to the curriculum, considering the initial objective and the unique characteristics of each institution. Aim for continuous improvement.

FINANCING: PUBLIC/PRIVATE

EXPECTED IMPACTS

· Clear understanding among both teachers and educational institutions regarding the need for cybersecurity updates.

· Prepared parents, caregivers, and teachers in cybersecurity hygiene topics, supporting the education of Chile's future.

· Strengthened and prepared human capital for the education of our future citizens.

Proposal 7 - Create a mandatory digital certification for students in schools and high schools

Digital competencies are becoming increasingly important for citizens, especially for young people who need to have basic knowledge and skills in this area, including cybersecurity and good practices. Some countries, such as France with the PIX program, have already implemented not only the teaching of these practices but also their mandatory evaluation for all students in schools and high schools, whether they are in general or vocational education. The PIX program aligns with the European Union's recommendations regarding digital competencies.

Short-term actions

* Design a program comparable to the PIX program in France for teaching good practices in the use of digital tools.
* Train teachers in schools for teaching related to the program. (See Proposal 1 - Proposal 2 - Proposal 4)

FINANCING: PUBLIC

Medium-term actions

* Design an assessment test for digital skills for students in schools.

FINANCING: PUBLIC

Long-term actions

* Implement the assessment test for all students in schools.

FINANCING: PUBLIC

EXPECTED IMPACTS

·Noticeable improvement in the level of good practices in the use of digital tools by the citizens.

·Noticeable improvement in the use of good practices in cybersecurity and cyber hygiene by the citizens, especially in the management of personal data.

4.2 HIGHER EDUCATION

The development of cybersecurity courses in higher education programs is a must to teach good practices to all students and also to train specialized professionals. The national situation is critical. The country is estimated to have a significant shortage of qualified professionals in cybersecurity. This can be explained by several reasons:

1. A lack of a general cybersecurity culture in Chile and a lack of awareness of the consequences that various cybersecurity events can have.

2. Limited availability of cybersecurity careers or specialization alternatives in higher education institutions in all regions of the country.

3. The lack of cybersecurity culture does not attract people to study topics related to cybersecurity.

The national academy is lagging in the implementation of training programs, inclusion in their curricula, and offering specialized careers in cybersecurity when compared to the implementation and offering of technical programs, engineering degrees, or postgraduate degrees.

In this context, it is necessary to make progress in terms of higher education offerings, which is why four proposals are being developed for this cycle

Proposal 8 - Creation of careers and programs for the training of cybersecurity specialists

It is necessary to increase the supply of qualified professionals in Chile by creating careers and providing training in the field of cybersecurity.

Short-term actions

*Create professional training programs in cybersecurity aimed at practicing professionals in IT and related fields.
* Develop cybersecurity training programs focused on building cyber capabilities in companies and public institutions.

FINANCING: PUBLIC/PRIVATE

Medium-term actions

* Establish new cybersecurity programs at various levels.

* 2-year technical programs to train higher-level cybersecurity technicians.

* Undergraduate programs in Computer Engineering or related fields with a specialization in cybersecurity.

* Postgraduate programs such as diplomas and/or Professional Master's degrees in cybersecurity to train high-level professionals in the field.

FINANCING: PUBLIC/PRIVATE

Long-term actions

* Foster international agreements for student and faculty exchange programs in cybersecurity fields.

FINANCING: PUBLIC/PRIVATE

EXPECTED IMPACTS

· Increase in cybersecurity specialists and qualified professionals throughout the country.

· Improved cybersecurity education in higher education.

· Increased availability of specialist training.

· Enhancement of national expertise in cybersecurity, both in private companies and in state institutions and agencies.

Proposal 9 - Include cybersecurity notions at all levels of education in computer science and related fields.

Currently, cybersecurity is included in computer science programs as a set of elective courses. The consequence of this approach is that students who do not take these elective courses do not have basic knowledge of cybersecurity and good practices in cyberspace.

Short-term actions

* Redesign the computer fundamentals courses to include notions of cybersecurity for all students, especially in courses such as:

→Operating Systems.
→Computer Networks.
→Programming.
→Databases.
→Software Engineering.
→Data Structures.
→Data centers.
→Cloud.

*Train the teachers of these courses to have knowledge of cybersecurity best practices related to the topic of their courses.

FINANCING: PUBLIC/PRIVATE

Medium-term actions

*Implement the courses with the new design, including tasks or labs related to cybersecurity aspects related to the course topic.

FINANCING: PUBLIC/PRIVATE

Long-term actions

* Incorporate cybersecurity training specific to their field of study for all technical and university degrees, similar to what mathematics or basic sciences courses are today.

* Provide training to non-scientific faculty members in cybersecurity best practices.

FINANCING: PUBLIC/PRIVATE

EXPECTED IMPACTS

· Improvement in the overall level of cybersecurity knowledge among students in computer science and related fields, regardless of their chosen specialization.

· General increase in cybersecurity knowledge among students from non-IT disciplines (especially in terms of best practices for using cyberspace).

· Enhancement of the cybersecurity knowledge among professors in higher education in computer science or related fields.

· Overall increase in knowledge of cybersecurity best practices among professors in higher education.

Proposal 10 - Organize educational cybersecurity events

It is necessary to disseminate knowledge and best practices in cybersecurity not only through university courses but also to a wider audience, including individuals interested in cybersecurity who may not have a formal education.

Short-term actions

*Enhance outreach activities during October, the month of Cybersecurity..

*Organize cybersecurity workshops for higher education students, including cybersecurity exercises.

*Organize regional Capture The Flag (CTF) events in the country to bring together groups of cyber-security expert students from different universities and identify regional talent in the field.

Medium-term actions

*Organize national university exercises during the month of cybersecurity (such as CTF or other formats) to identify and create a countrywide network of talent in the field.

*Organize cybersecurity workshops for companies, especially small and medium-sized enterprises (SMEs), to promote the use of good cybersecurity practices through educational games.

Long-term actions

*Organize events, exercises, and cybersecurity competitions tailored to both public and private institutions and organizations.

EXPECTED IMPACTS

- Identification of cybersecurity talents at both regional and national levels.
- Formation of cybersecurity defense training groups.
- Promotion of a cybersecurity and cyber hygiene culture in companies

Proposal 11 - Creation of cyber security-themed scholarships by the National Agency for Research and Development (ANID)

It is necessary to create scholarships specifically aimed at postgraduate programs and projects in innovation and applied cybersecurity research.

Short-term actions

*Creation of specific scholarships for applying to postgraduate programs (Scientific Master's, Professional Master's, Ph.D.) in cybersecurity.

*Creation of specific scholarships for internships abroad (in countries within the top 20 of the ITU ranking) in cybersecurity-related topics.

* Allocation of competitive funds for academies for applied cybersecurity projects that bring together local and international specialists.

Medium-term actions

* Creation of specific funding for research and innovation projects in cybersecurity, especially in topics related to cyber defense.

* Specific funding for the creation of regional innovation and research centers in cybersecurity with collaborations between academia and businesses.

Long-term actions

* Specific funding for the creation of regional innovation and research centers in cybersecurity with collaborations between academia and businesses.

EXPECTED IMPACTS

· Specific funding for the creation of regional innovation and research centers in cybersecurity with collaborations between academia and businesses.

4.3 CONTINUING EDUCATION IN CYBERSECURITY

Cybersecurity is an ongoing process where new threats constantly emerge and vulnerabilities are exploited with the use of new tools and technologies. People and institutions are exposed to new challenges that increase the need for continuous and permanent education, which should provide knowledge about new challenges, tools, and solutions in cybersecurity. and this is something we must address.

As a result, the following four proposals are suggested to address this aspect.

Proposal 12 - Generation of Diplomas and Certifications of Competence

Promote the generation of Diplomas and Certifications according to the needs of the Chilean ecosystem.

Short-term actions

*Generate comprehensive certification program plans that address the needs of both public and private institutions.

FINANCING: PUBLIC

Medium-term actions

* Promote the homologation of national certifications to international standards, which can be granted by national training institutions, with the corresponding accreditations.

FINANCING: PUBLIC

Long-term actions

* Establish certifications that allow the accreditation of basic cybersecurity competency (e.g., similar to a driver's license), aimed at encouraging professional careers in cybersecurity in line with international cybersecurity certifications.

FINANCING: PUBLIC

EXPECTED IMPACTS

· Promote, update, and standardize cybersecurity certification internationally for officials from various institutions (public and private) to reduce identified gaps.

· Encourage training of institutional personnel in international cybersecurity certifications defined in the accredited certification programs for the country in training institutions (public/private) certified.

· Make the country a reference in cybersecurity by generating a basic national certificate (open to the entire population) covering fundamental topics and providing further education with the highest international standards.

Proposal 13 - Training for companies and government agencies

Improve the overall level of cybersecurity training for personnel in companies and government agencies. Address the absence of a cybersecurity maturity assessment. Present a unique national model to develop maturity analysis.

Short-term actions

* Conduct a survey and assessment of cybersecurity levels in different institutions. Determine if there are competent or specialized personnel to operate in this area.

FINANCING: PUBLIC/PRIVATE

Medium-term actions

* The government should sponsor initiatives and incentives, promoting partnerships with other public and private institutions, both national and international, to bridge identified gaps. This will involve generating sector-specific training master plans to address these gaps.

FINANCING: PUBLIC

Long-term actions

* Consolidate the ecosystem (public and private) as a promoter of continuous improvement in cybersecurity education, with a focus on companies and government agencies.

FINANCING: PUBLIC/PRIVATE

EXPECTED IMPACTS

· Have an updated registry of strengths and weaknesses of public officials in various institutions. Determine the vulnerabilities of our institutions and if they have security systems in place. Assess the level of maturity (training) of these institutions–operational technological objective.

· Decrease the identified gaps through a continuous improvement ecosystem.

· Consolidate the ecosystem (public and private) as a promoter of continuous improvement in cybersecurity education, with a focus on companies and government agencies.

Proposal 14 - Citizen Awareness

Educating people about cybersecurity is vital for creating a national culture in this field. Awareness is the first step towards developing a citizenry with good cyber hygiene practices. It is crucial to create ongoing awareness campaigns tailored to citizens' specific needs, reinforcing the creation of a national culture of cybersecurity.

Short-term actions

*** CREATE A SLOGAN AND BRAND**. The slogan is a short, concise phrase that will be easily recognizable and will set the tone for the campaign. Together, the slogan and logo form the brief message and graphic image that announces to everyone, ***"Pay attention, there's something you need to know and apply."*** These two elements constitute the branding of the campaign.

→Develop a strong idea that can be conveyed through text and an image (a logo) to highlight the benefits of cybersecurity (similar to the "Choose Healthy Living" campaign by the Ministry of Health).

→Implement a massive dissemination program for this strong idea. Utilize it on all government portals by placing the logo and one or two campaign tips in a banner or pop-up window on all websites accessed by the public.
FINANCING: PUBLIC

Medium-term actions

***** Create and disseminate cybersecurity tools for businesses.

→Prepare an information sheet for employees that contains relevant messages for each area of the business (similar to the "Right to Know" in labor legislation).

→Provide a list of easily implementable measures to immediately improve their digital security (similar to personal protective equipment).

→Display cybersecurity signage in the workplace.

FINANCING: PUBLIC/PRIVATE

Long-term actions

***** Establish a Virtual Office for cybersecurity advice to Internet users, including telephone support.
FINANCING: PUBLIC/PRIVATE

EXPECTED IMPACTS

· The message and logo provide the program's identity.

· Raise awareness among entrepreneurs, workers, and the general public.

· Provide information and support to end users to address their security concerns and issues while navigating the internet, particularly for those who are new to technology.

Proposal 15 - Training and Support for Older Adults

Address the different challenges faced by older adults in the digital world. Showcase current national and international measures and analyze comparative experiences to propose new solutions.

Short-term actions

* Identify institutions/organizations to reach the target audience of older adults.

FINANCING: PUBLIC/PRIVATE

Medium-term actions

* Implementation of practical workshops; basic computer courses, basic cybersecurity measures, both in-person and online (depending on the level), for SENAMA (Older Adults Service) network users.

FINANCING: PUBLIC

Long-term actions

* Develop accompanying tools (contact hotlines, WhatsApp, applications, online tests) to help older adults access information and support for safe internet navigation.

FINANCING: PUBLIC/PRIVATE

EXPECTED IMPACTS

· Provide training in the following minimum aspects, promoting a peer facilitator policy:

→ Electronic Administration 1: Operation of the single key system and public services.

→ Electronic Administration 2 and Online Banking: Operations and precautions in electronic payment systems and banking.

- → Digital Communication: Communication tools, email, WhatsApp, and Video Conferences.
- → Mobile Phone Usage: Most common uses.
- → Mobile Applications: Most used applications.

· Building a support network for the elderly.

4.4 CROSS-CUTTING ISSUES

As mentioned earlier, we consider it necessary to include some complementary proposals that contribute to the development of cyber talent and should be considered for fostering a culture and the development of national cybersecurity.

This is reflected in the following 4 proposals:

Proposal 16 - Create the "National Cyber Training and Cyber Jobs Platform – focused on Cybersecurity"

Lack of efficient links for retraining. Present methods to promote retraining.

Short-term actions

* Conduct a study in collaboration with academia and societal organizations to estimate demands and target audience.

FINANCING: PUBLIC/PRIVATE

Medium-term actions

* The government will sponsor initiatives and incentives, through organizations such as SENCE (National Service for Training and Employment), to establish a national pool of technological, digital, and cybersecurity jobs. Additionally, a national professional retraining program in cybersecurity will be promoted. (Based on CORFO: Human Capital Scholarships)

FINANCING: PUBLIC

Long-term actions

* Organize job fairs focused on professional retraining for retired armed forces personnel, public employees, women, and neurodiverse citizens, similar to what is done in the United States.

FINANCING: PUBLIC/PRIVATE

EXPECTED IMPACTS

· Conduct a nationwide study of sectors and professions that could be part of an education program focused on retraining.

· Increase professional retraining for cybersecurity specialists.

· Create a human capital system to strengthen the demand for specialists in cybersecurity in Chile

Proposal 17 - Creation of a National Cybersecurity Institute **(INCIBER)**

It is necessary to create a National Cybersecurity Institute in Chile, similar to Spain's INCIBE. The role of the Chilean INCIBER would be to create a cybersecurity ecosystem, encompassing the dissemination, innovation, and promotion of cybersecurity, including the academic world, the business sector, government agencies, and organized civil society.

Short-term actions

* Creation of national reference standards for educating future cybersecurity experts in the country. Play an articulating role in national cybersecurity research and development. Establish links with related institutions at the international level.
FINANCING: PUBLIC

Medium-term actions

* Organize national cybersecurity exercises in collaboration with academia to promote group learning of cyber defense techniques and identify talent in the field.
FINANCING: PUBLIC

Long-term actions

* Establish national certifications in cybersecurity (similar to EC-Council) in cooperation with higher education institutions.

* Develop a cybersecurity accreditation system for courses in the field (a quality label: INCIBER Seal).
FINANCING: PUBLIC/PRIVATE

EXPECTED IMPACTS

· Creation of an ecosystem among the government, academia, and businesses to establish a framework for cooperation in cybersecurity education and awareness.

· Development of a certification model for cybersecurity education.

· Enhancement of cooperation between the academic and business sectors in cybersecurity.

Proposal 18 - Create an equivalent of Estonia's Estonian Defense League's Cyber Unit

The Estonian Defense League's Cyber Unit is an organization that aims to defend the country's cyberspace. It includes members from government institutions specializing in cybersecurity, as well as professionals from private companies and volunteers from civil society.

Short-term actions

* Creation of an association for the defense of Chile's cyberspace in cooperation with academia, government representatives, cybersecurity professionals, and volunteers from civil society.

FINANCING: PUBLIC

Medium-term actions

* Establish a division within INCIBER for the management, implementation, and training of this association.

FINANCING: PUBLIC/PRIVATE

Long-term actions

* Organize international training exercises for the members of this Chilean cyberspace defense association (for example, in cooperation with Estonia or other countries with a high ranking in cybersecurity).

FINANCING: PUBLIC/PRIVATE

EXPECTED IMPACTS

· Establishment of a national reserve of cybersecurity specialists to address any potential attack scenarios at a national level.

· Promotion of cooperation between the civilian and military sectors in cybersecurity (Ministry of Defense and Ministry responsible for Public Security).

· Identification and promotion of cybersecurity talents outside the traditional higher education system.

Proposal 19 - Create a culture of personal data protection among citizens

Protecting personal data is now crucial to safeguarding young people from cyberbullying attacks and ensuring privacy for individuals in general. The protection of personal data should be part of a national culture on the issue and the digital skills of each individual.

Short-term actions

* Launch awareness campaigns in the media about the importance of protecting and caring for personal data.

FINANCING: PUBLIC

Medium-term actions

* Make progress in enacting a personal data protection law based on the European General Data Protection Regulation (GDPR).

* Establish a robust national digital identity system with two-factor authentication.

FINANCING: PUBLIC

Long-term actions

* Restrict the use of the National Identification Number (RUT or ID number) as an identification method, subject to prior consent between parties regarding the use and destination of the provided information, and the existence of a robust digital identity system.

FINANCING: PUBLIC

CONCLUSIONS

For Chile to advance in cybersecurity, a significant effort in education is necessary, especially in training highly skilled professionals in the field. To achieve this, the creation of a comprehensive cybersecurity ecosystem at the national level is essential to align the academic offerings with the country's needs.

However, it is crucial to consider early education in cybersecurity to ensure proper preparation of children for the use of the Internet in general. Early education is the best way to build a national culture of cybersecurity, laying the foundation for high-level cyber hygiene across all layers of the Chilean population.

Additionally, cybersecurity is a highly dynamic field within computer science, constantly evolving. This means that continuous training in cybersecurity is vital to maintaining a high level of preparedness, both in private companies and government agencies. From this perspective, the provision of postgraduate studies, especially diplomas and certificates in cybersecurity, should be tailored to the needs of businesses and aimed at safeguarding the country and its citizens.

*Chapter 3_*

Advanced Research in Cybersecurity (IAC)

PARTICIPANTS IN THE ELABORATION OF THIS TEXT:

- Coordinating team of the working group "Advanced Research in Cybersecurity" subcommittee: Romina Torres and Pedro Pablo Pinacho.

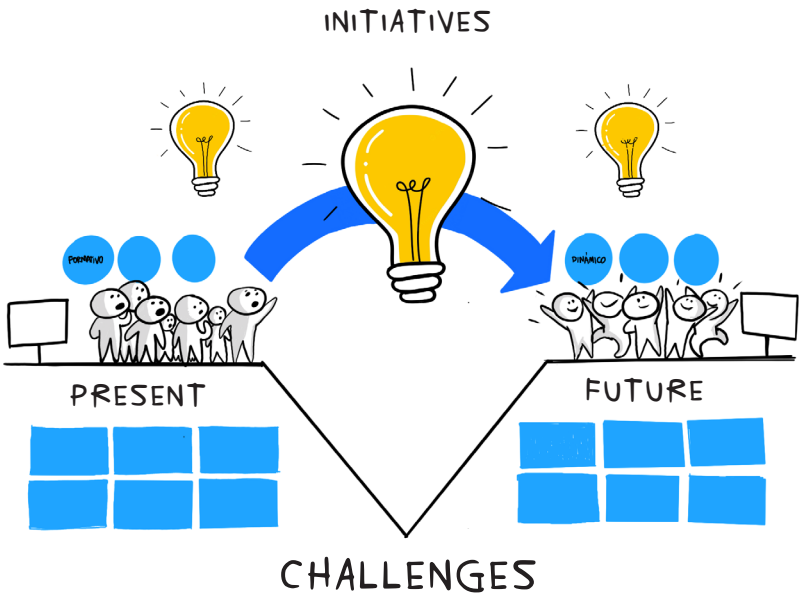
- Technical Working Committee of the working group "Advanced Research in Cybersecurity", convened by the Committee: Andres Barrientos, Mauricio Romo, Jorge Flores, Ricardo Monreal, Claudio Galleguillos Escobar, Danic Maldonado, Rodrigo Bustamante, Claudia Negri, Francisco Garcia, Sergio Leiva, Carlos Manzano, Julio Lopez Fenner, Ricardo Seguel, Rocío Ortiz, Alejandro Hevia, Gonzalo Díaz de Valdés, Javier Ramírez, and Amalia Pizarro Madariaga.

1. INTRODUCTION

In 10 working meetings/sessions held between July 16 and October 26, 2022, a team composed of 8 professionals in each meeting on average, with diverse backgrounds including engineers, businessmen, academics, and military personnel, achieved the results reflected in this chapter.

The purpose has been to analyze the current state of cybersecurity research and, based on that, propose a public-private strategy for advanced research, where academia plays the key coordinating role.

This chapter provides a prioritized list of initiatives in cybersecurity research that ensure access to infrastructure, resources, and spaces, which facilitate the visibility of their results and technological transfer for those aspiring to conduct advanced cybersecurity research in Chile. This gradual increase in the maturity level of R&D in cybersecurity, according to the University of Oxford model, aims to position the country as a relevant international actor by 2035. In the short term, the goal is "established" (4 years), in the medium term, "strategic" (8 years), and the long term, "dynamic" (12 years).



2. CONTEXT

Reference Models for Assessing Country Maturity in Research

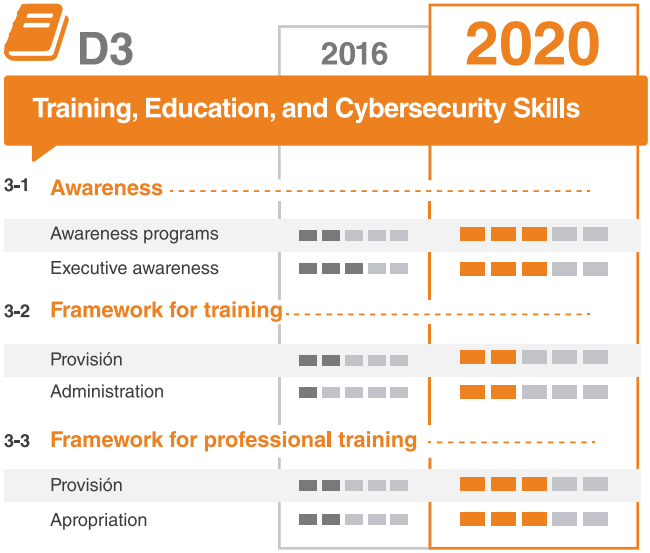
It is considered relevant to understand the models used to determine the maturity level of countries in the field of cybersecurity research, to establish a roadmap starting from a baseline level that aligns with the national reality.

Cybersecurity Maturity Model for Nations (CMM)

The Cybersecurity Maturity Model for Nations is proposed by the Global Cybersecurity Center at the University of Oxford. This model has been applied to evaluate Chile in 2016 and 2020. The model is divided into dimensions and factors, both of which can be assessed at five levels of maturity: "1-initial," "2-formative," "3-established," "4-strategic," or "5-dynamic."

Source: https://gcscc.ox.ac.uk/dimension-3-cybersecurity-knowledge-and-capabilities

Dimension 3 of this model focuses on Education, Training, and Cybersecurity Skills, where Factor D3.4: Cybersecurity Research and Innovation addresses the maturity of research capabilities in nations. However, this factor was added in the version released in 2021. Therefore, advanced research capabilities in Chile have not been evaluated by this model. In the following image, it is possible to see that Chile has reached Level 2 of maturity in terms of a framework for the training of new professionals, and has increased from Level 2 to Level 3 in terms of awareness and professional training.



Source: www.cibersecurityobservatory.org IDB-OAS 2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean

It is estimated that in Factor 3.4, the country exhibits a level between initial and formative, as there are limited **R&D activities in cybersecurity**. There are some collaborative research networks within the country (between academia/companies and police or armed forces), as well as incipient collaborations between countries. This estimation is based on the assessment criteria for Research and Development:

Factor - D 3.4: Cybersecurity Research and Innovation

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Research and Development	There are limited or no cybersecurity research and development (R&D) activities occurring in the country. There is no access to R&D activities in cybersecurity from other countries.	Some integration of cybersecurity R&D activities occurs within the country, or with a partner country that understands how cyberactivity R&D applies to the local context of the country. The country may participate in relevant regional/ international cybersecurity-related research collaboration networks. Cybersecurity R&D performance metrics are limited in scope, or *ad hoc*.	Cybersecurity R&D activities have been established and are indicated in the national cybersecurity strategy. R&D strategy may be in development. The resources and processes required to deliver the actions of cybersecurity R&D activities have been identified and are in place. Funding is adequate to deliver these actions. There is active regional/ international collaboration with leading practice and developments. The country is actively participating and contributing to regional/ international cybersecurity-related research collaboration networks. Metrics for measuring R&D performance are in place and allow progress to be measured and to improve the cybersecurity R&D capability of the country.	The country is actively building communities of interest around R&D priorities in cybersecurity. R&D strategy is in place and fully implemented. The country makes a major contribution to cybersecurity R&D and is actively involved in building innovation capacity through international R&D consortia and investment. Emerging cybersecurity risks are regularly assessed and used to update the national cybersecurity strategy and the development of future programmes of the R&D strategy. Synergy between academic institutions and industry supports R&D activities and is used to design cyber curricula that cover industry needs.	The country is a leading actor in cybersecurity research and innovation and is shaping international debates on the development of R&D strategic plans. The country is forward looking, seeing emerging issues (around new technology or new types of threat), and uses R&D to prepare a future threat environment. The country is contributing to international best practices in cybersecurity R&D.

Source: Cybersecurity Capacity Maturity Model for Nations (CMM) - 2021

1. Initial level

* If there are no or limited R&D activities in cybersecurity in the country.

2. Formative level

* If these activities occur within the country or with a partner country that understands how research and development apply to the local context.
* If the country is incipiently participating in regional/international collaborative research networks in cybersecurity.
* If there are performance metrics in R&D in cybersecurity, but they are still limited in scope or ad-hoc.

3. Established level:

* If R&D activities in cybersecurity have been established and are indicated in the national cybersecurity strategy.
* If the required resources and processes for carrying out R&D activities in cybersecurity have been identified and are operational.
* If the funding is adequate for conducting these activities.
* If there is active regional/international collaboration with practices and developments.
* If the country is actively participating and contributing to regional/international collaboration networks.
* If metrics to measure R&D performance are functioning, enabling the measurement of progress and improvement of R&D capabilities in the country.

4. Strategic level

* If the country is actively building communities of interest around R&D priorities in cybersecurity.
* If the R&D strategy is fully operational.
* If the country makes a greater contribution to R&D in cybersecurity and is actively involved in building innovation capabilities in this industry through international R&D consortia and investment.
* If emerging cybersecurity risks are regularly measured and used to update the national strategy and future development of R&D strategy programs.

5. Dynamic level

* If the country is a leading actor in research and innovation and is involved in international discussions on the development of strategic R&D plans in cybersecurity.
* If the country is forward-looking, identifying emerging issues related to new types of technology or threats, and using R&D to prepare for future threat environments.
* If the country contributes to best practices in R&D in cybersecurity.

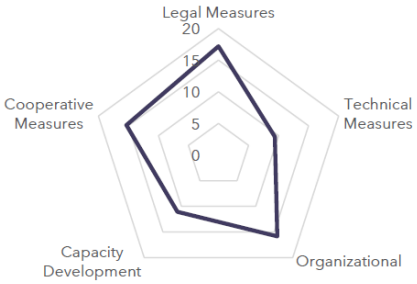
Cyber Security Index (CGI)

Another model is that of the **International Telecommunication Union (ITU)**, which helps establish a baseline situation. In particular, Pillar #4 focuses on "Capacity Building: Assessment of measures taken to generate **skills and competencies** (education and training) as well as certification processes for professionals (certifications, training, research, industry and service generation, prevention campaigns, among others), aimed at having a body of experts and professionals in the field."

In this regard, it is interesting to observe the indicators they use to measure investment in national research and development programs in cybersecurity in institutions, which may be private, public, academic, non-governmental, or international.

It considers the presence of a nationally recognized institutional body overseeing the program. Cybersecurity research programs include, among others, malware analysis, cryptography research, system vulnerability research, and security models and concepts. Cybersecurity development programs refer to the development of hardware or software solutions, including firewalls, intrusion prevention systems, honeypots, and hardware security modules. The presence of a national body will enhance coordination between various institutions and the exchange of resources.

Chile



Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
68.83	17.20	9.39	15.84	11.07	15.33

Source: ITU Global Cybersecurity Index v4, 2020

According to ITU Reports, to show evidence that a country is mature in advanced research, clear evidence of the following must exist:

- **R&D activities in cybersecurity** at the national level.
- **R&D programs in cybersecurity** in the **private sector.**
- **R&D programs in cybersecurity** in the **public sector.**
- Participation in **R&D activities by higher education institutions**, such as academia and universities.
- The existence of governmental incentive mechanisms in place, such as tax exemptions, grants, funding, loans, provision of facilities, and other economic and financial motivators, including nationally dedicated and recognized institutional motivators.
- Existence of a body overseeing capacity development activities in cybersecurity. Incentives increase the demand for cybersecurity-related services and products, which improves defenses against cyber threats.
- **Measures to foster capacity development for the cybersecurity industry.**

ENISA

ENISA (European Union Agency for Cybersecurity) published in September 2022 the framework to define the necessary skills for different profiles in cybersecurity research and other fields. link to the framework: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

It states that **"A cybersecurity researcher is someone who conducts research in cybersecurity subjects and incorporates these findings into cybersecurity solutions."** They conduct both applied and basic/fundamental research, collaborate with stakeholders, perform experiments, and develop proof of concepts, pilots, and prototypes for cybersecurity solutions. They are familiar with cybersecurity standards, methodologies, and frameworks, as well as legal and regulatory requirements, and information security procedures.

A cybersecurity researcher is expected to demonstrate knowledge, competencies, and skills in the following areas:

Knowledge:

- Research, development, and innovation in cybersecurity.
- Cybersecurity standards, methodologies, and frameworks.
- Legal, regulatory, and legislative requirements for deploying or using cybersecurity technologies.
- Multidisciplinary aspects of cybersecurity.
- Non-disclosure procedures.

Competencies:

- Monitoring technology trends.
- Innovation.
- Analytics and data science.
- Problem management.
- Information and knowledge management.

Skills:

- Generating new ideas and translating theory into practice.
- Analyzing systems to identify weaknesses and ineffective controls.
- Analyzing systems to develop solutions that address security and privacy requirements.
- Monitoring advancements in cybersecurity-related technologies.
- Communicating, presenting, and reporting to relevant stakeholders.
- Identifying and resolving cybersecurity problems.
- Collaborating with team members and colleagues.

The tasks performed by a cybersecurity researcher include:

- Analyzing and evaluating cybersecurity technologies, solutions, developments, and processes.

- Conducting research, innovation, and development in cybersecurity topics.
- Expressing and generating innovative ideas.
- Contributing to the state of the art.
- Assisting in the development of innovative cybersecurity solutions.
- Conducting experiments and developing proof of concepts, pilots, and prototypes for cybersecurity solutions.
- Providing innovative cybersecurity services, solutions, and products.
- Assisting in building cybersecurity capabilities such as awareness, technical and practical training, mentoring, testing, and supervision.
- Identifying advancements in cybersecurity and applying them in their approaches and solutions.
- Leading or participating in innovation processes.
- Publishing and presenting scientific papers and R&D results

3. COUNTRY'S SITUATION IN IAC (INFORMATION ASSURANCE AND CYBERSECURITY)

In our National Cybersecurity Policy 2018-2022 (NCP), Objective E states the following: "The country will promote the development of a cybersecurity industry that serves its Strategic Objectives, highlighted as:

SO-NCP1. Emphasizing the importance of innovation and development in cybersecurity.

SO-NCP2. Positioning cybersecurity as a means to contribute to Chile's digital development.

SO-NCP3. Enabling the development of the cybersecurity industry in Chile.

SO-NCP4. Contributing to the generation of supply by the local industry.

SO-NCP5. Stimulating demand from the public sector based on the strategic interests of the State.

Measure 41 - SO-NCP6: Encouraging the export of national products and services in the cybersecurity field by identifying international fairs and evaluating sources of support.

If this policy had achieved the objectives and measures mentioned above, it would be expected that the country would have a higher level of maturity in factor 3.4 of dimension 3 of the CMM regarding IAC.

Indeed, if a national cybersecurity industry existed, emphasizing innovation in cybersecurity, its products would already be operational, at least meeting local demand, contributing to Chile's digital development from a "secure" perspective, and starting to export these products internationally. Therefore, the country would likely be actively participating in international forums and discussions as a reference.

By analyzing the policy and its current operationalization according to the evaluation reference models, the following gaps (B) or needs are identified:

B1. Lack of reference to an International Policy in cybersecurity matters.

B2. Insufficient participation of the country in multilateral and global instances that support regional, subregional, and multilateral consultation processes in the area, particularly in Latin America (at least regarding R&D in cybersecurity).

B3. Lack of important alliances between internal security and external defense agencies with the national industry in the field.

B4. Failure to leverage the opportunity to grow the ICT sector (which represented about 3-4.12% of Chile's total economy in 2017, while the average participation of this sector in OECD countries was about 6% of their economies) by developing the cybersecurity component within that industry.

B5. Failure to identify strategic domains for short, medium, and long-term development. For example, the national industry is linked to the development and use of encryption standards.

B5.1. Failure to identify the supply of products resulting from R&D processes in cybersecurity by the local industry.

B5.2. Failure to identify the demand from the public sector that should be addressed by the cybersecurity industry.

B6. Insufficient level of maturity in the R&D dimension of Cybersecurity.

Specific measures in National Cybersecurity Policies that were declared to be implemented during the 2017-2018 period but are not evidenced with results are described in this document as gaps:

B-MINSEGPRES: Absence of a technical standard for the development or procurement of software within the State, following secure development standards.

B-MINREL-1: Non-existence or lack of awareness of an interagency working group to address international cyber-related issues.

B-MINREL-2: Insufficient exchange of experiences with other countries regarding cybersecurity (benchmarking).

B-CORFO-MINDEF-MINECON: Absence or an insufficient number of special programs to promote the national cybersecurity industry in defined sectors.

B-MINREL (Prochile)-MINECON: Insufficient means of support and promotion for the export of national products and services in the field of cybersecurity.

Furthermore, the following weaknesses are evident for conducting IAC in Chile:

-Lack of infrastructure for cybersecurity research and development.

-Lack of demand for research capabilities in cybersecurity at the national level, especially interdisciplinary demands.

-Lack of visibility for the results of existing research initiatives.

-Lack of a scientific and technological base for the cybersecurity industry.

-Lack of national budget for cybersecurity research and development activities.

4. FUTURE SITUATION

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

Taking the CMM as a model to consider, our development should aim to achieve a "3-Established" level of maturity in R&D for cybersecurity in the short term, a "4-Strategic" level in the medium term, and a "5-Dynamic" level in the long term.

For this purpose, it is relevant to develop a National Cybersecurity Strategy, along with an operational plan for the IAC that explicitly identifies and considers the following:

For the short term (4 years), to achieve a **"3-Established"** maturity level:

1. The IAC activities are being carried out in the country.

2. The resources and processes required to conduct IAC activities.

3. Adequate sources of funding for these activities.

4. Regional and international actors involved in research, showcasing evidence of regional/international collaboration networks, practices, and developments.

5. Metrics and their values allow measuring the performance of IAC actions and the progress made.

For the medium term (8 years), after establishing a foundation, to reach a **"4-Strategic"** maturity level:

1. Communities around priority areas of IAC.

2. Evidence that the R&D section of the National Cybersecurity Strategy is fully functioning.

3. Contribution of funding to support R&D in cybersecurity.

4. International R&D consortiums and investments to build innovative capacities in the field of IAC.

5. Emerging cybersecurity risks are being addressed, with evidence that they are regularly measured and used to update the national strategy, particularly the IAC programs section.

Finally, for the long term (12 years), to achieve a "5-Dynamic" maturity level, the following evidence must exist:

1. Recognition in relevant rankings that Chile falls into the quadrant of leaders in cybersecurity research and innovation.

2. Involvement of Chile in international discussions contributing to the development of regional strategic plans for R&D in cybersecurity.

3. An observatory unit that identifies emerging problems related to new technologies or threats.

4. R&D activities to prepare for future threats.

5. Generation of best practices in R&D for cybersecurity.

5. PROGRAM OF PRIORITY INITIATIVES

To progress toward the desired future situation as outlined in the previous point, the following action programs are proposed:

Program 1: National Research Center for Cybersecurity

Pillar: Research Capabilities

Objective: Consolidate in Chile a center for developing cyber capabilities that becomes a regional reference for advanced research in various areas of cybersecurity expertise.

Description: The program aims to have teams of researchers collaborating to address challenges and priority threats for the country. It will bring together new researchers at different levels to bridge entry gaps or retrain those from related fields.

Preparatory Actions:

• Establish:

→ A platform to conduct a national registry of cybersecurity researchers.

→ An indexed catalog on GitHub of publications (papers/theses/reports), codes, and datasets generated in Chile.

→ Registries of collaborative intersectoral research centers focused on cybersecurity.

→ A registry of collaborative research networks for cybersecurity within the country, between organizations, at regional and international levels.

Generate:

→ An annual report studying the current, emerging, and future priority areas in cybersecurity that can be addressed.

→ A dashboard of metrics associated with IAC in Chile.

→ An annual web dashboard of future threats and emerging risks in cybersecurity.

Actions

· Establish IAC Communities in:

→ Machine Learning Poisoning
→ Detection capabilities optimization
→ Cryptography
→ Interoperability
→ Digital identity with biometrics
→ Fake News and Disinformation Online
→ Resilience in Critical Infrastructure/IoT
→ Digital Forensic Investigation
→ Smart Cities and sub-communities (e.g., Smart Health)
→ Regulations and legislation
→ Cybersecurity by design
→ Privacy by design
→ Cybersecurity research

Metrics

· Number of:

→ IAC focus areas

→ Emerging cybersecurity risks from the previous year, current or future recognized as a priority for the country
→ Initiatives generating IAC in future threats
→ Scopus/WoS publications
→ Released datasets
→ Released tools
→ Training
→ Dissemination events held
→ Citations of publications
→ ANID-funded projects (National Agency for Research and Development) involving the community
→ Projects in collaboration with public and private organizations
→ International collaboration projects
→ Catalog contributions by type
→ Doctors in IAC working in the industry

· Percentages of:

→ Addressed threats
→ Addressed emerging risks
→ Doctors in IAC working in the industry
→ Active Communities
→ Researchers regularly update information in the platform annually
→ Use of Indexed Catalog

Program 2: Scaling and New Business Center for Research Results in Cybersecurity

Pillar: Innovation Capabilities, Applied Technological Development, and Business.

Objective: Facilitate the development of the scientific and technological-based products and services industry in the field of cybersecurity in Chile, which helps position the country in innovation, applied research, and technological development for cybersecurity.

Description: The program aims to bring together researchers working in silos within the country, fostering collaborative and multidisciplinary projects that involve public and private institutions, including those in defense and other relevant sectors. The goal is to incubate and scale scientific and technological-based developments in the national and international markets, either by entering or by converting others from related fields.

Preparatory Actions:

· Conduct an industry characterization study.
· Foster important partnerships between national security and defense agencies and the local industry.
· Establish an interdisciplinary platform for IAC challenges.
· Support a Public Innovation Challenge (a joint initiative by ANID and the Government Laboratory) in cybersecurity.

Actions:

· Develop

→ Open innovation models for applied research in IAC.
→ Scaling models.
→ Internationalization models.
→ Competitions for commissioned research and development in cybersecurity that require university-industry collaboration.

· Establish

→ Programs to strengthen the cybersecurity industry.
→ Entrepreneurship programs in cybersecurity.
→ Materials for disseminating and training on best practices to successfully turn applied research in cybersecurity into scientific and technological-based products in the industry.
→ Significant partnerships between national security and defense agencies and the industry.

· Actively participate in national and international fairs and forums to showcase and position Chile as a regional and global leader in various IAC capabilities. Participation in events such as FIDAE, EXPOMIN, and EXPONAVAL, among others, contributes to this objective.

Metrics

· Number of:

→ Active projects to strengthen cybersecurity in specific industrial sectors through multidisciplinary IAC approaches.

→ Participating institutions in open innovation initiatives in cybersecurity focused on solution, product, or service development.
→ Projects established after the open innovation challenge.
→ Commissioned research involving university and industry collaboration.
→ I+D+i projects based on IAC sponsored by the state.
→ IAC products at Technology Readiness Level (TRL) 5 or higher.
→ Scaled IAC-based products.
→ Businesses revolving around IAC-based products.
→ IAC-based products with international reach.
→ Licenses (or other intellectual property protection mechanisms) are effectively transferred for commercial exploitation.
→ National companies or scientific and technological-based startups offering or developing cybersecurity products or services for the local or international industry.
→ Relevant participants in events.

· Percentage of researchers involved in collaborative projects.

· Increase in the size of the ICT (Information and Communications Technology) sector due to IAC.

Program 3: Distributed National Laboratory for R&D in Cybersecurity

Pillar: Resource Capabilities

Objective: Enable a shared infrastructure for researching, developing, and testing algorithms/models/products in the cybersecurity segment for different industries while optimizing resources.

Description: This program addresses the lack of infrastructure to conduct cybersecurity research. It first identifies the existing requirements and resources as a baseline, then contrasts them with the needs posed by future priority threats to the country. Lastly, it facilitates joint applications to the Fondequip competition (ANID's Scientific and Technological Equipment Fund) for funding.

Preparatory Actions:

- Identify financing mechanisms or structures to ensure the continuity of capabilities development in cybersecurity and its various specialization areas.
- Provide a platform to collect infrastructure requirements in terms of processing resources.
- Identify potential geographical nodes that can integrate national digital research and development capabilities.
- Promote visibility of existing infrastructure resources in terms of processing and storage.

Actions:

- Create:

→ Testing and Prototyping Laboratories for R&D projects in Cybersecurity.
→ Distributed national laboratory for cybersecurity.

- Raise Projects

→ Raise emblematic projects in laboratories that allow leverage between industry, the State, and academia. (equivalent in scope to the National Satellite Project)
→ Fondequip with partners.

- Develop

→ Program allowing researchers to conduct experiments in IAC at no cost.
→ Guide to the best practices for resource and process requirements in IAC activities.

- Establish an Infrastructure Starter Kit to facilitate IAC activities.

Metrics

- Number of:

→ Nodes in the national IAC network.
→ Nodes providing infrastructure resources.

→ Users of Testing and Prototyping Laboratories.
→ Users of the Distributed National Laboratory.
→ New researchers are indirectly funded through the program.
→ Researchers benefiting from starter kits.
→ Recognized research results achieved using the infrastructure.
→ Concept tests are conducted in laboratories.
→ Sector-specific (industry, government, defense, retail, banking, etc.) development and research initiatives in cybersecurity focused on national development.

· Percentages of

→ Minimum required infrastructure for IAC in different areas.
→ Occupancy rate of the Distributed National Laboratory.
→ Coverage of infrastructure demands.
→ Satisfaction with the starter kit.
→ Improvement opportunities for the starter kit were identified by researchers and successfully addressed by the community.

· Financing and investments support the generation of a critical mass of specialists and the development of national cybersecurity capabilities and technological advancements.
· Funds obtained through Fondequip awards

Program 4: Ibero-American Center for Cybersecurity Research (CIICC)

Pillar: Coordination Capabilities

Objective: Position Chile as an IAC leader in Oxford CMM's 5 dimensions.

Description: CIICC is a coordinating body for a network of research, scaling, and dissemination centers. It monitors and supports compliance with the national cybersecurity policy and collaborates with different government organizations to advance IAC in Chile and enhance capabilities across the country, including the development of human resources. CIICC aims to have a continental reach, addressing the broad spectrum of cybersecurity based on the 5 dimensions of CMM. Will become the link related to Oxford.

Previous Actions:

· Create a web dashboard for
→ the operationalization of the current National Policy
→ the activities of the IAC network in the country.
· Establish a national registry of known vulnerabilities in solutions/devices used in Chile for proper patching, using tools like Jira.
· Officialize a process that facilitates the integration of academia in technological development areas within government organizations.
· Form a consortium of national universities to create a cybersecurity capabilities center following the model of the University of Oxford.

Actions:

· Integrate the consortium of universities into the "constellation" of Cybersecurity Capability Centers led by the University of Oxford, which includes countries like Australia and South Africa.

· Create

→ A coordinating entity for the national IAC network to strengthen cybersecurity capabilities in government organizations and companies in Chile.
→ A free public unit for ethical hacking.
→ A certification unit for software cybersecurity compliance.
→ A certification unit for IoT (Internet of Things) cybersecurity compliance.
→ A certification unit for medical device cybersecurity compliance.
→ Operational units to measure the level of cybersecurity maturity (CMM) in countries, enabled by the University of Oxford to conduct assessments.
→ A unit to be a counterpart of NIST (National Institute of Standards and Technology USA), providing free training on cybersecurity standards.
→ A study group to define standards, procedures, and guidelines in IAC.

· Facilitate the creation, with the corresponding agencies, of:

→ Scholarships for academic and scientific doctoral degrees in multidisciplinary IAC (other disciplines) and specific sectors.

→ ANID Millennium Institute/centers/Nucleus of Research with a focus on cybersecurity.
→ ANID/Corfo contests associated with FONDEF (Scientific and Technological Development Fund) for thematic cybersecurity ideas/technology.
→ National Research Center on Cybersecurity (not affiliated with any university or university consortium), similar to the INRIA (French Institute for Research in Computer Science and Automation).
→ International experts' import program (ANID contest).
→ Scholarships for researcher internships in international IAC centers.
→ IAC internship opportunities in cybersecurity research areas.
→ Internships in National Research Centers on Cybersecurity.
→ Internship opportunities for undergraduate and postgraduate students in national and international industries and government entities, as well as in the network of centers to accelerate technological capacity development in the country.
→ Incentives for startup-industry collaboration.
→ Scaling program and new business calls based on cybersecurity research results (CORFO-ANID).
→ International cooperation projects through International Collaboration Programs (PCI) with resources for networking, supported by ANID.
→ Financing instrument for attracting investments to foster the growth and development of the cybersecurity industry (ANID).
→ Incentive mechanisms for state sponsorship of R&D+i projects, whether publicly or privately funded, nationally or internationally, in the field of cybersecurity.
→ ANID/Corfo contests associated with thematic cybersecurity startups.

· Organize hackathons to detect vulnerabilities and develop patches for IoT devices, medical devices, and software solutions developed/used in Chile.

· Support the creation and participation in technical standards for software development or procurement in the government, aligned with secure development standards.

Metrics

· Number of:

→ Supported organizations.
→ Ethical hacks performed on small and medium-sized enterprises (SMEs).
→ Organizations are supported by the entity that has built defense capabilities.
→ Software compliance levels of cybersecurity.
→ Solutions including IoT compliance levels of cybersecurity.
→ Medical devices with compliance levels of cybersecurity.
→ Ethically hacked devices/solutions.
→ Incidents in the national registry.
→ Startups using the technical standard.
→ Centers with up-to-date information in the web dashboard.
→ Scholarships granted in IAC.
→ Scholarships granted in sector-specific IAC.
→ Research centers/institutes in IAC.
→ FONDEF projects in IAC.
→ International experts with stays longer than two weeks in Chile through IAC networks' initiatives.
→ Senior researchers benefit from internships at international IAC centers.
→ Junior researchers benefit from internships at national IAC centers.
→ Professionals/students benefiting from internships.
→ IAC Ph.D. graduates working in the industry (percentage of Ph.D. graduates working in the industry).
→ Chilean scientific-technological-based companies or startups offering or developing cybersecurity products or services for the local or international industry.
→ State-sponsored I+D+i projects based on IAC.

· Percentages of
→ Policy points addressed and documented showing evidence of progress.
→ Resolved incidents.
→ Non-technical IAC scholarship recipients.

· Average time to resolve incidents.

Additional Note: These proposed programs have successful references in other areas of science and technology in our country, such as:

•Proof-of-concept or simulation laboratories.
•ANID Corfo Centro 5G Lab - 5G Claro Innovation Center Uc. https://centrodeinnovacion.uc.cl/claro-y-el-centro-de-innovacion-uc-se-unen-para-impulsar-el-desarrollo-de-5g-en-chile/
•Simulation spaces like the NSU Broward Center of Innovation, Nova Southeastern University.
•https://www.corfo.cl/sites/cpp/convocatorias/centro_escalamiento_y_tecnologias_5g
•Applied research incentives and university-industry collaboration: The European Union granted 49 million euros in 2020 to boost innovation in cybersecurity and privacy systems.
•Corfo I+D challenges. : https://www.corfo.cl/sites/cpp/convocatorias/movil/crea_y_valida
-Dissemination events like Siemens Mineral Week. https://on.mediastre.am/events/mediastream--eventos-us/siemens-minerals-week
•Open Innovation challenges:
Boundless Challenges: https://centrodeinnovacion.uc.cl/sin-limites/ https://www.openinnovation.sg/imda
-Venture Capital Funds in Cybersecurity: https://topstartups.io/?industries=Cybersecurity
Advanced Human Capital Models in the Industry: https://www.anid.cl/concursos/concurso/?id=1199
•Cybersecurity venture capital funds.
•Advanced human capital models in the industry.
•National Satellite Project (SNSAT) as a model for national development in space-related matters, including integration into society as an opportunity for development in various educational and industrial sectors.
•International Air and Space Fair as a reference point for showcasing the country's advanced capabilities in the aerospace and cyberspace domains.

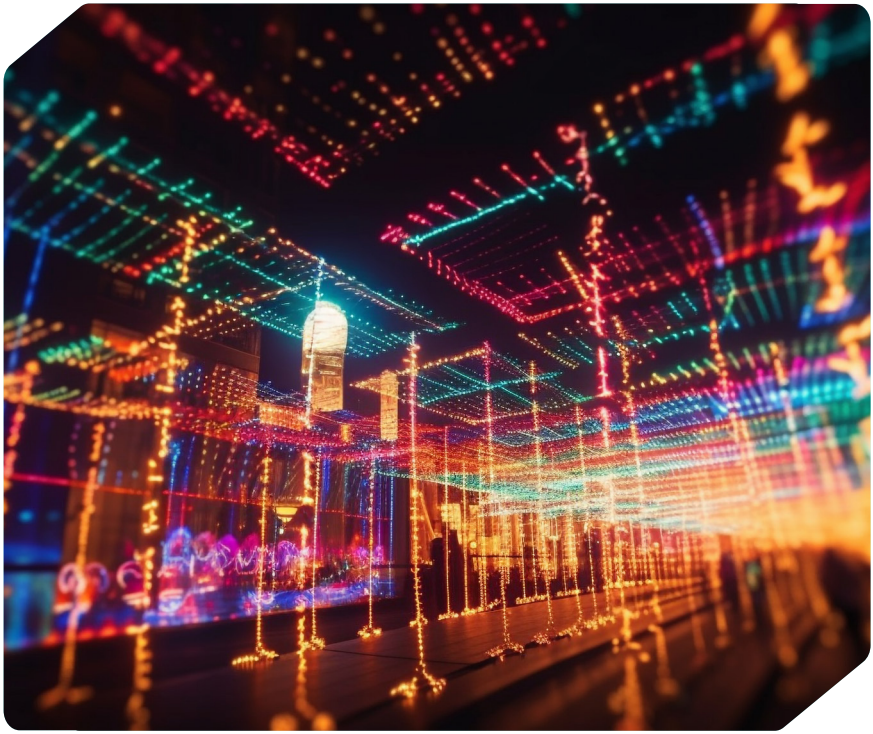
Analysis of Inputs/Literature

1. Estrategia Digital 2035
https://www.cepal.org/sites/default/files/events/files/estrategia_de_transformacion_digital_chile_2035_.pdf
2. Política Nacional de Ciberseguridad 2018-2022
https://www.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf
3. The Oxford Cybersecurity Capability Maturity Model, which positions Chile between 2 and 3, assesses the maturity of a nation's cybersecurity capabilities. This model specifically focuses on the research dimension. https://gcscc.ox.ac.uk/cmm-dimensions-and-factors https://www.youtube.com/watch?v=wrnxeaPKJfg
4. Estonia - National Cyber Security Index (NCSI https://ncsi.ega.ee/)
5. International Telecommunication Organization, ITU, known as the ITU. Global - Cyber Security Index (CGI)
6. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework
7. https://www.cyberroad-project.eu/
https://cybilportal.org/wp-content/uploads/2021/07/Global-Overview-of-Assessment-Tools_CLEAN_07July.pdf
8. Papers to read
The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions
S Creese, WH Dutton, P Esteve-González
Personal and Ubiquitous Computing 25 (5), 941-955
The Solution is in the Details: Building Cybersecurity Capacity in Europe
S Creese, WH Dutton, P Esteve-Gonzalez, M Goldsmith, E Nagyfejeo, ...
Available at SSRN 4178109

Glossary References: https://www.nsf.gov/news/special_reports/cybersecurity/glossary.jsp
.

*Chapter 4_*

Emerging Technologies in Cybersecurity for Chile



PARTICIPANTS IN THE ELABORATION OF THIS TEXT:

- Coordinating team of the working group " Emerging Technologies in Cybersecurity for Chile ": Rodrigo Alfaro and Luz Cardona

- Technical Working Committee of the working group "Emerging Technologies in Cybersecurity for Chile " convened by the Committee: Miguel Solís, Carlos, Bustos, Pablo Itaim, Yerka Yukich, Francisco Correa, Mirko Koscina, Ricardo Dorado, Juan Lopizic, Puppy Rojas, Juan Pablo Gonzalez y Ricardo Soto.

1. INTRODUCTION

The enactment of Law No. 21.180 on the Digital Transformation of the State has involved continuous modernization processes that have presented challenges in various areas. One such challenge has been fostering a culture of digital citizenship, while also addressing cybersecurity issues through coordination efforts between the public and private sectors.

It is important to identify the technologies that impact cybersecurity to incorporate them into the Digital Transformation Strategy for 2035. To achieve this, we need to understand the state of the art concerning emerging technologies, identify future challenges and their domains and categories, and propose their application and uses through a methodological analysis.

In more than 12 working meetings held between June 22 and November 30, 2022, a team composed of 13 professionals with diverse backgrounds, including lawyers, engineers, journalists, entrepreneurs, academics, and others, achieved the results reflected in this chapter.

2. CONTEXT

Emerging technologies are understood as those with the potential to transform an existing industry, either due to their novelty or their impact. The identified lines of work with emerging technologies include Cybersecurity, Analytics, IoT, New Dimensions, Artificial Intelligence, Robotics, Cloud Computing, Blockchain, and 3D Printing (Building the Digital State, 2019 EY Global).

For this work, the selected line of emerging technology is cybersecurity. It will be approached by recognizing its domains/categories to facilitate the fields of its application, evolution, and prospects.
The domains of cybersecurity refer to the various ways in which cybersecurity methodologies can be implemented.

They are highly complex and constantly changing. Common domains in cybersecurity include application security, physical security, risk assessment, and threat intelligence.

Each part of the cyber domain has its own distinct set of security challenges and risks that must be addressed. To protect the cyber domain, organizations must identify the challenges and risks associated with each subdomain and mitigate them.

There is a need to address cybersecurity risks from a multi-scale systems perspective, recognizing the diverse interactions between cyber, physical, and human systems (Lambert et al., 2013). In this regard, it is important to frame the problem in terms of cyber resilience, where Linkov et al. (2013) discuss how decision-makers require the ability to plan for threats and absorb, recover, and adapt to them across physical, information, cognitive, and social domains in which these multi-scale systems exist (Zachary A. C., Igor L., and James H. L., 2013).

The physical domain includes hardware, software, and networks as basic components of the cyberinfrastructure. For example, Gilmore et al. (2013) described the risks posed by counterfeit electronic components in the context of hardware security.

The information domain involves monitoring, information storage, and visualization. Baiardi and Sgandurra (2013) analyzed a risk assessment methodology based on simulation, which models adaptive threat agents and identifies effective countermeasures. Cam and Mouallem (2013) described a way to dynamically model mission assurance by monitoring cyber assets and included a risk management scheme to mitigate them to acceptable levels. Finally, Ezell et al. (2013) described a framework for modeling the risks and impacts of cyber attacks on traffic control systems.

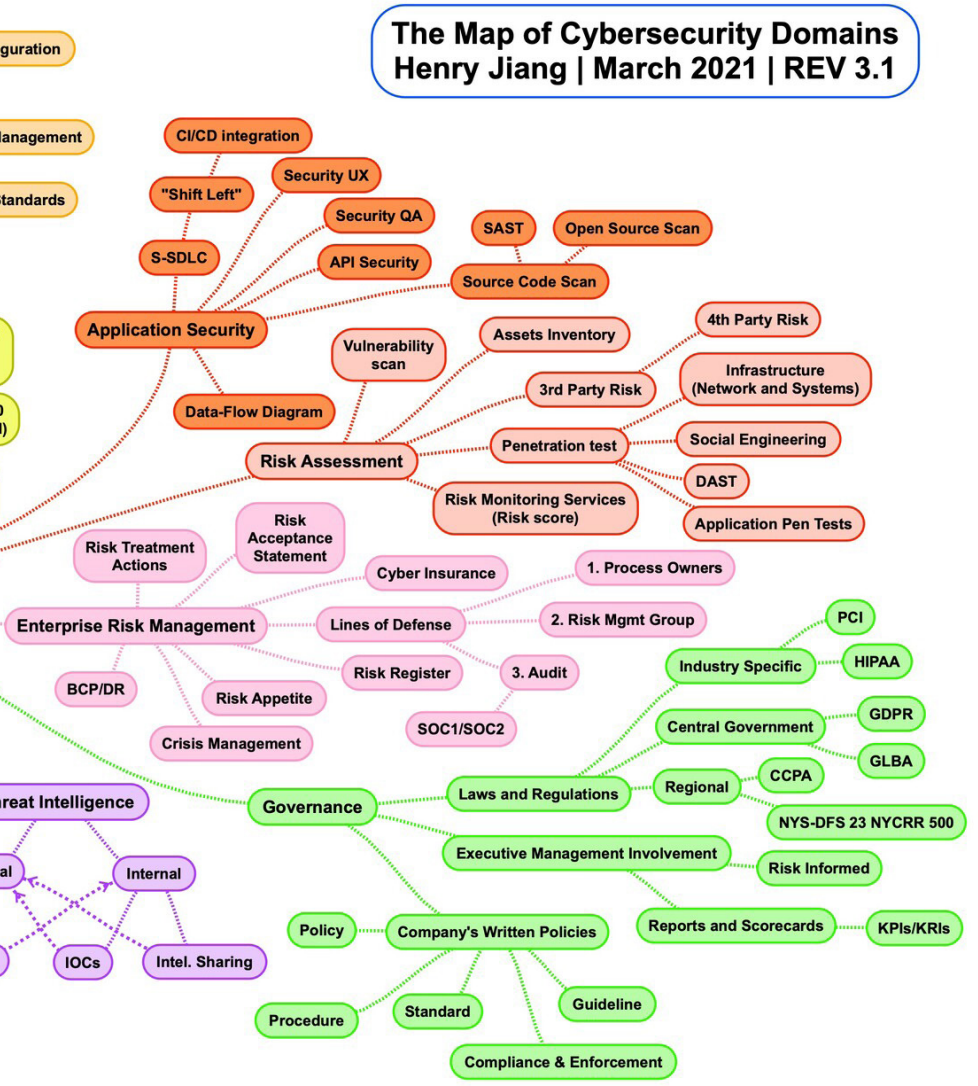
In the cognitive domain, information must be properly analyzed, detected, and utilized for decision-making. For example, Rosoff et al. (2013) explored the mental decision-making heuristics used by individuals when faced with a cybersecurity dilemma. They presented the results of two experiments in which the gain-loss framework for participants was modified when they were presented with cybersecurity scenarios.

Cybersecurity decisions must be consistent with the social, ethical, and other considerations characteristic of the social domain that surrounds them. Some authors have worked on the social domain, such as Sheppard et al. (2013), who addressed cybersecurity from an organizational perspective, described how organizations can be better prepared to respond to cyber threats, and provided a survey and dashboard to measure readiness levels. Pawlak and Wendling (2013) then explored existing and future trends in government policies related to cybersecurity, identified gaps, and possible paths forward. Kelic et al. (2013) described an agent-based decision framework to model the macroeconomic impacts of cyber attacks on vulnerable industrial sectors such as the oil and gas industry. Vaishnav et al. (2013) described a novel framework that connects cybersecurity and international relations as a unified system, commenting on the properties of such a system.

On the other hand, Jiang, H. (2021) proposes a map of 11 domains of cybersecurity with their respective subdomains or categories (see Figure 1).

Figure 1: Mind map of domains and subdomains in cybersecurity

Source: Henry Jiang, 2021


The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1
guration
anagement
tandards
CI/CD integration
Security UX
"Shift Left"
Security QA
S-SDLC
API Security
SAST
Open Source Scan
Source Code Scan
Application Security
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Infrastructure (Network and Systems)
Data-Flow Diagram
Risk Assessment
Penetration test
Social Engineering
DAST
Risk Monitoring Services (Risk score)
Application Pen Tests
Risk Acceptance Statement
Risk Treatment Actions
Cyber Insurance
1. Process Owners
Enterprise Risk Management
Lines of Defense
2. Risk Mgmt Group
PCI
Industry Specific
HIPAA
Risk Register
3. Audit
BCP/DR
Risk Appetite
SOC1/SOC2
Central Government
GDPR
GLBA
Crisis Management
reat Intelligence
Governance
Laws and Regulations
Regional
CCPA
NYS-DFS 23 NYCRR 500
Executive Management Involvement
Risk Informed
al
Internal
Reports and Scorecards
KPIs/KRIs
Policy
Company's Written Policies
IOCs
Intel. Sharing
Procedure
Standard
Guideline
Compliance & Enforcement

For the domains worked on, the following description was adopted:

1. Security Architecture: The domain of Security Architecture refers to a plan and a set of principles that describe the security services a system must provide to meet the needs of its users, the system elements to implement the services, and the performance levels required to address the threat environment. This domain also includes 23 subdomains.

2. Security Operations: The Security Operations domain primarily focuses on detecting and protecting confidential and critical business information within any organization. Some of its functions include threat hunting, incident response, threat intelligence, and forensic analysis. This domain also includes 16 subdomains.

3. Governance: IT Security Governance is the system through which an organization directs and controls IT security (adapted from ISO 38500). IT Security Governance should not be confused with IT security management. IT security management concerns itself with making decisions to mitigate risks, while governance determines who is authorized to make decisions. Governance specifies the accountability framework and provides oversight to ensure risks are adequately mitigated, while management ensures controls are implemented to mitigate risks. Governance ensures security strategies are aligned with business/strategic objectives and consistent with regulations. This domain also includes 20 subdomains.

4. Enterprise Risk Management: An ERM program can help increase awareness of business risks throughout the organization, instill confidence in strategic objectives, enhance compliance with regulatory and internal compliance mandates, and improve operational efficiency through more consistent application of processes and controls. This domain also includes 13 subdomains.

5. Physical Security: It describes measures designed to ensure the physical protection of IT assets, such as facilities, equipment, personnel, resources, and other properties, against damage and unauthorized physical access. Physical security measures are taken to protect these assets from threats such as theft, vandalism, fires, and natural disasters. This domain includes one subdomain.

6. Career Development: Cybersecurity professionals work in companies and industries of all sizes to protect organizations from attacks and data breaches. This domain also includes 6 subdomains.

7. Threat Intelligence: Also known as cybersecurity threat intelligence (CTI), is organized, analyzed, and refined information about potential or actual attacks that threaten an organization. The primary purpose of threat intelligence is to help organizations understand the risks posed by the most common and severe external threats, such as zero-day threats, advanced persistent threats (APT), and exploits. This domain also includes 5 subdomains.

8. Risk Assessment: It identifies various information assets that could be affected by a cyber attack (such as hardware, systems, laptops, customer data, and intellectual property), and then identifies the various risks that could affect those assets. This domain also includes 10 subdomains.

9. Frameworks and Standards: This is a voluntary guide based on existing standards, guidelines, and practices for organizations to better manage and reduce cyber security risks. In addition to helping organizations manage and reduce risks, it was designed to foster risk management and cyber security communications among internal and external stakeholders of the organization. This domain also includes 5 subdomains.

10. Application Security: The process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification. This domain also includes 10 subdomains.

11. User Education: It strives for the systematic delivery of awareness and training programs that provide security expertise and help establish a security-conscious culture. This domain also includes 3 subdomains.

Based on the above 11 domains, a review is conducted to identify companies that may be working in these fields at the national level, and in some cases, to assess the maturity level of the selected emerging technology

On the other hand, in the "Cyber Defenders 2021" report, 14 categories were presented that will guide the near future of companies dedicated to or involved in cybersecurity: "Identity orchestration, Data Firewalls, Security creds, Outsourced security, SaaS security, Crypto defense, Security-infused networks, Cyber automation, API Protection, Cyber Insurance, Shift Left Security, Secure Data Sharing, Auto Security, Post Quantum cryptography." Here are some reflections on the current discussions surrounding these categories:

1. Identity orchestration: Organizations operating in local systems and multiple clouds lack a single, unified solution to manage identity and restrict access to data and systems.

2. Data Firewalls: Organizations face financial costs and reputation damage when hackers steal their data or when it becomes publicly leaked.

3. Security creds: Past breaches have highlighted that an organization is only as strong as its weakest partner. To adapt to this new threat landscape, organizations are looking to differentiate themselves from competitors and win business by showcasing their security credentials.

4. Outsourced security: Managing multiple vendors, staying up-to-date on the latest technologies and threats, and hiring skilled talent can overwhelm corporate security teams.

5. SaaS security: Organizations across industries have increased their use of Software-as-a-Service (SaaS) applications, or third-party software running in the cloud, in recent years, introducing additional cybersecurity risks.

6. Crypto defense: While blockchain has properties that support security and privacy, it is not immune to cyber-attacks.

7. Security-infused networks: Companies rely on reliable networks to enable an effective remote workforce. Historically, these networks have been protected with numerous point solutions (e.g., VPN, firewalls, cloud access security brokers), which can frustrate IT teams and employees.

8. Cyber Automation: Cyber attacks, alerts, and vulnerabilities continue to increase, while the supply of qualified cybersecurity professionals remains limited. This imbalance challenges businesses seeking to protect their systems and data.

9. API Protection: The use of Application Programming Interfaces (APIs) has skyrocketed in all industries in recent years, bringing security risks that require new protections.

10. Cyber Insurance: Data breaches of all sizes have become more costly in the past three years.

11. Shift Left Security: When it comes to software development, security considerations are often the last step before release. Developing software without considering security can, at best, cause delays and inefficiencies, and at worst, create serious vulnerabilities.

12. Secure Data Sharing: To make use of data (e.g., identifying new treatments in medicine, developing customer profiles in retail, etc.), companies may seek to share, combine, and analyze sensitive information. Protecting this shared data while meeting regulatory standards presents a challenge.

13. Auto Security: As vehicles adopt new technologies and effectively become data centers on wheels, they create new opportunities for hackers.

14. Post Quantum cryptography: As quantum computing advances, it will eventually be able to decipher current methods of public key encryption.

According to Gartner studies (2021), emerging cybersecurity technologies have been generating significant impacts on organizations (see Table 1).

Table 1: Emerging Technology Trends

	Hoy	1 a 3 años	3 a 6 años	6 a 8 años
Business Enablers	• Low-code Application Platform (LCAP)	• Application Ecosystmes	• Smart Contract • Productuzation of Data • Distributed Ledgers • Packaged Business Capabilities • Distributed Cloud • Tokenization • mmWave 5G	• AR Cloud • AI-Generated Composite Applications
Productivity Revolution	• Deep Neural Networks • Cloud AI Developers Services • Edge AI	•	• Model Compression • Composite AI	•
Interfaces and Experiences	• Advanced Computer Vision	• Transformers-Based Language Models • Advanced Virtual Assistants	• Smart Personalization • IoT Platforms • Digital Twin	•

Source: based on Gartner, 2021

3. FUTURE CHALLENGES

3.1. Quantum Computing (QC)

Quantum Computing is a field of computer science that emerged in the early 1980s, based on the principles of quantum theory. It involves the behavior of matter, energy, and information at the subatomic level, to develop new systems that operate faster and more efficiently.

The impact of Quantum Computing on cybersecurity can be focused on cryptography, where there is already a need to work with post-quantum cryptography.

3.2. Artificial Intelligence (AI)

Artificial intelligence is a field of computer science that emerged in the mid-1950s, studying systems capable of perceiving their environment and taking actions to maximize their chances of achieving their objectives. Within this field, there is a subfield called Machine Learning, which proposes that machines can recognize patterns through the analysis of historical data. They use these patterns as examples to parameterize their models and once applied, their results are similar to what happened. Based on this, it is possible to automate decisions based on the defined pattern.

The impact of Artificial Intelligence on cybersecurity can be focused on pattern recognition. Through this, it is possible to classify objects, detect anomalies, and predict user behavior.

3.3. Web 3.0 (Blockchain and Metaverse)

Web 3.0 refers to the computer network where machines and humans are connected to process data and generate content quickly and easily. It relies on data analysis, accessible and intelligent machines, and decentralized services using blockchain technology and peer-to-peer (P2P) networks.

The impact of Web 3.0 on cybersecurity lies in its ability to ensure greater privacy and security while maintaining a personalized experience. More specifically, applications based on Blockchain should meet minimum security criteria before going into production. Regulatory policies and procedures should also be established to address vulnerabilities, ensuring the protection of end-users.

[1] https://es.wikipedia.org/wiki/Peer-to-peer

3.4. Cyberphysics Systems: Industrial Internet of Things (IIoT), IoT (Internet of Things)

Cyber-physical systems integrate processing, storage, and communication capabilities to monitor and possibly control physical variables in the environment. These systems form the foundation of the Internet of Things (IoT)[2] and the Industrial Internet of Things (IIoT)[3], where electronic devices communicate with objects, people, or other Internet-connected devices. When it involves automatic communication of data related to individuals, such as through wearable devices, it is referred to as the Internet of Everything (IoE)[4].

The impact on cybersecurity of cyber-physical systems, especially IoT and its derivatives, can be focused on communication security and data integrity transmitted through the network of devices. As this data may be related to sensitive information, the hijacking of devices could directly and critically impact the affected process, which becomes particularly relevant in industrial environments.

3.5. Industry 4.0 and Cloud platforms (CP)

Industry 4.0 refers to the integration of new digital technologies in industrial production processes. It involves the use of computer systems and various types of sensors to improve business efficiency and gain greater control. These technologies are based on the integration of more advanced processes in production facilities, including Big Data, Cloud Computing, Robotics, the Internet of Things (IoT), and Augmented Reality.

In this context of the integration of digital technologies into organizational production processes, cybersecurity becomes increasingly important.

3.6. Neurotechnology

Neurotechnology refers to technologies focused on understanding the functioning of the human nervous system, especially the brain. These technologies enable the visualization of internal processes and the alteration, control, repair, or improvement of brain functions. Neurotechnology utilizes other technologies such as Artificial Intelligence and sensors.

While there have been technologies in this field for decades, the increasing development and interest in these technologies have generated controversies regarding the possibility of altering systems to control humans.

[2] https://es.wikipedia.org/wiki/Internet_de_las_cosas
[3] https://en.wikipedia.org/wiki/Industrial_internet_of_things
[4] https://www.computerweekly.com/es/definicion/Internet-de-todo-IoE

3.7. Human Capital to identify risks and implement changes. Timely regulation. Training.

Human capital is crucial for fostering a cultural revolution that places people at the center. It is necessary to begin with the improvement and professionalization of the human team to enhance their approach and stay up-to-date. This must go hand in hand with identifying new required professional skills and redesigning work models.

4. PROPOSAL

4.1. Methodology to structure cybersecurity guidelines and manage innovations

How to address new challenges (framework). Considering that the implementation of emerging technologies in a business or industry often involves investments that can have a profound impact, and given that not all emerging technologies endure over time, it is necessary to first analyze their impact, relevance, and potential.

To analyze the potential of a specific emerging technology, it is suggested to reidentify the problem that the technology aims to address, as innovation often changes the perspective from which the problem is viewed. Additionally, while it is possible to project the advancement of technology over time, to maintain its potential for real-world application, the technical feasibility of implementing solutions based on that emerging technology should be considered, taking into account available resources and current technological progress.

A framework can be understood as a reusable design, including models and/or code, which can be specialized and expanded to provide a part of the general functionality of many applications (ISO/IEC/IEEE, 2010). For this work, a framework is defined as a reusable design composed of a methodological analysis

4.2. Methodology for Managing Innovations

Based on the reviewed literature and the context described above, the following methodological proposal of a framework for managing innovations based on emerging technologies in the field of cybersecurity is presented.

The objectives of the methodology are as follows:

1. Generate a standardized process that allows for the adoption of emerging technologies.
2. Identify and validate emerging technologies.
3. Appropriation of the emerging technology.
4. Build capabilities in the country to address cybersecurity threats and attacks.

The proposed methodological approach can start by answering the following questions:

***Why? This question would be associated with the organization's needs that motivate the use of new technologies.**

***What should be considered when implementing emerging technologies once their purpose of use is clear?**

***How do adopt and make use of emerging technologies by leveraging the capabilities, architecture, and structure of organizations seeking to implement these technologies?**

The following stages are proposed for implementation:

1. Generate Strategies: Develop strategies that lead to the implementation of the emerging technology.

Emerging technologies will fulfill their mission when the implementation driver is aligned with an objective, problem, or need of the organization.

a. Analyze the emerging technology to be implemented. Analyze which objectives could be supported by emerging technologies, and which problems have not been solved with classical/traditional technologies.

b. Analyze the internal/external environment of the organization and the current regulations.

c. Categorization Process: Identify the domain/categories with which it will be related.

d. Review its maturity level through the Technology Readiness Levels (TRLs) methodology.

e. Identification of use cases: Identifying use cases will facilitate understanding of the new technologies, in the sense that they will be compiled based on their applicability rather than technical language. Identifying and prioritizing the correct use cases will help deliver maximum value in their implementation.

f. Identification of companies that can provide emerging technology: It is suggested that efforts be made to develop local capacity.

g. Viability verification: Verify the benefits to be achieved versus the efforts required to implement the emerging technology. Additionally, the viability verification is related to the maturity level of the emerging technology, the use cases it should cover, and the associated risks.

2. Design:

a. Establish prerequisites for implementing the emerging technology: Determine the enablers for conducting pilot tests and the necessary capacities for conducting such tests, such as trained human resources, identification of partners, and required environments for conducting the tests, among others.

b. Analyze the organization's current state concerning this technology and its requirements.

c. Schedule and develop a pilot.

3. Install:

a. Establish the architecture, enabling the necessary capacities for its implementation, such as the innovation process, user experiences, risks, and required human talent, among other aspects.

b. Governance: Establish an effective governance model that will help maintain and/or update the innovations generated through the use of emerging technologies.

4. Implement:

a. Test the established governance framework and designed solutions.

b. Monitoring, maintenance, and control: Measure the results of the implementation of the emerging technology, provide feedback to the process, and make changes/ adjustments when required.

Summary of Functions

Stages	Strategies	Operationalization
Generate Strategies	- Analysis of the emerging technology - Viability verification	- Categorization - Maturity level - Identification of use cases
Design	- Prerequisites - Environmental analysis	-Pilot
Install	- Architecture - Governance	
Implement		- Test -Monitoring, maintenance, and control

5. CONCLUSIONS

The high level of digitization that exists today, along with the continuous proliferation of new technologies, generates significant vulnerabilities in systems, which are exploited by cybercriminals to carry out attacks aimed at disrupting services, stealing or hijacking stored information, or identity theft, among others. These attacks result in serious losses in all sectors, breaches of confidential information, and/or significant impacts on a country's security.

Cybercrime grows as cybercriminals quickly adopt new technologies, there is a constant increase in online users, it is easier to commit cybercrimes, and cybercriminals become more sophisticated in monetizing their crimes.

Cybersecurity, as an emerging interdisciplinary discipline, requires contextualization and a push to open up to different perspectives and knowledge related to other disciplines such as political science, economics, law, biological sciences, and medicine to characterize a common good with a cross-cutting vision and global implications (Ramírez, 2017).

This will require the development of an interdisciplinary approach that recognizes the limits of disciplines, experiences, and previous knowledge to address an emerging, complex, and uncertain reality. It is necessary to explore the new circumstances posed by the new digital scenario and build proposals that can respond to the new challenges.

In this sense, global trends illustrate how connectivity will enable possibilities while also presenting new threats that go beyond traditional standards and good security and control practices.

Consequently, the development of a cybersecurity culture and its regulation must be a priority to contain and act upon cybercrimes and, on the other hand, adopt emerging technologies that promote national security and defense across different sectors.

Bibliography

Baiardi F, Sgandurra S (2013) Assessing ICT risk through a Monte Carlo method. Environ Syst Decis. doi:10.1007/s10669-013-9463-4.

Cam H, Mouallem P (2013) Mission assurance policy and risk management in cybersecurity. Environ Syst Decis. doi:10.1007/s10669-013-9468-z.

Cavelty D.M. y Wenger A. (2022). Cyber Security Politics Socio-Technological Transformations and Political Fragmentation. 1 Edition. New York, NY: Routledge.

Ezell B, Robinson EM, Foytik P, Jordan C, Flanagan D (2013) Cyber risk to transportation industrial control systems and traffic signal controllers. Environ Syst Decis. doi:10.1007/s10669-013-9481-2.

Gilmore ET, Frazier PD, Collins IJ II, Reid W, Chouikha MF (2013) Infrared analysis for counterfeit electronic parts detection and supply chain validation. Environ Syst Decis. doi:10.1007/s10669-013-9482-1.
Henry Jiang, 2021, The map of cybersecurity domains.

Kelic A, Collier ZAC, Brown C, Beyeler WE, Outkin AV, Vargas VN, Ehlen MA, Judson C, Zaidi A, Leung B, Linkov I (2013) Decision framework for evaluating the macroeconomic risks and
policy impacts of cyber attacks. Environ Syst Decis. doi:10. 1007/s10669-013-9479-9

Lambert JH, Keisler JM, Wheeler WE, Collier ZA, Linkov I (2013). Multiscale approach to the security of hardware supply chains for energy systems. Environ Syst Decis 33(3):326–334

Linkov I, Eisenberg DA, Plourde K, Seager TP, Allen J, Kott A (2013). Resilience metrics for cyber systems. Environ Syst Decis 33(4). doi:10.1007/s10669-013-9485-y

Pawlak P, Wendling C (2013) Trends in cyberspace: can governments keep up? Environ Syst Decis. doi:10.1007/s10669-013-9470-5

National Cybersecurity Center of New Zealand. (2016). Unclassified Cyber Threat Report. Retrieved from: https://www .ncsc .govt .nz /assets /NCSC -Documents /NCSC -2016 -17 -Unclassified -Cyber -Threat -Report .pdf

National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Versión 1.1 - 2018.

Ramírez, R. (2017). Making cyber security interdisciplinary: recommendations for a novel curriculum and terminology harmonization. (Master Thesis) Massachusetts Institute of Technology, School of Engineering, Institute for Data Systems, and Society, Technology and Policy Program.Recuperado de: https://dspace.mit.edu/ndle/17.1/111132.

Rosoff H, Cui J, John RS (2013) Heuristics and biases in cyber security dilemmas. Environ Syst Decis. doi:10.1007/s10669-013-9473-2

Sheppard B, Crannell M, Moulton J (2013) Cyber first aid: proactive risk management and decision-making. Environ Syst Decis. doi:10.1007/s10669-013-9474-1

Vaishnav C, Choucri N, Clark D (2013) Cyber international relations as an integrated system. Environ Syst Decis. doi:10.1007/s10669-013-9480-3.

Zachary A. Collier • Igor Linkov • James H. Lambert (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions. Springer Science+Business Media New York (outside the USA).

*Chapter 5_*

Essential Services Operators

PARTICIPANTS IN THE ELABORATION OF THIS TEXT:

- Coordinating team of the working group "Essential Services Operators": Eduardo Morales and Igor Carrasco

-Technical Working Committee of the working group "Essential Services Operators" convened by the Committee: Patricio Leyton, Igal Neiman, Fernando Muñoz, Juan Huechucura, Marcelo Wong, Mauricio Cartergiani, Carlos Fuentes, Jorge Rojas, Pamela Calisto, Cristian Rojas, Paz Suarez, and Freddy Macho.

1. INTRODUCTION

We understand that an essential service is one whose disruption or interruption has a disruptive impact on the normal functioning of national defense, society, or the economy, and that is an integral part of what we call Critical Infrastructure.

The provision of the service depends on networks and information systems, and a cybersecurity incident would have a disruptive impact on its provision.

The impact of disruption must consider the following factors: potentially affected users, interdependence with other services of equal importance, impact on life, integrity, or health of individuals, impact on economic activity, geographical extent, and importance of the service.

The concept of Critical Infrastructure (CI) not only encompasses physical or material aspects but also includes communication equipment and information systems, in other words, what we commonly refer to as the virtual aspect. A critical infrastructure may or may not include Essential Services (EESS), depending on its function or purpose. For example, a pedestrian bridge may only qualify as a CI, while an airport has extensive physical infrastructure but requires a complementary set of essential operators to be operational.

During more than 15 plenary and thematic working meetings held between August 15th and November 20th, 2022, a team composed of professionals from diverse backgrounds including lawyers, engineers, journalists, entrepreneurs, academics, police officers, and military personnel achieved the outcome reflected in this chapter. Concepts and examples obtained from policies implemented by other countries are gathered here. The ultimate purpose is to structure a policy that promotes collaboration between the public and private sectors.

2. CONTEXT IN CHILE

The widespread use of the Internet, Information and Communication Technologies (ICTs), and the Internet of Things have become prevalent in both public and private organizations worldwide. Their implementation has even reached the infrastructures supporting essential services of countries to improve their productivity and efficiency, following the trend of Industry 4.0 and the Digital Transformation that is permeating all sectors of the economy and society.

Thus, today's critical infrastructures become much more vulnerable than before due to the increased attack surface resulting from the digitized devices and systems that are part of Critical Infrastructures, which possess unpredictable vulnerabilities and potential threats. Additionally, the protection and governance of critical operational data and personal data, which many Critical Infrastructures possess, currently have a low maturity in data management.

If we analyze the high number of attacks on both physical and virtual infrastructure associated with cyberspace globally, we can identify at least three main underlying reasons or root causes: Money, Power, and Subversion[5]. It is important to highlight that the groups associated with each root cause are different: Money (Organized Cybercrime), Power (Cyberarmies of countries that do not align with our national vision), and Subversion (Cyberterrorists or Hacktivist Groups). Distinguishing them allows an understanding of the goals pursued by each of these groups, enabling the implementation of appropriate strategies and measures for each case.

According to the latest report developed by the Economic Commission for Latin America and the Caribbean (ECLAC)[6], the cybercrime industry has increased in complexity through the use of Machine Learning and Artificial Intelligence (AI) tools, as well as in volume, through the Malware-as-a-Service (MaaS) market offered on the Deep Web. At the same time, the pandemic has led to an annual increase in total internet traffic and has changed usage habits. Additionally, the region has seen a year-on-year increase in October 2020 of 67% in ransomware attacks, 71% in malware through secure web pages, and 510% in attacks on Internet of Things devices (according to SonicWall, 2020).

This emerging scenario found different countries in the region with varying degrees of maturity in cyber defense, affecting both the private and public sectors.

[5] Plan Director de Ciberseguridad para el Sector Eléctrico 2021-2023, Cigré Chile Septiembre 2020.
[6] Estado de la ciberseguridad en la logística de América Latina y el Caribe, serie Desarrollo Productivo, N° 228 (LC/TS.2021/108).

As an example, the most affected countries in terms of security incidents in logistics companies are Brazil and Chile. Logistics, by the way, is present in all strategic sectors with critical infrastructures and essential service operators.

From the perspective of protecting essential services for the population, it is clear that cybersecurity plays a fundamental role. Behind these essential services, there are critical infrastructures necessary for the economic and social development of countries. These infrastructures currently incorporate cyber-physical systems that connect to cyberspace to enhance their efficiency and productivity, but they also leave us vulnerable, requiring the expansion of our protection efforts.

3. ANALYSIS OF ENVIRONMENT AND STANDARDS IN IICC AND EESS IN CHILE

The implementation of global cybersecurity standards and strategies in critical infrastructure and essential services (IICC and EESS) such as the banking industry, telecommunications, or the electricity generation, transmission, and distribution sector in Chile, helps in preventing and responding to potential threats, vulnerabilities, or cyber incidents. It enables companies to develop a culture of cyber resilience and improve their response efficiency, minimizing the impact on users and organizations that depend on them.

The electrical power industry serves as an important example to highlight some relevant aspects. The management and production of electricity have evolved over the years to meet the ever-growing demand with high levels of availability. This transformation has involved the digitalization of development models, incorporating new technologies and control mechanisms. However, the nature of these technologies has introduced new weaknesses and vulnerabilities that must be properly managed to mitigate risks, as immersion in cyberspace is a common denominator.

These complex systems are often targeted by sophisticated attacks from criminal groups and organizations.

The NERC-CIP (North American Electric Reliability Corporation - Critical Infrastructure Protection) standard is the cybersecurity standard applied by companies in the industry in the United States, Canada, parts of Mexico, and several Latin American countries, including Colombia, Ecuador, Brazil, Chile, and Peru. It aims to establish specific requirements for the security management of IICC and EESS related to the production and management of electrical grids.

The adoption, implementation, and deployment of a standard itself do not solve the complex dynamics in which the actors behind threats and cyberattacks operate. It has been demonstrated that these globalized and organized groups aim to cause damage to the value chain of the electricity industry and destabilize the energy infrastructure of one or more countries.

Best practices and protection standards help establish the foundations on which to install strategies and operational controls that, together and in a systematic manner, progressively improve energy resilience at the national and continental levels.

The national electricity sector has been working for some time to improve the maturity indices of industrial cybersecurity in coordinated entities, adopting international standards such as the NERC CIP and Cybersecurity Incident Notification Protocols, as well as the Continuous Monitoring of a Strategic Cybersecurity Plan and Critical Infrastructure for the Short, Medium, and Long Term in the Electric sector.

By doing so, they have set an example for continuous improvement in security levels, particularly industrial cybersecurity, becoming the obligatory reference for the rest of the industrial sectors, CCII and related EESS.

4. BREACHES AND SECURITY RECOMMENDATIONS IN IICC AND EESS

It becomes evident that the development of cybersecurity shows notable advances in the so-called administrative networks and operational systems before the industrial networks, SCADA (Supervisory Control And Data Acquisition: a concept used to create software for computers that allows controlling and supervising industrial processes remotely), and OT (Operational Technology: operational technology that includes both hardware and software that detects or causes a change through the direct supervision and/or control of industrial equipment, assets, processes, and events). This trend is observed worldwide, where recurrent

cyberattacks and historical compliance requirements for sectors with high exposure to personal data and a high volume of data transactions, such as the financial, retail, and e-commerce sectors, have driven the development of a wide range of solutions.

In contrast, the industrial and IICC sectors have lagged in this matter. While large financial or commercial institutions have made the position of Chief Information Security Officer (CISO) mandatory, this is not necessarily the case in the industrial context. Internalizing cybersecurity within the top management of the industrial and service sectors, both in medium and large companies, has led to the creation of specialized areas and the hiring of specialists, including a Chief Information Security Officer. Initially, their focus lies on administrative networks, and gradually, they incorporate the risks specific to industrial cybersecurity, which include vulnerabilities in online machinery, SCADA systems, Internet of Things (IoT), and robotics, among others.

With increasing interconnectivity, it becomes increasingly difficult to conceive isolated operations as a significant number of equipment and systems have communication and processing capabilities to facilitate continuous functioning. However, this interconnectivity also represents a vector for possible cyberattacks that can disrupt operations for indefinite periods, ranging from hours to days or even weeks, as seen in cases like Norsk Hydro[7] and Mondelez[8], causing damages worth over $100 million. Industrial equipment can even come "infected" from the factory of origin, akin to the "Trojan horse" concept, and once installed in an industrial or critical infrastructure plant, it can propagate across the entire operation, as seen with the uranium centrifuges in Iran.

Some IICC and EESS organizations have established operational policies aimed at separating their industrial networks from administrative networks to prevent or mitigate the spread of potential cyberattacks and their operational effects. Unfortunately, cybersecurity solutions for OT networks are relatively unknown and undeveloped, creating gaps in their effective incorporation.

[7] https://ics-cert.kaspersky.com/publications/news/2019/03/22/metallurgical-giant-norsk-hydro-attacked-by-encrypting-malware/

[8] https://www.leonoticias.com/comarcas/ciberataque-nivel-internacional-20170627190313-nthtml?ref=https%3A%2F%2Fwww.google.es

Moreover, the level of cyberculture, cybersecurity awareness, and knowledge about the potential impacts of cyberattacks in our country is relatively low. It is noteworthy that Chile ranks among the countries with the highest per capita phishing attacks globally[9], with reports indicating that more than 2 out of 10 Chileans have been victims of phishing within a year.

International experience, reflected in multiple publications on cybersecurity, points out that companies and institutions have sought ways to improve their standards and maturity levels in cybersecurity usually after one of these three events occurs:

i) the institution itself suffers a cyberattack,

ii) a similar institution or known individuals suffer a cyberattack,

iii) the regulator demands it.

Especially in this last case, the reaction has been to promote internal cybersecurity programs to "at least" comply with regulatory requirements. However, many still see cybersecurity as an expense rather than an investment that not only protects their assets but also defends against potential reputational damage.

Other countries with higher levels of cybersecurity, such as Israel and Spain, have approached the issue with a dual focus on both compliance with standards and a risk matrix. They identify specific situations that can affect the cybersecurity of IICC and EESS, as well as mitigating measures involving people, processes, and technologies. This allows for a narrowing of both the probability of occurrence and the undesired effects of a potential attack. This approach has the advantage of focusing on the use of resources since achieving total invulnerability of systems is impossible.

The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has published a set of best practices for cybersecurity in Industrial Control Systems (ICS). These practices are recognized as important for supporting the security of IICC and EESS and maintaining national security[10].

[9] https://diario.uach.cl/chile-es-el-cuarto-pais-de-america-latina-con-mas-intentos-de-ciberataques-por-mensajes-fraudulentos/

[10] https://www.cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems

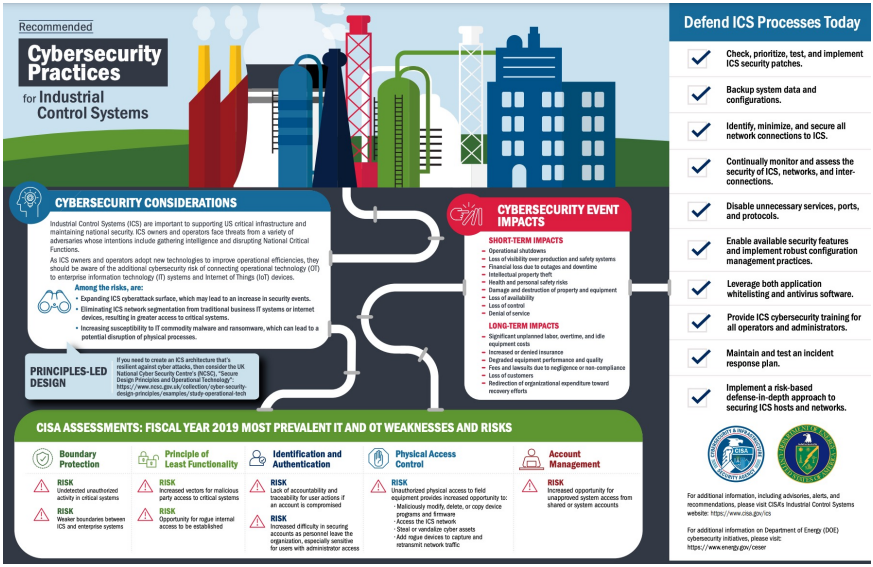


Figure 1: Cybersecurity Practices for Industrial Control Systems

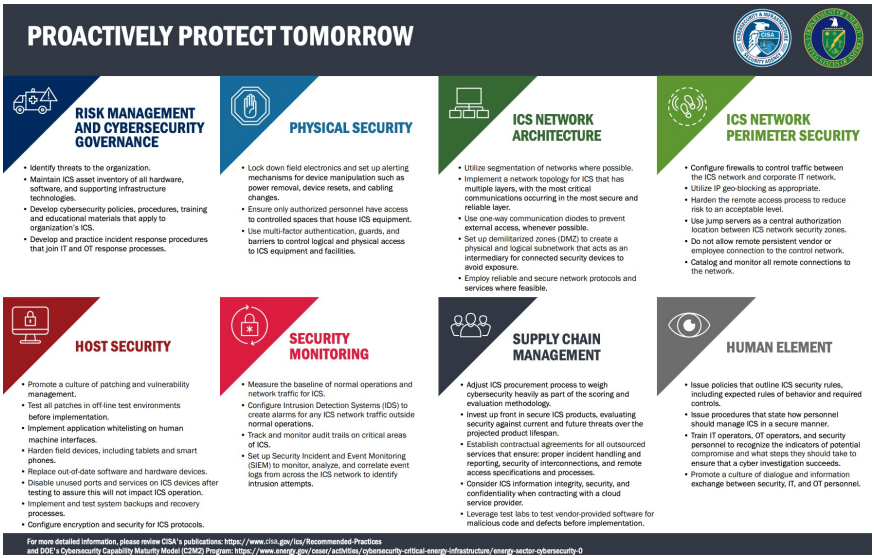


Figure 2: Recommendations for the Protection of Industrial Control Systems

5. DEFINITIONS AND PROPOSAL OF STRATEGIC SECTORS

Below are some definitions and proposals based on Spanish Law 8/2011 (April 28)[11], which establishes measures for the protection of critical infrastructure:

*** Essential Service (EESS): The necessary service for maintaining basic social functions, population health, safety, social well-being, and economic development of citizens, delivered by public or private entities.**

***Strategic Sector: Each of the differentiated areas within the country's labor, economic, and productive activity provides an essential service or guarantees the exercise of state authority or national security.**

The following are proposed as 14 basic strategic sectors:

- → **Energy**
- → **Telecommunications**
- → **Water**
- → **Public Administration**
- → **Health and Emergency Services**
- → **Financial**
- → **Transportation**
- → **Critical Industry**
- → **Food**
- → **Education**
- → **Research Facilities**
- → **Technological Organizations**
- → **Chemical Industry**
- → **Commercial Installations**

Additionally, 2 special strategic sectors are considered due to their special regulations and future development:

- → **Defense and Public Security**
- → **Space**

[11] Disponible en: https://www.boe.es/eli/es/l/2011/04/28/8

***Critical Infrastructures:** These are infrastructures composed of physical facilities, networks, clouds, IT technologies and/or Operational Technologies (OT), Industrial Control Systems (ICS), and Internet of Things (IoT/IIoT) devices. They support the operation of essential services and their functioning is indispensable with no alternative solutions. Disruption or destruction would have a serious impact on essential services.

***Risk Analysis:** The study of possible threat hypotheses necessary to determine and evaluate existing vulnerabilities in different strategic sectors and the possible repercussions of disrupting or destroying the supporting infrastructures. It is usually presented in the form of a Risk Matrix.

***Critical Zone:** A continuous geographic area where multiple critical infrastructures are established under different and interdependent operators, declared as such by the competent authority. Declaring a critical zone aims to facilitate better protection and coordination among the different operators of critical infrastructures (public or private) located within a limited geographical area, as well as with the State Security Forces and Police.

***Criticality Criteria:** Parameters used to determine the criticality, severity, and consequences of disrupting or destroying a critical infrastructure are evaluated based on:

1. **The number of affected people is assessed by the potential number of deaths or severe injuries and the consequences for public health.**

2. **Economic impact is based on the magnitude of economic losses and the deterioration of products and services.**

3. **Environmental impact, degradation on-site and in the surrounding areas.**

4. **Public, reputational, and social impact due to the influence on public trust in the capacity of Public Administration, physical suffering, and disruption of daily life, including the loss and severe deterioration of essential services**.

SECURITY LEVEL: Defined in a National Plan for the Protection of Critical Infrastructures, under the overall threat assessment and the specific evaluation of each infrastructure. It determines the concrete degree of intervention by different responsible entities in terms of security.

INTERDEPENDENCIES: The effects that a disruption in the operation of an installation or service would have on other installations or services, distinguishing between repercussions within the same sector and in other sectors, as well as local, national, or international repercussions.

PROTECTION OF CRITICAL INFRASTRUCTURES: The set of activities aimed at ensuring the functionality, continuity, and integrity of critical infrastructures to prevent, mitigate, and neutralize the damage caused by a deliberate attack against such infrastructures. It also ensures the integration of these actions with other responsible subjects within their respective competencies.

SENSITIVE INFORMATION ON THE PROTECTION OF CRITICAL INFRASTRUCTURES: Specific data about critical infrastructures that, if revealed, could be used to plan and carry out actions aiming to disrupt or destroy them.

CRITICAL OPERATORS OR ESSENTIAL SERVICE OPERATORS: Entities or organizations responsible for investments or daily operation of critical infrastructures, whether public or private.

TECHNOLOGICAL ORGANIZATIONS: Companies that provide support and outsourcing management for critical infrastructures at the level of their IT systems, clouds, and networks in the fields of Information Technology (IT), Operational Technologies (OT), Industrial Control Systems (ICS), and Internet of Things (IoT/IIoT) devices. (These providers are not responsible for the security of essential services but are required to promptly alert, inform, and report any cybersecurity threats, entailing the need for a robust early warning system for cybersecurity incidents as part of regulations.)

NATIONAL CATALOG OF CRITICAL INFRASTRUCTURES AND ESSENTIAL SERVICES: The comprehensive, up-to-date, verified, and computerized information on the specific characteristics of each existing critical infrastructure in the national territory. It is maintained and managed confidentially by the competent authority.

6. MAIN PROPOSED STRATEGIC GUIDELINES

A future National Policy or Strategy for Critical Infrastructures and Essential Services should consider the following strategic guidelines:

1. CYBER RESILIENCE: The country should possess resilient critical infrastructure, both physical and virtual, prepared to identify, protect, detect, anticipate, respond, mitigate, and recover from cybersecurity incidents. This should be achieved through a risk management and information security-focused approach.

2. CULTURE AND AWARENESS: It is imperative to develop and establish a Culture of Protection for our Critical Infrastructures and Essential Services at a national level, to raise awareness among citizens. This culture should be an integral part of the ongoing management of each critical service operator through the adoption of best practices, international standards, sector-specific training, competency accreditation, and periodic campaigns promoting individual and collective responsibility.

3. SECTORIAL CSIRTS: Establish Sectorial Computer Security Incident Response Teams (CSIRTs) according to the cybersecurity framework law. These teams should closely coordinate with the National CSIRT, which will be part of the National Cybersecurity Agency, to handle issues such as early alerts, tracking, and joint response to cyber incidents.

4. GOVERNANCE: Establish an Organizational Structure for the Protection of Critical Infrastructures to ensure governance and compliance with sector-specific protection plans and programs. This structure should also facilitate coordination, communication, and planning for security incidents that could compromise our national critical infrastructure while maintaining a National Catalog of Critical Infrastructures and Essential Services.

5. SECTORIAL REGULATIONS: Define and create specific Sectorial Plans and Programs for each critical sector based on a National Policy for Critical Infrastructures and Essential Services. Disseminate and promote the adoption of standards.

(Note: Points 3, 4, and 5 are addressed in the processing of the Cybersecurity Framework Law (Bill 14,847-06), currently in the legislative process).

6. CYBER EXERCISES: Develop and participate in National (multi-sectoral) and International Cyber Exercises to assess the cyber resilience of Critical Infrastructures and Essential Services. These exercises should also improve the capacity and expertise of specialized human resources within critical service operators.

7. CRITICAL INFRASTRUCTURE PROTECTION MONTH: Establish a national month focused on Critical Infrastructures and Essential Services, as done in other countries. The aim is to promote awareness of their importance and coordinate activities such as simulations and assessments of multisectoral failure effects.

8. MATURITY MEASUREMENT: Annually measure the progress and evolution of cybersecurity maturity in the country according to standards such as the Oxford Cybersecurity Maturity Model for Nations (CMM). This will help identify gaps and develop action plans for improvements in each sector.

9. TALENT MANAGEMENT: Foster training, education, innovation, and the development of new talent in universities, public and private organizations, and those responsible for critical infrastructures. This can be achieved through a National Cybersecurity Institute with international and national partnerships for capacity development in the protection of Critical Infrastructures and Essential Services.

10. PARTNERSHIPS AND COOPERATION: Establish and promote national and international alliances and cooperation with government agencies, research centers, universities, and cyber incident response teams, among others. These partnerships will facilitate knowledge transfer, training, and certifications, both globally and within specific sectors, to enhance national defense capabilities.

7. PROPOSED INITIATIVES

Proposing a roadmap for Critical Infrastructure Protection helps align cross-cutting and multisectoral efforts on the subject. This perspective captures the sense of urgency in implementing short-medium-long-term measures.

Taking a holistic approach, a set of initiatives are proposed, some of which are overarching and go beyond Critical Infrastructures and others that specifically address strategic sectors.

These initiatives align with each of the 9 proposed strategic guidelines for the Protection of Critical Infrastructures and Essential Services. Initiatives marked with (*) are considered of high strategic priority:

1) GOVERNANCE

Short-term actions

→ Establishment of a National Policy for Cyber Protection of Critical Infrastructures and Essential Services.
→ Creation of a National Cybersecurity Agency.
→ Establishment of the National CSIRT (Computer Security Incident Response Team) under the National Security Agency.
→ Creation of the National Agency for Personal Data Protection.
→ Obligation to report incidents that compromise Critical Infrastructures and/or Essential Services, with an impact on the population.
→ Establishment of a legal framework to sanction those who attack Critical Infrastructures or Essential Services through digital means, as well as those responsible for negligent actions (deliberate or through omission) within institutions that result in cyber-attacks.

Medium-term actions

→ (*) Creation of a National Center for Critical Infrastructure Protection or a related entity.
→ Critical Infrastructure and Essential Service operators must implement ISMS (Information Security Management Systems) that incorporate Industrial Cybersecurity into their critical processes.
→ Alignment of Industrial Security with internationally recognized standards, such as IEC 62443 (Security for Industrial Automation and Control Systems), as a baseline for secure designs.
→ Creation of a National Cybersecurity Institute aimed at promoting cybersecurity, guiding research, and developing human talent in the field.

Long-term actions

→ Establishment of a National Cybersecurity and Cyber Defense Office (similar to Senapred) to coordinate responses to incidents that affect the country due to cyber-attacks on Critical Infrastructures and Essential Services.

2) CYBER RESILIENCE

Short-term actions

→ Development and dissemination of a Risk Assessment Methodology with a focus on Critical Infrastructure and Essential Services Protection, under the supervision of the National Cybersecurity Agency in collaboration with leading experts in the field, aligned with a National Policy for the Protection of Critical Infrastructures and Essential Services.

Medium-term actions

→ Establishment of a national catalog of Critical Infrastructures and Essential Services based on criteria and standards set by the competent authority. This will enable the authority to establish interdependence maps (domino effect management) and enforce Cybersecurity Incident Management and Response Plans.

Long-term actions

→ Automated risk and impact assessment plan leveraging AI (Artificial Intelligence) tools to enhance decision-making in response to various scenarios that may arise from a cyber-attack.

3) SECTORIAL REGULATIONS

Short-term actions

→ Promulgation of regulations, guidelines, and directives for sector-specific best practices, led by the National Cybersecurity Agency.

→ Mandatory requirement for all Critical Infrastructures and Essential Services to have a registered Cybersecurity Officer (CISO) who interacts with the National Cybersecurity Agency and sectorial CSIRTs. Establishment of a national registry of responsible individuals.

→ Establishment of sanctioning frameworks for non-compliance with cybersecurity regulations.

Medium-term actions

→ Development of sector-specific cybersecurity plans and programs aligned with a National Policy for Critical Infrastructures and Essential Services.

→ Implementation of standardized certifications for regulatory compliance.

Long-term actions

→ Establishment of sector-specific regulations and norms for the Protection of Critical Infrastructures and Essential Services (including Cybersecurity and Data Protection), under the responsibility of the National Cybersecurity Agency.

4) SECTORIAL CSIRTS

Short-term actions

→ Strategic planning (budget, design, staffing, training) for the defined sectorial CSIRTs, with support from the National Cybersecurity Agency through the National CSIRT.

Medium-term actions

→ (*) Establishment of Strategic CSIRTs.
→ Strategic sectors that cannot have their own sectorial CSIRT will be subordinate to the National CSIRT.

5) PARTNERSHIPS AND COOPERATION

Short-term actions

→ Establish collaboration alliances between strategic sectors, the National CSIRT, Defense CSIRT, Police Investigative Unit, and Cybercrime units, as well as research centers in cybersecurity and cyber intelligence.

→ Foster public-private cooperation alliances to support the development of policies for the digital security of interdependent Critical Infrastructures and Essential Services.

Medium-term actions

→ Partnerships and cooperation between sectorial CSIRTs and regional and international centers for Critical Infrastructure Protection (such as Spain, Estonia, the United Kingdom, and the United States).

Long-term actions

→ Alliances and cooperation with the National CSIRT and Defense CSIRT to establish protection elements in cyber warfare scenarios.

6) CYBER EXERCISES

Short-Term Actions

→ Organize National Cybersecurity Exercises in the public, private, academic, and defense sectors, targeting critical information infrastructure and sensitive systems to enhance human capabilities and improve resilience.

Medium-Term Actions

→ Conduct International Cyber Exercises with Regional Allies.

Long-Term Actions

→ Engage in International Cyber Exercises with international organizations and allies.

7) MATURITY MEASUREMENT

Short-Term Actions

→ Measure Cybersecurity Maturity Levels to assess initial gaps and define Key Performance Indicators (KPIs), under the leadership of the National Cybersecurity Agency.

Medium-Term Actions

→ Conduct Annual Measurement of Cybersecurity Maturity Levels, based on the University of Oxford's Model (CMM), and take actions to improve performance and reduce gaps.

Long-Term Actions

→ Continuously monitor sector-specific management indices to maintain and improve cybersecurity maturity.

8) TALENT MANAGEMENT

Short-Term Actions

→ Develop and promote a Curriculum for operators in critical information infrastructure and sensitive systems, inspired by programs such as the SANS Institute, and National Initiative for Cybersecurity Education (NICE), among others, supported by the National Cybersecurity Agency and the National Institute of Cybersecurity (yet to be established).

Medium-Term Actions

→ Coordinate through the National Institute of Cybersecurity to establish educational programs for careers, specializations, diplomas, and other related subjects in cybersecurity, including a Master's in IICC protection.

→ Establish recognized certifications and accreditations for cybersecurity specialists (accreditation processes).

Long-Term Actions

→ Establish Research and Development activities in cybersecurity products and solutions, personal data protection, and cyber intelligence as a national development hub.

9) CULTURE AND AWARENESS

Short-Term Actions

→ Propose a Law declaring November as the National Month of Critical Information Infrastructure and Sensitive Systems, complementing Cybersecurity Month.

Medium-Term Actions

→ Educate and create awareness about cybersecurity at an early age, with a focus on cyber hygiene for proper behavior and data protection in cyberspace, emphasizing the care of our Critical Information Infrastructure and Sensitive Systems.

Long-Term Actions

→ Conduct ongoing cybersecurity promotion campaigns targeting the public and private sectors, as well as within organizations related to the protection of our Critical Information Infrastructure and Sensitive Systems.

Additionally, the following sector-specific initiatives are proposed to reinforce the protection of Critical Information Infrastructure and Sensitive Systems, recognizing that industries such as banking and telecommunications are heavily regulated by their sector authorities regarding cybersecurity. These initiatives serve as a reference for other sectors that need to further develop their cybersecurity maturity in the future.

Operational tactical sector initiatives for the Water Sector:

1) Governance

Short-Term Actions

→Have Cybersecurity Officers with competence and accreditation.

Medium-Term Actions

→Design policies, roles, and access profiles for OT-IoT-IIoT environments.

Long-Term Actions

→Evaluate and develop risk treatment plans in industrial cybersecurity.

2) Cyber Resilience

Short-Term Actions

→Securitization and hardening policies for OT-IoT-IIoT operational computers.
→Privileged user management.
→Implement perimeter protection controls.

Medium-Term Actions

→Securitization and hardening policies for OT-IoT-IIoT operational computers.
→Privileged user management.
→Implement segregation of OT-IoT-IIoT environments.

Long-Term Actions

→Apply controls on peripherals (USB blocking, solidification of operational computers) as alternatives.
→Dedicated Active Directory for OT-IoT-IIoT environments.

3) Sector-specific regulations

Short-Term and Medium-Term Actions

→ISA 95 - ISO 27001.

Long-Term Actions

→IEC 62443.

4) Sectoral CSIRT (Computer Security Incident Response Team)

Medium-Term Actions

→Establish a sectoral CSIRT for the Water industry.

5) Alliances and Cooperation

Medium-Term Actions

→Collaboration with organizations in the same sector. Coordinate with the National CSIRT.

6) Cyber Exercises

Medium-Term Actions

→ Develop Business Continuity Plans, Regulatory Impact Analysis (RIA), and Business Impact Analysis (BIA) for OT-IoT environments as part of sector-specific regulations.

7) Maturity Measurement

Medium-Term Actions

→ Audits and vulnerability reviews.

Long-Term Actions

→ Apply Cyberintelligence tools.

8) Talent Management

Medium-Term Actions

→ Form a sector-specific cybersecurity team regarding industrial cybersecurity threats and vulnerabilities.

9) Culture and Awareness

Short-Term Actions

→Develop a training and cyber-education plan for Industrial Cybersecurity.

Medium-Term Actions

→Provide talks and training on industrial cybersecurity for operations personnel in OT-IoT-IIoT environments.

Long-Term Actions

→Evaluate and monitor the effectiveness of culture and awareness in industrial cybersecurity.

Operational Tactical Sectorial Initiatives for the Critical Industry Sector

1) Governance

Short-Term Actions

→Define specific sub-sectors and thresholds for high, medium, and low risk of Critical Industry Operators (based on size and potential impact on society and the economy).

Medium-Term Actions

→Define mechanisms for interaction between Critical Industry Operators and the National Cybersecurity Agency.

Long-Term Actions

→Define mechanisms for interaction between Critical Industry Operators and the National Center for Critical Infrastructure Protection.

2) Cyber Resilience

Short-Term Actions

→Develop an annual self-assessment plan for cybersecurity risks based on predefined guidelines. The results will help maintain up-to-date risk levels.

Long-Term Actions

→Include High-Risk Critical Industry Operators in end-of-day (COB) testing plans for Essential Operators.

3) Sectorial Regulations

Medium-term actions

→Establish regulations and implementation deadlines for Critical Industry Operators based on identified risk levels (high, medium, low).

Long-term actions

→Disseminate and train Critical Industry Operators in agreed methodologies. Implement periodic compliance review processes.

4) Sectorial CSIRTs

→Not applicable

5) Alliances and Cooperation

Medium-term action

→Enhance cooperation and knowledge exchange in cybersecurity with international parent companies or related companies of Critical Industry Operators.

6) Cyber Exercises

Medium-term actions

→Include Critical Industry Operators in sectorial exercises.

Long-term actions

→Consider exercises involving catastrophic failure scenarios for Critical Industry Operators.

7) Maturity Measurement

Short-term actions

→EEstablish cybersecurity maturity levels for Critical Industry Operators based on operator risk levels and set deadlines to achieve desired objectives.

Medium and Long-term actions

→Develop metrics to measure maturity levels and set deadlines for achieving objectives.

8) Talent Management

Short-term actions

→Define requirements for the need or obligation to have an internal or external Chief Information Security Officer (CISO) for High-Risk Critical Operators.

Medium-term actions

→Extend and standardize internal courses provided by the National Center for Critical Infrastructure Protection and Essential Operators to Critical Industry Operators.

Long-term actions

→Define requirements for the need or obligation to have an internal or external Chief Information Security Officer (CISO) for Medium and Low-Risk Critical Operators.

9) Culture and Awareness

Medium and Long-term actions

→Establish cybersecurity awareness programs and evaluate and monitor the effectiveness of cybersecurity culture and awareness.

These proposals consider the existence of cybersecurity and essential services governance based on legislation being processed in parliament, which includes a focus on cybersecurity education and culture, as well as robust and up-to-date data protection legislation.

Furthermore, it is important to reiterate that a regulatory framework for Critical Infrastructure and Essential Services is essential, as it allows the creation of sectorial CSIRTs, critical infrastructure catalogs, and the measurement of cybersecurity management maturity (creating Key Performance Indicator indices KPI)

8. MAIN CONCLUSIONS AND RECOMMENDATIONS

Cybersecurity is a cross-cutting element for digital transformation, not only for an ecosystem involving companies and their stakeholders but also for all states around the world. Today, states need to defend themselves more than ever against the malicious intent in cyberspace, which is repeatedly impacting public and business activities. This includes cyber warfare, organized crime, hacktivism, and criminal organizations, particularly targeting Critical Infrastructure on which the stability and daily operation of the population depend, such as energy, water, telecommunications, healthcare, finance, and transportation, among others.

The cybersecurity culture is still in its early stages in Chile and has not fully permeated the industry, economy, current legislation, and citizenship of our country. In this scenario, cybersecurity initiatives that involve close collaboration between the public and private sectors are highly valuable, as they help to understand and combine efforts to promote the necessary mechanisms and instruments to ensure both cybersecurity and resilience in the face of disruptions.

Only through these measures can we prevent jeopardizing the integrity and operational continuity of our Critical Infrastructure and essential services. These instruments should be based on a legal, normative, and regulatory framework, which should lead to a **National Cybersecurity Strategy**, understood as a State Policy.

The common goal of this strategy should be to guarantee a secure and reliable use of Chile's cyberspace and protect the rights and freedoms of its citizens, promoting socio-economic progress. Key factors include:

1. Protection of Critical Infrastructure: Promote and encourage a legal framework, similar to that of other countries, which allows defining roles and responsibilities, both public and private. Establish a set of alerts, notifications, and responses to cybersecurity events associated with critical sectors essential for the public.

2. Establish a cybersecurity culture nationwide: Involve academia, industry, the government, and society. According to the Global Risk Report 2022 by the World Economic Forum, 95% of cybersecurity risks are due to human error.[12] For this reason, it is necessary to generate and promote a comprehensive cybersecurity culture that addresses the industry, economy, public sector, and academia. This will help mitigate the risk of potential breaches resulting from human error.

[12] Disponible en: https://www.marsh.com/co/risks/global-risk.html

3. Create the National Cybersecurity Agency: Provide the necessary tools to prevent and combat cybercrimes that occur on the internet. This agency should ensure cybersecurity for Chileans in cyberspace, protect digital assets and society, and coordinate continuously with the private sector to guarantee citizens' security in cyberspace.[12]

4. Establish regulatory frameworks at the sector level: Define duties and responsibilities for each member of a specific sector, providing minimum guidelines for the prevention, response, and resolution of cybersecurity incidents.

5. Certification in cybersecurity for Critical Infrastructure and essential services: All public and private organizations classified as Critical Information Infrastructure should implement and maintain Information Security Risk Management and Business Continuity Management systems certified by industry-validated organizations and academia.

6. Implementation of sectorial CSIRTs: These should respond to cybersecurity incidents that may jeopardize the facilities, networks, systems, platforms, services, and physical and IT equipment of their respective regulated sectors.[13] They should also report and coordinate with the National Cybersecurity Agency.

7. Support for academia and cybersecurity R&D industry at the national level: The legal framework should facilitate agreements between the public, private, academic, and cybersecurity R&D industry sectors. This aims to establish cooperation, knowledge transfer, and research that adds value by providing specific solutions tailored to the country.

8. Supply chain protection: Since many inputs used for production are not handled internally, organizations depend on highly integrated supply chains. It is necessary to regulate critical infrastructure providers with security requirements, both physical and logical, to prevent and address cyber incidents and mitigate potential impacts on service continuity.

[12] https://www.csirt.gob.cl/noticias/presidente-pinera-anuncia-proyecto-de-ley-que-crea-la-agencia-nacional-de-ciberseguridad/

[13] https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06

9. Strategic alliances with other countries: Establish the necessary network of contacts to bring together the public, private, and academic sectors, where interests and knowledge in cybersecurity can be shared. This should also foster education, responsible technology use, and communication channels not only at the national level but also across borders, expanding the knowledge base.

In short, the joint effort of all sectors and organizations, both private and public, as well as the executive and legislative branches, should converge in the future establishment of a **National Policy for Critical Infrastructure.** This policy will establish the foundation for facing risks and threats, originating from both the physical and digital worlds, that could compromise our country's operations.

Given our country's significant development of technological infrastructure, adoption of international standards, and a solid foundation for embracing the necessary Digital Transformation, it is crucial to collaboratively work towards developing the required regulations and norms to enhance necessary protection against threats associated with technological advancements. This will directly benefit our society.

As a proposal, this document will serve as an important reference and input for decision-makers, as it reflects the diverse vision of professionals and specialists who have selflessly worked together, combining multiple perspectives to contribute to national cybersecurity. This contribution will help us maintain our standing as a reference point in the Latin American context.

Additional Information:

PROTECTION OF INFORMATION IN CRITICAL INFRASTRUCTURE

As a reference to promote the protection of information in our Critical Infrastructures and Essential Services, the following outlines some aspects of the USA's PCII program (Protected Critical Infrastructure Information) on how to manage information generated between essential service operators and the competent authority.

The PCII program is part of the National Protection and Programs Directorate (NPPD) of the US Department of Homeland Security (DHS). It aims to protect information and enhance information exchange between the private sector and the government. The Department of Homeland Security and other federal, state, and local analysts use PCII to:

1. **Analyze and secure critical infrastructure and protected systems.**
2. **Identify vulnerabilities and conduct risk assessments.**
3. **Enhance preparedness measures for recovery.**

The PCII originates from the Critical Infrastructure Information Act of 2002 (CII Act) which protects voluntarily shared information regarding the security of private and government critical infrastructure. 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) are established in Title 6 of the Code of Federal Regulations (CFR) Part 29, Final Rule for Critical Infrastructure Information Handling Procedures.

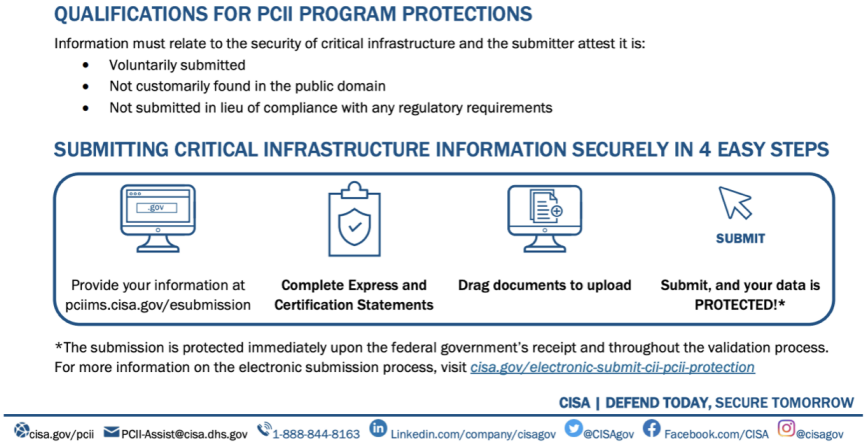
The safeguards or precautions provided by the PCII Program facilitate the voluntary exchange of information between owners of CII and ESOs and the government. These safeguards provide the necessary confidence that ensures that confidential, commercially sensitive, and exclusively owned data will not be disclosed.

The information sent for PCII protection should:

* **Be submitted voluntarily**
* **Not be available in the public domain**
* **Not be submitted in place of complying with any regulatory requirement**

The information submitted will maintain the confidentiality and secrecy safeguards of the PCII, unless the PCII Program Office determines that the information, at the time of submission, was already in the public domain, or the sender requests in writing for the restrictions to be removed.

Below is a summarized overview provided by CISA:



BIBLIOGRAPHY AND REFERENCES

1. Cybersecurity Fundamentals Glossary, ISACA, 2016.
2. Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Revision 2, May 2015.
3. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST, April 16, 2018.
4. Libro Ciberseguridad Industrial e Infraestructuras Críticas, Fernando Sevillano, Ra-Ma Editorial, 2021.
5. Zero Trust Architecture, NIST Special Publication 800-207, August 2020.
6. Guidelines for Planning an Integrated Security Operations Center, EPRI, December 2013.
7. NISTIR 7628 Revision 1, Guidelines for Smart Grid Cybersecurity.
8. Política Nacional de Ciberseguridad, Agosto 2017, Ministerio del Interior, Chile
9. Estándar de Ciberseguridad para el Sector Eléctrico, Publicación Coordinador Eléctrico Nacional, Octubre 2020.
10. Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1 February 2014, DOE-DHS, USA.
11. Plan Director de Ciberseguridad para el Sector Eléctrico 2021 – 2023, Cigré Chile, Agosto 2020.
12. National Energy Security Strategy, July 2015, Presidencia del Gobierno, España.
13. Technical Brochure: Cybersecurity: Future threats and impact on electric power utility organizations and operations, Reference: 796, WG D2.46_CIGRE, March 2020.
14. Technical Brochure: Electric Power Utilities' Cybersecurity for Contingency Operations, Reference: 840, WG D2.50_CIGRE, June 2021.
15. ENISA Report - How to setup up CSIRT and SOC, December 2020.
16. Ten Strategies of a World-Class Cybersecurity Operations Center, MITRE, Carson Zimmerman, 2014.
17. G DATA Whitepaper, El nuevo Reglamento de Protección de Datos de la UE (GDPR) – Lo que las empresas deben saber, Septiembre 2017.
18. Anexo Técnico: Sistemas de Medición, Monitoreo y Control, CNE, Agosto 2019.(
19. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team, September 2016, Homeland Security.
20. ENISA Baseline security recommendations for IoT in the context of Critical Information Infrastructure
21. Blockchain-Government-Transparency-Report.
22. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
23. Gobernanza Digital e Interoperabilidad Gubernamental Cepal
24. Hacia la republica digital en Chile. Inciber.
25. Institucionalidad en ciberseguridad e infraestructura crítica a nivel internacional. Julio 2022 Biblioteca del Congreso Nacional de Chile.
26. Consideraciones de Ciberseguridad el Caribe democrático para del proceso América Latina y el Caribe. OEA.
27. Digital Democracy. The tools transforming political engagement Julie Simon, Theo Bass, Victoria Boelman and Geoff Mulgan.February 2017.

28. Procedimientos administrativos electrónicos Experiencia Extranjera. Biblioteca del Congreso Nacional Mayo 2019
29. Riesgos, avances y el camino a seguir en américa latina y el caribe. reporte ciberseguridad 2020
30. Proyecto Ley Marco de Ciberseguridad.
31. Proyecto de Reforma Constitucional sobre Infraestructura Crítica - Oficio de Ley 12.7.22
32. Política integral de seguridad de la información, ciberseguridad e infraestructura crítica. Coordinador Eléctrico Nacional
33. Risk Assessment Methodology for Critical Infrastructure Protection Georgios Giannopoulos Bogdan Dorneanu Olaf Jonkeren.2013. Comisión Europea
34. Cyber Defense Doctrine Managing the Risk: Full Applied Guide to Organizational Cyber Defense. Cyber Israel National Cyber Directorate
35. Identificación y reporte de incidentes de seguridad para operadores estratégicos. Guía básica de protección de Infraestructuras Críticas. Centro nacional de Infraestructuras Críticas CNPIC
36. Protección de infraestructuras críticas guía para la elaboración de planes de seguridad del operador y planes de protección específica agrupación empresarial innovadora para la seguridad de las redes y los sistemas de información. AEI
37. Seguridad Agrupación empresarial innovadora para la seguridad de las redes y los sistemas de la información
38. Estado de la ciberseguridad en la logística de América Latina y el Caribe . Rodrigo Mariano Díaz Desarrollo Productivo Serie 228. Cepal
39. La protección de infraestructuras críticas y la ciberseguridad industrial. Primera edición: 1 de octubre de 2013 ISBN: 978-84-616-6330-9
40. Estrategia de Transformación Digital 2035
41. Comparativa de estrategias de Ciberseguridad de LATAM
42. California Ocean Plan 2019
43. El ecosistema de I+D+i y la colaboración público-privada en ciberseguridad 4 de julio de 2022 Miguel Ángel Cañada Responsable de Relaciones Institucionales y Estrategia de INCIBE
44. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
45. CISA Strategic Plan 2023-2025
46. https://www2.deloitte.com/ec/es/pages/risk/articles/cyber-risk-2018.html.
47. https://www.cci-es.org/web/cci/detalle-pais/-/journal_content/56/10694/445446.
48. https://resources.infosecinstitute.com/threatmetrix-cybercrime-report-an-interview/.
49. BID (2016), disponible en https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean.
50. https://www.oxfordmartin.ox.ac.uk/cyber-security/.
51. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0.
52. Global Cyber Security Capacity Centre.
53. https://technewstt.com/caribbean-cybersecurity-dev/.
54. https://www.caricom.org/media-center/communications/news-from-the-community/caribbean-nations-sign-off-on-cyber-crime-action-plan.

*Chapter 6_*

National Strategy Against Online Disinformation

PARTICIPANTS IN THE ELABORATION OF THIS TEXT:

- Coordinating team of the working group " National Strategy Against Online Disinformation ": Jorge Gatica and Felix Staicu.

- Technical Working Committee of the working group " National Strategy Against Online Disinformation " convened by the Committee: Ricardo Vásquez, María Paz Ilabaca, Juan Ignacio Nicolossi, Sebastián Carey, Carlos Parker, Jorge Astudillo, Pedro Huichalaf, Victoria Hurtado, y Andrés Barrientos.

1. INTRODUCTION

The explosive growth of information technologies and their widespread accessibility have facilitated communications but have also imposed new challenges. Today, each individual, completely autonomously, has the potential to generate content and, depending on their capabilities, even shape public opinion.

The effects of our relationship and dependence on cyberspace are producing significant changes in society, the full magnitude of which is still being quantified. Concepts such as cyber sociology and cyber psychology have yet to be fully developed to respond effectively to the importance of these changes.

The unquestionable power of information and its potential misuse poses a real danger to individuals and society as a whole. A well-crafted photograph, video, or narrative with defined purposes can dramatically distort reality, manipulate minds, solidify convictions, or destroy the image of an institution, organization, public figure, or citizen.

Manipulating individual, group, or societal thinking is achieved through the dissemination of maliciously distorted information to gain political advantage, such as destabilizing institutions and subverting order. These are forces that generate powerful negative effects on society and democracy.

The speed, virality, and anonymity of social media have exacerbated partisan polarization, hate speech or incitement, mass public humiliation, foreign interference in internal affairs, and the spread of false or mistaken information. Each new information technology reaches more people at a faster pace. Virality, driven by algorithms that amplify intense emotions, especially outrage, leads to errors by conflating popularity with legitimacy. Anonymity, fundamental for freedom of expression, has influenced a deafening and hurtful dialogue that hinders people's understanding and may seriously undermine the negotiation capacity inherent in any democracy.

In the face of advanced disinformation campaigns that exploit human psychological vulnerabilities, the notable algorithms of social media, and actors who constantly perfect the art of deception, societies are extremely vulnerable.

The information explosion and the habituation of individuals to information overload have opened a Pandora's box that has led to the decline of collective critical thinking. Traditional defenses are ineffective against this modern threat. The first step in building a defense is to comprehend the threat and then counter it proactively and reactively.

Information systems built upon the foundations of democracy and freedom of expression have proven vulnerable to external influence operations that use disinformation as a tool. Disinformation can directly affect democratic foundations, and efforts to counter disinformation can undermine freedom of expression. Striking a delicate balance that takes both into account is necessary.

Various tools and actions are needed to address the issue systematically, from diagnosis to implementation of solutions. To achieve this, measures can be categorized based on their focus: prevention, reaction, and effective engagement among stakeholders.

There is no perfect model for combating disinformation since it is a loose and dynamic concept, but one thing is clear: inaction in the face of this phenomenon is not an option due to its severe social consequences. Some countries have developed governance models that respect and reinforce democratic processes, but each one is subject to criticism and can be improved. Lawmakers should learn from the successes and failures of other countries and develop a model that can effectively counter-influence operations, with a medium- to long-term perspective.

In over 50 working meetings held between June 22 and November 30, 2022, a team of 11 professionals with diverse backgrounds, including lawyers, engineers, journalists, businesspeople, academics, and military personnel, achieved the results reflected in this chapter. It brings together concepts and examples from policies implemented by other countries that have made progress in addressing online disinformation. The diagnosis delves into a phenomenon that exploits human psychological vulnerabilities and social divisions, culminating in a proposal for a comprehensive strategy that approaches the problem in a multidimensional and multisectoral manner. The ultimate goal is to establish a social, political, and cultural foundation upon which an effective defense of information can be built, fostering collaboration between the public and private sectors.

2. CONTEXT: THE SCOPE OF THE WORD DISINFORMATION

The practice of disinformation, as such, is an accepted form in the array of tools that an actor possesses for managing conflicts of all kinds (military, social, individual, public or private, etc.). It stems from the application of the principle of deceiving the adversary.

In the 5th century BC, military strategist Sun Tzu wrote in Chapter I of his work "The Art of War" that deception is the essence of conflict and the fundamental principle for manipulating the adversary.

Over time, this principle developed based on the manipulation of individual, group, or social thinking, mainly associated with counterinsurgency during the Cold War in the 20th century. These practices were implemented in numerous wars instigated by the two hegemonic superpowers of the time.

The essentially subversive and clandestine methodology for disseminating disinformation, aimed at destabilizing the social order in countries where the adversary was located, led to the development of modern theory on information manipulation, primarily known as Psychological Operations (PSYOPS). These operations have become one of the preferred destabilization tools used by special operations organizations, often associated with intelligence services.

Thus, the services dedicated to this function, whether military or civilian, subtly implemented disinformation processes to alter the morale and stability of the adversary.

There are various tactics for disinformation, including misinformation, disinformation, and malformation, which will be defined later. It is worth noting that disinformation is a strategy, while fake news is a type of tactic used to generate disinformation, although it is not the only one. The art of disinformation combines a good understanding of psychology, sociology, history, politics, economics, and other relevant concepts to skillfully manipulate and spread narratives that influence how individuals and groups think and make decisions.

If we understand technology and access to it as force multipliers, in digital technologies and their platforms, we find an asymmetric relationship between the costs of disseminating manipulated information and its effect. In other words, there is an economic relationship of low implementation costs and high impact.

There are various tactics for disinformation, including misinformation, disinformation, and malformation, which will be defined later. It is worth noting that disinformation is a strategy, while fake news is a type of tactic used to generate disinformation, although it is not the only one. The art of disinformation combines a good understanding of psychology, sociology, history, politics, economics, and other relevant concepts to skillfully manipulate and spread narratives that influence how individuals and groups think and make decisions.

If we understand technology and access to it as force multipliers, in digital technologies and their platforms, we find an asymmetric relationship between the costs of disseminating manipulated information and its effect. In other words, there is an economic relationship of low implementation costs and high impact.

2.1 Disinformation

With the advent of information technologies, their transnational nature, and their lack of oversight, today any individual or group can use disinformation practices at minimal cost and reach massive audiences in real-time. Disinformation is used as a political tool to influence elections and political decisions, create instability and divisions within society, and is currently an effective tool in the arsenals of states, influential groups, and intelligence services.

Preparing a disinformation offensive requires relatively low effort and resources compared to the effects it generates. However, defense is very complicated to achieve, and most of the time, reactions come too late to achieve a proper positive effect and reverse the damage already caused.

Defining the problem of online disinformation is key to specifying objectives and developing responses. This is considering that there are multiple terms to describe the phenomenon. Therefore, adopting official definitions and using them consistently, as proposed in this chapter, can help institutionalize approaches and ensure that the multiple causes and manifestations of online disinformation are accurately addressed.

In that sense, it is essential, first and foremost, to define the concept of online disinformation and differentiate it from the popular term "fake news." Particularly, the notion of "fake news" became globally known during the 2016 United States presidential elections. The frequency of the term increased significantly due to false stories shared massively through social media, leading it to be named the word of the year in 2017 by the Collins Dictionary.

Although disinformation is not a new phenomenon and information has been invented and manipulated since time immemorial to win wars, promote political ambitions, harm the most vulnerable, or obtain economic profit[14], it was not until the rise of social media as a news distribution channel that the concept regained strength.

Experts, authors, and international organizations have encouraged and recommended the use of the term "online disinformation" instead of "fake news."[15]

Among the arguments for reaching this conclusion is the fact that the term "fake news" does not capture the full extent of the disinformation problem. It has the problem of hiding certain aspects of the phenomenon of disinformation related to content, format, motivations, and agents involved in its distribution (Kalsnes 2018; Wardle and Derakhshan 2017).

[14] Asamblea General de las Naciones Unidas, La Desinformación y la Libertad de Opinión y de Expresión Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Irene Khan, pág. 2.

[15] Report of the Independent High-Level Group on Fake News and Online Disinformation (European Commission), A Multi-Dimensional Approach to Disinformation, 10.

Additionally, the term has been wrongly used by various actors (especially politicians) to discredit news they disagree with. It is used generically for any information that people do not believe (Nielsen and Graves 2017; Waisbord 2018) or to delegitimize an opponent's point of view (Farkas and Schou 2018). Furthermore, the concept of "fake news" is also inappropriate because it suggests a true/false dichotomy instead of a continuum (Mourao and Robertson 2019) Following this line of thought, UNESCO, and the OECD, among other institutions[16], have decided to use "online disinformation" to refer to this problem. The EU Commission adopted the term "online disinformation" and defines it as "verifiably false or misleading information that is created, presented, and disseminated for profit or to deliberately deceive the public, and can cause public harm."[17] Public harm refers to threats to political processes and public goods, including the protection of health, the environment, or citizens' security. Similarly, the OECD, when referring to disinformation, defines it as the act of "knowingly sharing false information to cause harm."[18]

Finally, national laws and policies in different countries around the world use the concept of online disinformation, which they define by combining a variety of distinctive elements. These elements include (i) false or misleading information, (ii) the intention to cause harm or not, and (iii) the nature of the harm caused or sought.[19]

Concrete examples can be found, such as Estonia, where online disinformation is defined as "false or misleading information that is intentionally created and disseminated for political, economic, or personal benefit."[20] In the United Kingdom, its "online harms" report, defines it as information created or disseminated with the deliberate intention to mislead; this could be to cause harm or to gain personal, political, or financial benefits.[22]

[16]Ver, por ejemplo, C. Iretony, J. Posetti y otros (UNESCO), Periodismo, "Noticias Falsas" & Desinformación Manual de Educación y Capacitación en Periodismo, 6; C. Matasick, C. Alfonsi & otros (OECD), Governance Responses to Disinformation: How Open Government Principles Can Inform Policy Options, OECD Working Papers on Public Governance, No. 39, OECD Publishing, Paris (2020), 12.
[17]European Commission, Communication from the Commission, Tackling Online Disinformation: a European Approach, 3.
[18]OECD, Draft Principles of Good Practice for Public Communication Responses to Mis-and Disinformation, Anexo II (pág. 13).
[19]Asamblea General de las Naciones Unidas, La Desinformación y la Libertad de Opinión y de Expresión Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Irene Khan, pág. 3.
[20]Tyler McBrien, Defending the Vote: Estonia Creates a Network to Combat Disinformation, 2016-2020, Princeton University, pág. 3.
[21]Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department (UK), Online Harms White Paper, pág. 22

Considering all of the above, for the Strategy presented in this report, online disinformation is defined as:

"Deliberately manipulated information that is crafted and/or disseminated with the potential to both deceive and obtain benefits and/or cause public or private harm."[22]

2.2 Associated Concepts

Other concepts associated with online disinformation are discussed below. It is important to understand these concepts in terms of their particularities and differences because they can significantly change the nature of the threat.

2.2.1 Misinformation (misleading)

As a general rule, misinformation or misleading information refers to false information that is created and/or shared without the intention of causing harm or damage. For example, the European Commission defines it as information with false or misleading content shared without the intention to harm, although its effects can be harmful, meaning when people share false information with friends and family in good faith.[23]

2.2.2 Disinformation (sabotage):

Regarding disinformation, its definition aims to capture information that is based on real facts but is used out of context to deceive, harm, or manipulate. In this regard, the OECD defines it as sharing genuine information to cause harm, often bringing into the public sphere what was intended to remain private.[24] This occurs, for example, in the case of information leaks.

2.2.3 Influence Operations:

This concept encompasses the coordinated efforts of national and/or foreign actors, or both collectively, to influence a target audience using a series of deceptive means, such as suppressing independent sources of information, combined with disinformation.

Influence operations consist of sophisticated networks that propagate manipulated information to influence the outcomes of collective decision-making processes or public sentiment in general. They are rarely limited to one medium and are usually distributed across different platforms, including offline sources.

[22]Some clarifying notes: although its dissemination is digital, its origin could be from other sources of different nature (for example, a politician's comment); within the notion of online misinformation, it does not include misleading advertising, information errors, satire, and parody; among its objectives may be causing public harm, threatening political processes, affecting health, the environment, or citizen safety; when it is spread through digital media, it is referred to as "online misinformation."

[23] Comisión Europea, Plan de Acción para la Democracia Europea, pág. 22.

[24] OECD, Draft Principles of Good Practice for Public Communication Responses to Mis-and Disinformation, Anexo II, pág. 13.

Historically, influence operations have taken various forms, from covert campaigns based on false identities to overt media efforts controlled by the state using authentic and influential voices to promote messages that may or may not be false. However, when an actor hides their identity through deceptive behavior, the public lacks sufficient signals to judge who they are, how reliable their content is, or what their motivation might be.

It is important to distinguish between disinformation and influence operations because both have different characteristics, impacts, and solutions to the problem. As part of a potential solution in this document, communication with social media platforms is essential to limit the effects of identified malicious behavior on their platforms as soon is detected. Thus, understanding the differences and speaking the same language in terms of the nomenclature of phenomena is essential for a productive result.

2.2.4. Foreign Interference in the Information Space

Foreign interference can take the form of external actors seeking to manipulate internal politics, even through covert and deceptive means, to undermine political sovereignty and harm social cohesion. In recent times, the threat of foreign interference has increased in potential and severity due to the internet and social media. These platforms have contributed to the growing ease, sophistication, and impunity with which hostile foreign actors can carry out influence operations.

This idea encompasses coercive and deceptive efforts to disrupt individuals' free formation and expression of political will by a foreign state actor or its agents. As a general rule, they are carried out as part of a broader hybrid operation (e.g., cyber warfare).

2.3 Long-Term Disinformation (2035)

Disinformation, as a modern threat, is still in its early stages. Social media began to gain strength just around 15 years ago. The information ecosystem is becoming increasingly complex due to the explosion of information that surrounds users. Recently, artificial intelligence (AI) technologies have been developed that are trained to generate written content with manipulation objectives.

The dissemination of content on social media is mostly carried out by networks of bots controlled by AI algorithms, which better understand the peculiarities of social media algorithms than humans. However, the most concerning aspect is the improvement of deep fake technology that uses AI, through generative adversarial networks (GANs), to generate video content that extremely realistically imitates the appearance and voice of real people, being imperceptible to an untrained person or the human eye.

In another 15 years, the dangers in the information space will reach alarming levels, and current strategies will likely be obsolete and ineffective. This field, which is in continuous dynamics, similar to cybersecurity, will open the doors to some threats that, if left unchecked, could dangerously undermine the foundations of democracy, the rule of law, and human rights in every state. Ignoring the threat will not make this problem disappear; it will only create conditions for more painful effects

3. CURRENT SITUATION IN CHILE

An exhaustive analysis of the current issues of misinformation in Chile has been conducted, and the findings are structured in three sub-chapters that will form the basis for the strategy's action axes:

- **Institutional Framework**
- **Education**
- **Defense**

The strategy acknowledges the identified problems and proposes a roadmap of solutions that can be implemented to mitigate these issues.

3.1 Institutional Framework

3.1.1 Regulatory Framework

The current lack of regulation in Chile promotes a systematic growth of misinformation without imposing any limits. The absence of a regulatory framework that establishes rights, obligations, and responsibilities within a sustainable architecture creates an environment where rules and responsibilities are not defined, leading to uncontrolled gaps that generate more problems.

The unregulated relationship with social media companies is hindering the efforts of relevant institutions to limit misinformation campaigns. In countries with more advanced legislation in this regard, rules are imposed on social media companies, and direct communication channels with these companies are established.

3.1.2. Lack of Responsible Institutional Approach

In Chile, there is currently no organized institutional approach to address risks, implement regulatory, oversight, and punitive measures, and establish countermeasures processes for expedited information verification, whether via digital or traditional media.

Delimiting responsibilities is of utmost importance when dealing with the phenomenon of misinformation at a state level. Without clear definitions or associated metrics, an appropriate response cannot be executed. When it comes to misinformation, the opportunity presents itself within limited timeframes, and fast action is crucial since its propagation is rapid.

Given that misinformation affects society as a whole and involves numerous government and civil society organizations, the lack of a normative definition regarding tasks and responsibilities is a significant flaw.

Additionally, strategic communication is vital for the state to effectively engage with civil society. The government needs to respond effectively to misinformation campaigns and have a prepared communication strategy with established actions to address contingencies.

This requires a high-level political body responsible for centralizing efforts in this matter, without becoming a censor or a "ministry of propaganda," which could be detrimental to democracy and institutional integrity, as observed in various instances throughout history.

Successful experiences in countries like France and Sweden can serve as references, where such an organization focuses on aspects related to education, legislation, and defense, with mechanisms in place to prevent institutional instability or democratic imbalances.

3.1.3 Insufficient Operational Capacity

In terms of operations, the lack of analytical and responsive capabilities to dynamic threats posed by different actors is evident. Most decision-makers currently do not fully grasp the extent of hybrid threats and are not prepared to respond to a crisis. In such situations, time, processes, roles, and responsibilities are fundamental and need to be explicit and trained by all involved actors to achieve an efficient response.

Without a technological and operational environment capable of detecting and adequately understanding the spread of information threats, misinformation campaigns are detected too late or even go unnoticed, and their effects can be severe, long-lasting, or difficult to reverse.

A systemic approach is essential to achieve proper synergy, avoid overlaps or gray areas, and attain efficiency and effectiveness. This is a requirement for adopting a modern approach that safeguards the interests of Chilean society regarding misinformation matters

3.2 Education

3.2.1 Critical Thinking

Critical thinking is crucial in the fight against misinformation as it allows individuals to discern between true and false information and make their own decisions. More resilient countries when it comes to this anomaly, like Finland, have incorporated critical thinking as an integral part of their educational curriculum from an early age, which has not been achieved in Chile. As Jorge Gatica indicates, referencing a study by the University of Chile, "44% of Chileans do not understand what they read; furthermore, 80% of the adult population falls into the two lowest levels of basic competencies associated with literacy, both in prose, documents, and quantitative information." [25]

3.2.2 Disinformation Training

The lack of general population knowledge about disinformation techniques and the ability to detect them is creating an environment where most people do not fully understand the spectrum of the threat and how to build personal resilient defenses against it. Awareness campaigns, both targeted and general, are needed to introduce and train the population to detect manipulated information and report it to appropriate institutions.

[25] Gatica, Jorge. (2016). El enfoque curricular por competencias y la necesidad de innovar en la docencia. En Revista Educación del Ejército de Chile N 43. p. 107

Information culture is a highly important topic for the country's future. ***A culture of not sharing before verifying*** is crucial to limit the spread of disinformation among social groups. Educators are not adequately trained to educate their students on this topic, and they also lack access to tools and materials to develop in students the intuition, attitude, and predisposition to filter information before spreading it.

3.2.3 Advanced Research

There is a lack of academic development in researching this topic, and higher education institutions in Chile are not employing enough efforts to incentivize it. This deficiency in cutting-edge research on the phenomenon is crucial. It is not enough to solely replicate knowledge gained in other countries because idiosyncrasies are relevant characteristics that impact how those who employ disinformation operate, and consequently, the preventive and remedial measures taken.

3.3 Defense

3.3.1 Doctrine

In the current environment, the use of information for influencing military operations plays a significant role. Though it has always been important, the reach it holds today due to the massification of information and communication technologies gives it special significance.

The constant development of hybrid warfare mechanisms, below the threshold of armed conflict, creates a new scenario of threats for Chile. The Armed Forces and Security forces must maintain capabilities to address these new dimensions of conflict, which can serve as enablers for conventional military operations and also act as an independent variable in military operations other than war.

Additionally, updating the doctrine of the Armed Forces and Security organizations is essential to align it coherently with the efforts that will be implemented in these areas by other state institutions and civil society.

3.3.2 Reactive and Proactive Capability

Foreign influence and interference operations represent one of the biggest dangers to the stability of Chilean democracy. In the current stage, the responsibility to respond to an information threat is not adequately understood due to the lack of regulations, knowledge, and understanding of the phenomenon.

Institutions also lack a responsible body that is capable of responding to the threats presented in this document. The organizations responsible for influence operations must not only have the ability to react to an attack but also defend themselves proactively, in line with the development of an Active Cyber Defense Strategy.

Similar to cybersecurity, a reactive approach is being employed after the damage is already done, to prepare the defense for the types of threats that will continue to evolve. Without offensive capabilities, organizations are doomed to fail against actors employing advanced attacks, as the current reality shows that most states (such as the US, France, the UK, or Australia) are using an active cyber defense strategy to protect their critical assets and neutralize threats.

4. INVOLVED ACTORS

4.1 State Actors

This phenomenon has become a risk to the rule of law, democracy, and human rights. Given this scenario, the state must take responsibility and measures to protect the institutions and its citizens.

Drawing upon the ideas of various thinkers since ancient times, Maritain stated almost a century ago that the state has three fundamental tasks: maintaining the law, promoting the common welfare and public order, and administering public affairs.

Consequently, the state plays an essential role in addressing this new threat. It should be capable of creating a conceptual framework to harmonize the efforts of the public and private sectors, state organizations, civil society, academia, and the general public.

This requires establishing an appropriate institutional framework with specialized bodies and specific regulations. Additionally, education aimed at producing collective and individual cultural change, as well as proactive and reactive capabilities to address potential attacks in this area, affecting the country and each citizen, must be encouraged.

Just as disinformation is relevant to internal affairs, it also extends to external affairs. Nowadays, disinformation is used by state actors as a low-cost and effective tool to influence the internal or external affairs of other countries. Current conflicts demonstrate that a significant part of the battle takes place in the virtual world, employing a set of techniques to weaken countries and instill social reflexes that favor the perpetrators.

4.2 Non-State Actors and Social Networks

Non-state actors are increasingly becoming important in the information space. While some states still have prominence in managing information, particularly those with totalitarian or undemocratic governments, the qualitative and quantitative expansion of the internet over the past three decades has given non-state actors the ability to influence the information space.

The problem not only pertains to social media companies or social communication media but also extends to NGOs, lobbyists, social movements, terrorist groups, cybercriminals, large corporations, and many other actors who utilize these platforms for propaganda or other antisocial actions.

The issue lies in the fact that while there exist international and internal regulations governing state actions, non-state actors can operate with greater freedom due to the lack of norms, ease of evading them, or simply the perceived or effective impunity surrounding their actions. This is significantly contributed to by the increasing difficulty of attribution.

To maintain the information space free from interference and malicious actions, special attention must be given to social media companies. The major platforms operating in Chile have their headquarters abroad. Although they have a significant impact on the quality of information with which the Chilean population interacts, there is currently no direct means of communication with them or regulation that incentivizes the removal of conflicting material.

As previously mentioned, social media companies serve as platforms for state and non-state actors who utilize the power of digital information for their political purposes. It could be the responsibility of these platforms to limit disinformation in their spaces. However, most of the time, they lack sufficient personnel and expertise to detect every attempt at disinformation.

On the other hand, should they exercise censorship? Can they, based on their own judgment and ethical standards, limit citizens' freedom of expression?

Recently, social media platforms have improved their detection capabilities for bots, making large coordinated campaigns of inauthentic behavior less improbable than before but still possible.

Where social media companies struggle the most is in dealing with influence operations. These operations are structured in detail and are very difficult to detect for inexperienced observers who do not understand the intricacies of a country or its idiosyncrasies.

Foreign information analysts, without proper training, knowledge, and experience, will find it challenging to understand Chilean society's culture, making it difficult for them to identify and understand when influence operations are taking place.

That is why, in advanced countries that take disinformation seriously, local agencies dedicated to this phenomenon complement the work of social media companies' Trust and Safety departments and can alert social media companies about suspicious operations as they occur. This allows the companies to become more efficient in neutralizing questionable content. Adequate regulations that define the responsibilities and obligations of social media companies should serve as the foundation for efficient cooperation to incentivize their collaboration on these issues.

Finally, it is necessary to remember that there is a large number of other relevant non-state actors operating in the information space. Unfortunately, it is challenging to regulate their actions. Therefore, cultural changes are required to achieve an ethical framework that leads to the self-regulation of organizations and individuals, through robust collaboration among all actors.

This collaboration with civil society is vital for a healthy information space, and ongoing cooperation is necessary to ensure a transparent process of tackling disinformation. The state alone is not sufficiently robust to operate in this field, so the action of all actors, especially civil society, is indispensable.

5. PROPOSAL FOR A NATIONAL STRATEGY AGAINST ONLINE DISINFORMATION

A strategy, in general terms, is the coordination that an entity undertakes to utilize its available resources to achieve its objectives and materialize the desired condition within a specific timeframe.

To design this strategy, a deductive approach was adopted. Initially, operational definitions were established to define the scope of the various concepts associated with the notion of online disinformation, using different references. Subsequently, to determine the current situation of this phenomenon in Chile, a collaborative analysis was conducted, which allowed for the identification of different variables, their interrelationships, and their impacts.

Following this, the present strategy was developed, focusing on three thematic pillars: institutional framework, education, and defense. For each pillar, initiatives were established, outlining actions aimed at achieving specific objectives, defining responsibilities, involved actors, as well as an estimated timeframe.

The three pillars are interdependent, complementary, and mutually reinforcing, and they are closely interconnected, just like the initiatives themselves.

Considering that the attainment of each objective is directly linked to resources, particularly financial resources, the established timeframe is merely indicative. Additionally, it attempts to reflect a sequential approach based on the cause-effect relationship that occurs between them.

In the following table, an explanatory overview of the strategy is presented, indicating the activities, actions, responsible parties, involved actors, timeframe, and objectives for each pillar, highlighting the aspects to be developed:

"National Strategy Against Online Disinformation 2035 (ESNACDEL-2035)

Eje	Iniciativa	Acción	Responsable	Involucrados	Plazos	Objetivo
Institucionalidad	Elaborar documentos normativos (matriz o complementarios a lo que ya hay)	Promulgación de una Ley Anti-Desinformación, para: • Normar una arquitectura • Regular el comportamiento de y en las redes sociales • Asignar/crear los órganos responsables de responder a cada amenaza identificada, tanto de desinformación como de misinformación. • Regular las operaciones de influencia. • Disponer medidas de defensa y de inteligencia. • Regular el potencial de injerencia extranjera y otras medias para resguardar al país y a su población.	• Congreso	• Otras entidades de gobierno. • Sociedad civil (Colegio de Periodistas, ACHIPEC, etc.)	2023	Generar un marco normativo que regule los aspectos de desinformación operaciones de influencia y otros conceptos relacionados.
	Crear una Agencia Nacional Antidesinformación (**ANAD**) u otro organismo responsable	• Desarrollo de un organismo destinado a coordinar, implementar acciones vinculadas a la prevención en material de desinformación.	• Presidencia • MININT • Congreso Nacional	• SIE • Sociedad civil • Organismos públicos	2024	Contar con un organismo independiente y robusto, en el más alto nivel político responsable de gestionar los esfuerzos nacionales antidesinformación.
	Generar capacidad de gestión y respuesta	• Juegos de guerra y simulacros de emergencia para toma de decisiones y gestión	• ANAD *	• Gobierno • FFAA • EMCO • Infraestructura crítica • SIE • ONEMI • SERVEL • Otros	2024	Preparar los tomadores de decisiones para enfrentar emergencias generadas por el fenómeno.
Institucionalidad	Implementar alianzas internacionales	• Generación de vínculos internacionales de diverso orden, destinados a potenciar iniciativas y medidas.	• MINREL	• ANAD • Sociedad Civil	2024	Incrementar las capacidades de identificación y respuesta antes del fenómeno.
	Establecer relaciones directas con empresas de redes sociales	• Desarrollar relaciones basadas en reglas con empresas de RRSS y media presentes en Chile	• MININT • ANAD	• Empresa privada asociada a RRSS.	2024	Generar comunicación con las empresas para poder limitar campañas dañinas de desinformación.
	Generar capacidades operacionales	• Desarrollar una cultura y una comunidad de verificación de datos.	• Ministerio de Interior • ANAD	• Sociedad civil • MINEDUC	2024	Aumentar la cultura de verificación de datos
		• Desarrollar capacidades de inteligencia de amenazas.	• ANAD • SIE	• FFAA • Carabineros • PDI	2024	Generar capacidades de alerta temprana
		• Desarrollar capacidades tecnológicas y procedimientos.	• MININT • ANAD	• CORFO • Sociedades privadas • Sociedad civil • SIE	2024	Generar tecnología para prevenir y responder al frente del fenómeno
	Garantizar la viabilidad del proyecto a largo plazo	• Sostener la operacionalización de la estrategia. • Garantizar el presupuesto. • Sensibilizar a la opinión pública. • Legitimar la función. • Generar / incrementar las capacidades de comunicación estratégica	• MININT	• Todos los organismos del Estado	2024	Asegurar la permanencia de la institucionalidad desarrollada.

* Once this organization or the body implemented for these purposes is formed, this provision applies from here onwards in the present strategy

Eje	Iniciativa	Acción	Responsable	Involucrados	Plazos	Objetivo
Educación	Desarrollar pensamiento crítico mediante educación formal	• Cambio de estrategia curricular en todos los niveles de educación • Implementación de asignaturas destinadas a desarrollo de pensamiento crítico	• MINEDUC • ANAD	• Profesores • Estudiantes • Especialistas en educación	2030	Desarrollar el pensamiento crítico nacional en instancias de educación formal, a objeto de incrementar la capacidad de evaluar la información que se recibe desde medios digitales.
	Capacitar, mediante instancias informales, a los jóvenes y adultos	• Cursos de capacitación gratuitos, financiados por el Estado. • Generación de oferta de cursos de capacitación en el ámbito privado. • Talleres, juegos, mini-videos, quizz	• MINEDUC • ANAD	• Estaciones media • Gobierno Digital • Universidades • Escuelas • Artistas • Influencers • SERVEL	2026	Desarrollar el pensamiento crítico nacional en instancias de educación informal y masiva, a objeto de incrementar la capacidad de evaluar la información que se recibe desde medios digitales.
	Fomentar investigación aplicada en estas temáticas	• Incentivo a productividad académica en estas áreas. • Generación de vínculos internacionales con otras instituciones relevantes.	• MINEDUC • ANAD	• Universidades • MINREL • MINDEF • ANID	2024	Generar conocimiento nuevo sobre el fenómeno su efecto y soluciones.
	Sensibilizar mediante campañas	• Implementación de actividades en MMCS y RRSS	• MININT • ANAD	• MMCS • Gestores de RRSS	2024	Fomentar el conocimiento sobre la desinformación y generar habilidades de identificación de información manipulada.
	Desarrollar instancias de formación de formadores	• Implementación de talleres de desarrollo de capacidades de formación, es estudiantes y monitores.	• MINEDUC • ANAD	• Universidades • Colegios	2024	Desarrollar una modalidad sostenible de educación transversal en la sociedad.

Eje	Iniciativa	Acción	Responsable	Involucrados	Plazos	Objetivo
Defensa, Orden y Seguridad	Actualizar el fenómeno en la doctrina de las FFAA y de Orden	• Revisión y actualización de documentos doctrinarios.	• MININT • MINDEF	• EMCO • FFAA • FFOyS • ANAD	2024	Incorporar el fenómeno en la doctrina institucional, de forma tal de garantizar el manejo seguro de medios y responsabilidad social, en coherencia con lo que se desarrolle en otros sectores de la vida nacional.
		• Incorporación en la malla curricular de los diversos cursos.	• MININT • MINDEF	• EMCO • FFAA • FFOyS • ANAD	2025	Incrementar la educación formal en las diversas instancias formativas de la FF.AA.
		• Implementación de Lecciones Aprendidas.	• CJ Inst. FFAA. • GD Carabineros • DG PDI	• Instituciones • ANAD	2023	Optimizar el desempeño en la prevención y neutralización de las amenazas.
	Entrenar y generar conocimientos en distintas instancias	• Implementación de ejercicios y otras instancias específicas de entrenamiento.	• CJ Inst. FFAA. • GD Carabineros • DG PDI	• Instituciones • ANAD	2024	Entrenar capacidad preventiva y reactiva, como respuesta a acciones de desinformación.
		• Incorporación de la temática en actividades académicas.	• CJ Inst. FFAA. • GD Carabineros • DG PDI	• Instituciones • ANAD	2025	Desarrollar docencia e investigación de frontera, para incrementar la capacidad de respuesta al impacto del fenómeno en un contexto holístico.
	Generar capacidad reactiva y proactiva a través de un organismo especializado	• Organización de entidad de defensa especializada. • Implementación de la doctrina de ciberdefensa activa para la guerra informacional. • Capacitación de analistas. • Desarrollo de capacidades técnicas de análisis.	• MININT • MINDEF	• EMCO • FFAA • FFOyS • ANAD	2025	Generar la capacidad para accionar y reaccionar frente a amenazas informacionales, para identificar y contrarrestar operaciones de influencia digitales

6. CONCLUSIONS

In conclusion, given the available evidence, the development and implementation of a national strategy that addresses a threat, which first needs to be understood to proactively counteract it, is considered crucial.

The proposed axes and actions presented here cover various aspects, providing a perspective that allows for both prevention and response, as well as effective collaboration among stakeholders. It must be considered that this phenomenon will continue to grow, therefore requiring a multidimensional and multisectoral approach involving everyone to advance towards the defense of accurate information.
To summarize, the following three axes should be considered in the process of an effective and efficient strategy:

1. Institutional Framework: This involves the development and implementation of a regulatory and administrative framework that enables the execution of regulatory, preventive, and responsive actions to tackle online misinformation and its effects.

2. Education: Recognizing that combating the phenomenon of online misinformation requires a profound cultural shift, it is necessary to develop both collective and individual capacity to operate ethically and protect oneself from its harmful effects, through the application of critical thinking.

3. Defense: Given that ensuring the safety of individuals, institutions, and society, in general, is one of the exclusive responsibilities of the State, a preparedness to respond to any events that threaten the normal development of activities, both domestically and internationally, must be established.
As previously stated, there is no perfect model in the fight against misinformation since it is a fluid concept. However, one thing is certain: inaction in the face of this phenomenon is not an option due to the serious social consequences it can entail. Legislators should learn from the successes and criticisms of other countries and develop a model that can effectively counteract influence operations in the short, medium, and long term.

*Chapter 7_*

Interoperability and Digital Identity

PARTICIPANTS IN THE ELABORATION OF THIS TEXT:

- Coordinating team of the working group " INTEROPERABILITY AND DIGITAL IDENTITY ": Francisco Mendez and Carla Illanes

- Technical Working Committee of the working group " INTEROPERABILITY AND DIGITAL IDENTITY " convened by the Committee: Berioska Contreras, Marco Zúñiga, César Galindo, Jose Luis Pérez, Álvaro Vásquez, Patricio Ovalle, Ítalo Foppiano y Raimundo Roberts.

1. INTRODUCTION

We inhabit cyberspace in the same way we inhabit a city, which requires us to establish a way of coexisting and relating to each other safely and reliably.

To achieve this, parallel to the physical world, conditions must be established for information to flow in secure and robust infrastructures, allowing interaction between individuals and institutions, as well as between institutions themselves, to enable data flows with the highest possible trust, without compromising their integrity, secure accessibility, and traceability.

Digital trust is the foundation of a digital society, and it is built on two fundamental pillars: digital identity and interoperability. Both concepts will be further developed and are linked to another fundamental ingredient: cybersecurity.

In the process of the State's Digital Transformation, in which we are immersed, digital identity and interoperability must be the axes of the transformation process that allow citizens to interact securely with the State's Informatic and computer systems, and thus effectively make technological progress a facilitator that improves quality of life.

The task entrusted to the authors of this chapter, following what was established when convening the Cybersecurity Work Task and based on the experience of the specialists convened and considering some publications from ECLAC, established two challenges to be developed regarding these matters.

The **first challenge** is the construction of a robust digital identity, with means that ensure not only identity but also authentication that leaves no doubt about who someone claims to be, to finally grant access to computer systems that handle personal data and allow us to carry out the interactions we deem necessary.

Considering the growth of digital transactions, it is necessary to advance the identification and verification of individuals in the world of digital services. Digital identity technologies are evolving rapidly, giving rise to new business, service, and operational models, creating a variety of systems that require support not only in technology but also in regulations that expand their use both privately and publicly.

[26] "Gobernanza Digital e Interoperabilidad" disponible en: https://repositorio.cepal.org/bitstream/handle/11362/47018/1/S2100258_es.pdf

[27] "La gestión de la identidad y su impacto en la economía global" disponible en: https://publications.iadb.org/es/la-gestion-de-la-identidad-y-su-impacto-en-la-economia-digital

The **second challenge** is the implementation of interoperability, which is the exchange of information between multiple systems that handle diverse data so that it can be shared electronically in real-time from the places where it is stored and processed. It is the systems that transfer information to each other in limited terms, and thus, among other benefits, users can obtain diverse information from multiple sources. Furthermore, the Inter-American Development Bank (IDB) described interoperability as:

"The ability of ICT systems to interconnect data and processes to share information and knowledge within the framework of protection, ethics, and security, in an agile, efficient, and transparent manner, with the ultimate goal of making fact-based decisions."

Interoperability is also a requirement to enable digital communication and information exchange between public administrations, as well as between these administrations and private companies and non-governmental organizations that require interaction with the government, to achieve a single digital market. If we leave interoperability as a topic to be resolved among interested parties, the complexity in terms of cybersecurity multiplies significantly.

Interoperability must be understood from at least four perspectives: normative/legal, process, semantic, and technological in their respective architectures and combinations of available tools. The existing international experience reaffirms this distinction, as will be explained later.

Digital Identity and Interoperability are fundamental pieces that allow the construction of cybersecurity building in terms of the relationships between users and institutions in cyberspace, and they must be based on secure, robust, and resilient models so that they guarantee secure and expedited data.

In over than 9 working meetings, both in-person and virtual, some plenary and others partial, representing more than 40 hours of work, developed between June 22 and November 30, 2022, a team made up of professionals from diverse backgrounds including lawyers, engineers, journalists, entrepreneurs, academics, and military personnel, achieved the result reflected in this chapter. It brings together concepts and examples obtained from policies implemented by other countries. The purpose is to structure a theoretical, technical, and political foundation to be considered to have a robust digital identity and implement the necessary interoperability that allows the objectives of Law N°21.180 on Digital Modernization of the State to be fulfilled.

2. CONTEXT

Interoperability, that is, the ability to securely, quickly, and efficiently share information between public entities, as well as between public and private entities, is a requirement to enable e-government and the exchange of information between public administrations, and between these and private companies and non-governmental organizations that need to interact with the State.[28]

Interoperability within the State:

→Simplifies the relationship between citizens, companies, and organizations with State institutions.
→Enhances cooperation between State institutions to meet the needs of citizens, companies, and organizations.
→Incorporates basic standards (data, technology, communication) in the interaction between State institutions.
→Integrates institutions regardless of their level of technological development.
→Enhances administrative simplification and processes within and between institutions.
→Reduces costs and efforts for both institutions and citizens, companies, and organizations.
→Promotes a favorable and competitive business climate for countries.

To build trusted digital services that promote a secure society and a unified digital market, electronic transactions with legal certainty are required. This would make it possible to develop the growth potential of the digital economy. As an example, it is estimated that the European Union and England would achieve associated growth worth €1,036.71 billion by 2025.[29]

As important as the legal certainty of electronic transactions is the data economy, which involves an interoperable digital identity for the exchange of documentation and digital signatures between services provided by multiple digital governments.

Now, expansive digitization and connectivity increase the risk of cybersecurity, society is more vulnerable to cybercrime and hybrid cyber threats. At the same time, according to The Identity Defined Security Alliance, during the first half of 2022, 84% of 504 organizations have experienced identity breaches, and 96% of them have reported that to minimize breaches they need to strengthen identity-centric security.[30]

[28] "Interoperabilidad en gobierno electrónico. Conceptos y regulación extranjera Estonia, Costa Rica y Provincia de Neuquén", Asesoría Técnica Parlamentaria, enero 2023, Biblioteca del Congreso Nacional. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33950/2/Informe_BCN_interoperabilidad_comparado_Est_Neu_CrRc.pdf

[29] https://es.statista.com/Statista GmbH es un portal de estadística que pone al alcance de los usuarios datos relevantes que proceden de estudios de mercado y de opinión

[30] https://www.idsalliance.org/press-release/new-study-reveals-84-of-organizations-experienced-an-identity-related-breach-in-the-last-year/

Considering the above, and understanding that cybersecurity constitutes an enabling axis for the development of a digital government and is the foundation of the digital economy (involving both public and private actors, non-governmental organizations, citizens, and individuals) and that digital identity and interoperability contribute to and enable this scenario, the development of these topics will be addressed with a top-down integrative approach with the following lines of work as structuring axes:

1. Governance Model: Considering the complexity and cross-cutting scope of Interoperability and Digital Identity issues, it is necessary to have a Governance Model that articulates all the actors that contribute to the success of its implementation horizontally and at different levels of influence (Strategic, Governing, and Executing) in such a way that guidelines, attributions, inputs, resources, and capabilities required in the ecosystem in which the skills of interoperability between actors and digital identity will intervene for the generation of public value.

2. Institutional Model: It is necessary to have updated legislation to implement a governance model. This should develop a defined institutional framework that allows for the establishment of attributions, organizational structure, resources, and sustainability models.

3. Reference Framework for Country Interoperability and Digital Identity: Specify the dimensions of each topic, establishing coverage and interrelationships. The European Union's interoperability framework (EIF)[31] can be mentioned as a reference for both interoperability and digital identity.

4. Value Generation Model: The conception of a modern state where its processes add value through digitization in the handling of information required from one institution or company to another, which can be made available to improve process efficiency, both internally and to facilitate the procedures that the population must carry out.

5. Technological Criteria to Use: Bilateral or decentralized, central, federated, four corners, or other. It is possible to propose, as an example, some enabling tools or platforms based on successful experiences from other countries.

6. Change Management and Culture Model: It should address the identification of impacted and influential institutions and target groups, identify the hierarchies of resistance generated by interoperability and digital identity (at a technical and adaptive level), and propose action plan structures for each domain of resistance (Adaptive, Knowledge, Information).

[31]https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail

3. GOVERNANCE MODEL

The correct identification of the actors involved, their degrees of influence, and hierarchies in decision-making, is a key aspect for the success of cybersecurity and, within it, interoperability and digital identity.

To develop this, it is necessary to have a reference definition of what will be understood as Governance:

The management of relationships between various actors involved in the process of deciding, executing, and evaluating public value issues, is a process that can be characterized by competition and cooperation where possible rules coexist; and that includes both formal and informal institutions. The form and interaction between the various actors reflect the quality of the system and affect each of its components, as well as the system as a whole.

The actors involved in the decision-making process are a key factor for the different instances of Governance detailed below. In this identification, the level of impact that cybersecurity will have on their daily work (impact on the generation of benefits as well as changes in usual activities) must be taken into account, as well as the identification of the influence of the actors involved. Both concepts are presented in the Change Management section.

Given the different nature of the actors involved in the process of achieving cybersecurity implementation, ECLAC proposes the following classifications or hierarchies of Governance associated with Digital Government that can be extrapolated and/or identified as requirements for cybersecurity, namely:

Strategic Governance	Establishes priorities, policies, strategies, stakeholders, and attributions.
Steering Governance	Establishes priorities, policies, strategies, stakeholders, and attributions.
Implementing Governance	Define, design, implement, assist, accompany, resolve.

Where:

→Strategic Governance: contributes to the articulation and coordination of different sectors (or related institutions) in the search for identifying components of shared value that can only be achieved through joint and coordinated action. This requires having the binding authority to convene, prioritize, allocate resources, build shared plans, and commit to results.

→Governing Governance: contributes to the identification of laws, technical standards, rules, roles, methodologies, and compliance audits (evaluation of the impact of initiatives), as well as the definition, design, and implementation instructions of the cross-cutting pillars of Digital Government solutions such as Country Interoperability, Digital Identity, Digital Signature, Digital Mailbox, Digital Folder, Single Window, Cybersecurity, and any other cross-cutting solution for institutions such as personnel management, accounting, budgeting, document management, Unique Digital Address, or others.

→Executive Governance: contributes to the implementation of Digital Government solutions in their components of Processes, People, and enabling Information Technology. This involves coordinating platforms, technological tools, and specialized professionals, through in-house teams, contracting application solution services, and/or third-party development.

Each governance area contributes, through its actions, to the flow from the horizontal to the vertical (articulation of actors, resources, initiatives; strategically, governing and executing) and between each governance area, in coordinated cycles of actions and actors with a shared purpose and goal that contributes to making digital government feasible and generates the expected and committed public value.

This is materialized with a governance structure that includes at least:

→Materialization of Strategic Governance: Council of Ministers where the axis of Cybersecurity is permanently installed and/or a high-level Digital Government Commission that defines, prioritizes, and validates policies and initiatives of State interest and acts as a board of directors, ensuring that some members are permanent to mitigate the effects of changes in presidential terms.[32]

[32] Actualmente, existen tres instancias de alto nivel que ven temas relacionados directa o indirectamente con estos aspectos:
1.Consejo Asesor Permanente para la Modernización del Estado y el Comité de Modernización del Estado: ambos establecidos en el Decreto N°5, de 2021 (que modifica el Decreto N° 12, de 2018, del Ministerio de Hacienda (https://www.bcn.cl/leychile/navegar?idNorma=1163311&idParte=10256530) que tiene un objeto más amplio, pues pretende "asesorar al Presidente de la República en el análisis y evaluación de las políticas, planes y programas que compongan la agenda de modernización del Estado; formular recomendaciones sobre tales materias; someter a su consideración, propuestas de reforma estructural o institucional para ser llevadas a cabo como iniciativas de ley o dentro de las competencias que en materia de organización interna le confiere el ordenamiento jurídico; y dar respuesta a las consultas que dicha autoridad le formule" (art.2).
2.Comité Interministerial de Ciberseguridad: el Decreto N° 533, de 2015 (modificado por el Decreto N°579, de 2020 creó el Comité Interministerial de Ciberseguridad, "...cuya misión es proponer una política nacional de ciberseguridad, sugerir alternativas de seguimiento a su avance e implementación, y asesorar en la coordinación de acciones, planes y programas en materia de ciberseguridad de los distintos actores públicos y privados en la materia."
Resulta claro que este último tiene como finalidad tratar temas específicos de ciberseguridad, pero no abarca materias de identidad digital o interoperabilidad.

→Materialization of Governing Governance: an entity (Agency, Ministry, or other) that channels and governs State-level initiatives in a cross-cutting manner. For this, an institutionality is required that has binding cross-cutting powers to define models, legal regulatory frameworks, technical frameworks, and support regarding cross-cutting technological enablers such as Digital Identity, Interoperability, and cybersecurity.

→Materialization of Executive Governance: an entity that carries out the implementation, support, maintenance, and operational continuity of the defined cross-cutting solutions and technological enablers.

4. Regulatory Framework for Interoperability and Digital Identity in Chile Today

4. 1. Interoperability

Currently, our country does not have a specific general regulation on interoperability, even though, within the Administration, information transfers have been based on the principle of cooperation that governs public bodies, following DFL 1/DFL 1-19653,[33] of 2001, which establishes the consolidated, coordinated, and systematized text of Law No. 18.575, the constitutional organic law on the general bases of the State Administration.

On the other hand, the enactment of Law No. 19.799, on electronic documents, electronic signatures, and certification services for such signatures, brought about a significant change to this legal framework, as one of its technical provisions introduced the concept of interoperability, determining obligations and the entity responsible for establishing standards.

Subsequently, Law No. 19.880, which establishes the Bases of Administrative Procedures governing the actions of State Administration bodies, incorporated certain guiding principles that served to facilitate data transfers, but always from a cooperative perspective. Only the enactment of Law No. 21.180 represented a transcendental change, as will be explained.

Law No. 19.880, which establishes the basis of Administrative Procedures governing the actions of State Administration bodies

[33] "Artículo 5º.- Las autoridades y funcionarios deberán velar por la eficiente e idónea administración de los medios públicos y por el debido cumplimiento de la función pública.
Los órganos de la Administración del Estado deberán cumplir sus cometidos coordinadamente y propender a la unidad de acción, evitando la duplicación o interferencia de funciones."

Incorporates, the principle of no excuse in Article 14, by establishing in its second paragraph: *"If an Administration body is required to intervene in a matter that is not within its competence, it shall immediately send the relevant information to the authority that should handle it according to the legal framework, informing the interested party of this."* In this way, it establishes the obligation to interoperate information (in a broad sense).

In addition, it incorporates as a right of individuals in their relationship with the Administration, the exemption from presenting documents that are already in its possession (art. 17 letter d) [34]

Decree No. 14, 2014, of the Ministry of Economy, Development and Tourism, Amends Decree No. 181, 2002, which approves the Regulation of Law No. 19,799, on Electronic Documents, Electronic Signature, and Certification of said signature, and repeals the decrees indicated.

The aforementioned technical standard of Law No. 19,799, on Electronic Documents, Electronic Signature, and Certification Services of said Signature, was the first regulatory body to establish the power of the General Secretariat of the Presidency Ministry to propose the technical standards that the organs of the State Administration must follow to guarantee interoperability in the use of electronic documents, among other aspects. In this way, the focus of this regulation was on the interoperability of electronic documents between organs of the State Administration (art. 47).

Law No. 21,180, on Digital Transformation of the State

The enactment of this law changed the paradigm in terms of interoperability, as its establishment was determined as a principle of electronic means (new art. 16 bis of Law No. 19,880) and a standard of electronic record management platforms (modified art. 19 of Law No. 19,880).[35] In this way, interoperability is, for the first time, a mandatory principle in the interaction between organs of the State Administration, and it goes beyond electronic documents, as the law refers to electronic means.[36]

Thus, the legislator enhances the transfer of information within the Administration, an idea that is also reflected in Article 24 bis of Law No. 19,880, which states: *"Following the principles of interoperability and cooperation, in any administrative procedure, the*

[34] Art. 17 letra d): "Eximirse de presentar documentos que no correspondan al procedimiento o que emanen y se encuentren en poder de cualquier órgano de la Administración del Estado. En este último caso, dichos documentos deberán ser remitidos por el órgano que los tuviere en su poder a aquel que estuviere tramitando el procedimiento administrativo"

[35] El art. 16 bis lo define como:"El principio de interoperabilidad consiste en que los medios electrónicos deben ser capaces de interactuar y operar entre sí al interior de la Administración del Estado, a través de estándares abiertos que permitan una segura y expedita interconexión entre los mismos."

[36] Si bien la ley no define medio electrónico, si se hacen referencias en la Historia de la Ley, donde se definieron como: "Son las formas a través de las cuales los documentos o los insumos electrónicos se entregan. Puede tratarse de un video, de un documento electrónico, de un audio o de datos de una base de datos. Esta información puede ser almacenada en un expediente electrónico y ser guardada e integrada en un procedimiento administrativo." Disponible en Primer Informe de la Comisión de Gobierno Interior, Nacionalidad, Ciudadanía y Regionalización, de 26 de junio de 2019.

State Administration bodies that have documents or information regarding matters within their competence, which are necessary for their knowledge or resolution, must send them electronically to the body processing the respective procedure, upon request."

4. 2. Digital Identity

Our country also does not have a specific regulation for digital identity as a whole, but rather it refers to regulations (one of which has already been repealed and another one is in progress) on authentication and electronic signature, as described below.

Law No. 19,477, of 1996, which approves the Organic Law of the Civil Registry and Identification Service.

Article 4, recognizes as a function of the Service to establish and register the civil identity of individuals and issue the official documents that certify it.

In this sense, Article 33 No. 5 of the mentioned regulation establishes an obligation of the Civil Officers "...to supervise the correct issuance of identity cards, passports, and other identification documents processed in their Office."

Law No. 19,799, of 2002, on Electronic Documents, Electronic Signature, and Certification Services for said signature.

Article 12, section e) of this law states that the electronic signature certification service provider should verify the identity of the applicant when granting advanced electronic signature certificates. For this purpose, the provider will require the personal and direct appearance of the applicant or their legal representative, if it is a legal entity, before themselves or before a notary public or civil registry official. This article serves as the basis for Decree No. 24 of 2019, issued by MINECON, which will be discussed later.

This law, as its name indicates, is the only one that thoroughly regulates all issues related to electronic signatures in Chile.

[Repealed] Decree No. 77 of 2004, issued by the Ministry of the General Secretariat of the Presidency, which approves the Technical Standard on the efficiency of electronic communications between government agencies and between these and citizens; repealed by Decree No. 14 of 2014, issued by the Ministry of Economy, Development, and Tourism.

Scope of application:

→Communications made through electronic means.
→Taking place between government agencies and between these and individuals.
→In all areas not regulated by other specific legal, regulatory, or administrative norms.

References to authentication:

→The first mention was made in Article 4: to the extent that a public service interacts through a website with individuals (natural and legal persons) and there is a home page associated with a specific Internet address (URL), the government agencies must declare the formats and means compatible with their systems to send emails and/or authenticating and accessing the site.

→On the other hand, Article 11 established that to protect the confidentiality of information in communications, an authentication or access control mechanism could be used for the email addresses that contained the responses provided by the State Administration to individuals.

Supreme Decree No. 83, of 2005, of the Ministry General Secretariat of the Presidency, which approves the Technical Standard for the Government Agencies' security and confidentiality of electronic documents.

Defines "authentication" as the process of confirming the identity of the user who generated an electronic document and/or who uses a computer system (literal a] of article 5)

On the other hand, letter k) of the aforementioned article conceptualizes the "Formal authentication identifier" as a technological mechanism that allows a person to prove their identity using electronic techniques and means.[37] Later, it states that the use of this mechanism is essential for the use of electronic signatures.

It also indicates that the security of an electronic document is achieved by guaranteeing - among other things - its feasibility of authentication, understood as one of the essential attributes of the document.

Decree No. 14, of 2014, of the Ministry of Economy, Development and Tourism, Amends Decree No. 181, of 2002, which approves the Regulation of Law No. 19,799, on Electronic Documents, Electronic Signature, and the Certification of said signature, and repeals the decrees indicated.

[37] Art. 17 letra d): "Eximirse de presentar documentos que no correspondan al procedimiento o que emanen y se encuentren en poder de cualquier órgano de la Administración del Estado. En este último caso, dichos documentos deberán ser remitidos por el órgano que los tuviere en su poder a aquel que estuviere tramitando el procedimiento administrativo"

In its transitional provisions, in section 1.2 on Technical Standards for Electronic Communications, it makes a vague reference to the forms of access to electronic communications, specifying in subparagraph b) that it is the responsibility of the State Administration bodies to take security measures to prevent interception, obtaining, alteration, and other unauthorized forms of access to their electronic communications. It states that all of this must comply with the technical standards established in Supreme Decree No. 83, of 2005, of the Ministry General Secretariat of the Presidency.

Decree No. 24, of 2019, of the Ministry of Economy, Development, and Tourism, which approves the Technical Standard for the provision of advanced electronic signature certification service.

In its considerations, it defines ClaveÚnica (unique key, a kind of personal password) as a digital identification mechanism that allows users to prove their identity on digital platforms, as the Civil Registry and Identification Service verifies that the digital identity corresponds to a specific person, validating it against its database. Furthermore, it establishes that ClaveÚnica is a digital mechanism for verifying the identity of the applicant for an advanced electronic signature certificate, in the terms required by article 12 letter e) of the signature law.

[In process] Technical Standard for Authentication, derived from the Digital Transformation of the State Law.

Establishes ClaveÚnica as the official authentication mechanism for stakeholders' access to electronic platforms of the Administration.

The enrollment process for ClaveÚnica and the customer service for individuals in this regard depend on the Civil Registry and Identification Service.

States that it is an Official Authentication Mechanism administered by the Ministry General Secretariat of the Presidency through its Division of Digital Government, which validates the identification data of individuals based on the OpenID Connect standard, whose authentication factor is a password created and managed by the individual, linked to their national unique role (RUN or ID National Personal Number)). It allows the enablement of ClaveÚnica for State Administration bodies, the platform infrastructure, monitoring its proper functioning, and validating identification data. On the other hand, it determines that the Tax Key will be the authentication mechanism for legal entities and entities and associations without legal personality.

However, it establishes the possibility of creating new authentication mechanisms by State Administration bodies, as long as they meet the technical requirements established in the same regulation and are validated by the Division of Digital Government.

5. INTEROPERABILITY WORK ENVIRONMENTS

Interoperability is the ability for organizations to interact to achieve common goals that are mutually beneficial and have been previously and jointly agreed upon, by sharing information and knowledge between organizations through the institutional processes they support, through the exchange of services, data, and/or documents between their respective ICT systems (European Commission, 2010). It is an approach to adding value to the provision of services in an interoperable manner.

Government interoperability is a requirement to enable digital communication and automated information exchange between public administrations, private companies, and non-governmental organizations that require interaction with the State, to achieve a single digital market.

Over the past 20 years in Chile, the conversation regarding interoperability has mainly been related to interoperability between government agencies. Some interoperability initiatives between private sector entities and the public sector, or between private sector entities, have led to specific initiatives, such as EDI (Electronic Data Interchange) models for the Exporter/Importer sector in the 1990s and some information exchange initiatives within the financial industry.

But without a doubt, Chile lacks a systematic approach that, in the various indicated dimensions, allows for the establishment of national initiatives that generate opportunities for multisectoral collaboration. This is although there are processes that interoperate, albeit in a limited manner, between institutions.[38] [39]

5.1 Interoperability Dimensions

Following the European framework for interoperability[40] and the publication of digital governance and governmental interoperability by ECLAC,[41] four levels or dimensions of interoperability are determined:

[38] https://www.latercera.com/opinion/noticia/interoperabilidad-un-nuevo-escenario-para-la-modernizacion-del-estado/DMKBEH4IWJE7BPIM5XFTMZU6JM/

[39] https://digital.gob.cl/plataformas-transversales/

[40] Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52017DC0134&from=LT#:~:text=El%20Marco%20Europeo%20de%20Interoperabilidad%20es%20un%20enfoque%20concertado%20con,principios%2C%20modelos%20y%20recomendaciones%20comunes.

[41] A. Naser (coord.), "Gobernanza digital e interoperabilidad gubernamental: una guía para su implementación", Documentos de Proyectos (LC/TS.2021/80), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2021.

→Legal or juridical interoperability: Consists of ensuring that organizations operating under different legal frameworks, policies, and strategies can work together. Clear agreements must exist on how to address differences in legislation, including the option to adopt new legislation.

The first step is to carry out "interoperability checks" by examining existing legislation to identify obstacles to interoperability. This includes identifying contradictory requirements for similar or identical institutional processes, outdated security, and data protection needs, etc. The coherence of legislation must be assessed to ensure interoperability. Proposed legislation must undergo "digital checks" to:

***Ensure that it not only aligns with the physical world but also the digital world;**

***Identify obstacles to digital exchange; and**

***Determine and evaluate the impact of ICT on stakeholders.**

This will facilitate and increase the potential for reusing existing ICT solutions, thereby reducing costs and implementation time.

→Organizational interoperability: means that services are available, easily identifiable, accessible, and user-centered. It has two components:

i. Alignment of institutional processes: All public institutions that contribute to the provision of public services must have a global understanding (end-to-end) of the institutional process and their role within it.

ii. Institutional relationships: Structure the relationship between service providers and their consumers. It requires finding instruments that allow for formalizing mutual assistance, joint action, and interconnected institutional processes, such as Memorandum of Understanding (MoU) and Service Level Agreements (SLA) between participating public administrations.

→Semantic interoperability: Ensuring that the format and exact meaning of exchanged information are understood and preserved in all exchanges between parties, i.e., "what is transmitted is what is understood." Semantic and syntactic aspects:

The semantic aspect refers to the meaning of data elements and their relationship. It includes creating vocabularies and schemas to describe data exchanges and ensuring that all communicating parties understand data elements in the same way.

The syntactic aspect refers to the description of the exact format of the information to be exchanged in terms of grammar and format.

A starting point for improving semantic interoperability is to perceive data and information as a valuable public good. Agreements on reference data in the form of taxonomies, controlled vocabularies, thesauri, code lists, and reusable data structures and models are key requirements for achieving semantic interoperability.

→**Technical interoperability:** It encompasses the applications and infrastructures that connect systems and services. It includes elements such as interface specifications, interconnection services, data integration services, data presentation and exchange, and secure communication protocols.

The IDB (2019) complements this domain with the following sub-dimensions:

***Institutional architecture:** implementing software technology in a structured and organized manner, with a focus on governance and with the clear purpose of meeting established objectives and ensuring software development links between multiple areas of an institution, or between institutions, both within and outside of IT.

***Technical standards:** a set of requirements, specifications, guidelines, or characteristics that can be consistently used to ensure that the information technology to be implemented and the processes conform to their purpose. Standards provide a common language and a set of expectations that enable interoperability between systems and/or devices. These include standards for exchange, transmission, messaging, security, and privacy. They include aspects of the methodology for developing institutional architecture, as well as agile methodologies for project management and the so-called DevOps as an innovative way of developing software + information technology operations.

***Operation and maintenance:** developing optimal management, operation, monitoring, and maintenance processes to ensure availability, continuity, and security under the established service level agreements between the parties.

***Computer equipment and access networks:** infrastructure elements necessary for the deployment and execution of programs, platforms, application servers, and containers, as well as execution environments, packaged applications, virtual machines, etc., that are found in the hardware and are necessary.

***Communication networks:** Understanding how networks are configured and established to align service levels and continuity plans and adapt them to strategies already conceptualized in other domains.

***Data management:** includes, although not exclusively, its collection, visualization, storage, exchange, aggregation, and analysis. The central concept of data management is responsibility, which corresponds to a duly appointed administrator, who is responsible for ensuring the proper use of information and preventing and avoiding incorrect uses. Data is an asset of institutions, and in that sense, they must be treated and protected like any other asset.

The main functions of data management are as follows:

→Data governance: planning, monitoring, and control in the management and use of data.

→Data architecture: design of models, policies, and rules to manage them.

→Data modeling and design: design, implementation, and support of the database.

→Data storage: the function that determines how, how much, and what is stored.

→Data security: everything related to privacy, confidentiality, and appropriate access.

→Data integration and interoperability: function related to their integration and transfer.

→Documents and content: includes the rules applicable to data outside of databases.

→Reference and master data: provides a 360° view of information, its properties, and consent.

→Data storage and business intelligence (BI): everything related to historical and analytical data.

→Metadata: data set that describes the informative content of a resource, files, or information about them. In other words, it is information that describes other data.

→Data quality: refers to the definition, control, and improvement of its quality.

5. 2 Interoperability domains

→**Interoperability governance:** Refers to decisions about interoperability frameworks, institutional agreements, organizational structures, functions and responsibilities, policies, agreements, and other aspects aimed at ensuring and monitoring interoperability.

→**Governance of integrated public services:** Services must be governed to ensure integration, uninterrupted execution, reuse of services and data, and the development of new services.

→**People domain:** The IDB (2019) includes in this domain the set of principles, guidelines, and norms that an institution adopts to help manage personnel. Maintaining an interoperable system requires a highly trained institution. In the operation and maintenance stage, the institution must have a technical team to carry out these tasks and a project team to develop and expand capabilities. It is structured into two subdomains:

* Skills: sufficient and sustainable staffing with the appropriate combination of skills to support the institution in the areas of the social sector. There is a strategic human resources plan to improve their competencies so that they can execute the best international practices.

* Capacity development: training and development activities aimed at imparting knowledge, building specific competencies and capabilities in personnel, and shaping attitudes, all to achieve clear learning outcomes and improve interoperability results.

6. DIGITAL IDENTITY WORK ENVIRONMENTS

A digital identity is a unique representation of a subject willing to carry out an electronic transaction (NIST, 2017). In turn, identification allows relating a set of characteristics of a generalized entity to specify a unique identity in the context of a valuable digital service. The legitimacy of a digital identity is verified through authenticators that grant or deny access to protected data. Once the validity of an identity has been verified, trust relationships are established between entities that interoperate with each other, that is, between digital citizens, private organizations, and public authorities (EU EIF, 2017). A reliable digital identity is also based on the principles of authenticity and non-repudiation security, which seek to guarantee a genuine entity and avoid arbitrary denial or rejection of an action, respectively.[42]

[42] Identidad digital: conceptos y legislación", Asesoría Técnica Parlamentaria, octubre de 2022, Biblioteca del Congreso Nacional. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33658/2/Identidad_Digital_BCN_2022.pdf

There are multiple definitions of Digital Identity, depending on the context. In general terms, we understand Digital Identity as the set of information attributes that allow distinguishing a person, a legal entity, or an information object individually and uniquely, enabling their presence and interactions in the digital world.

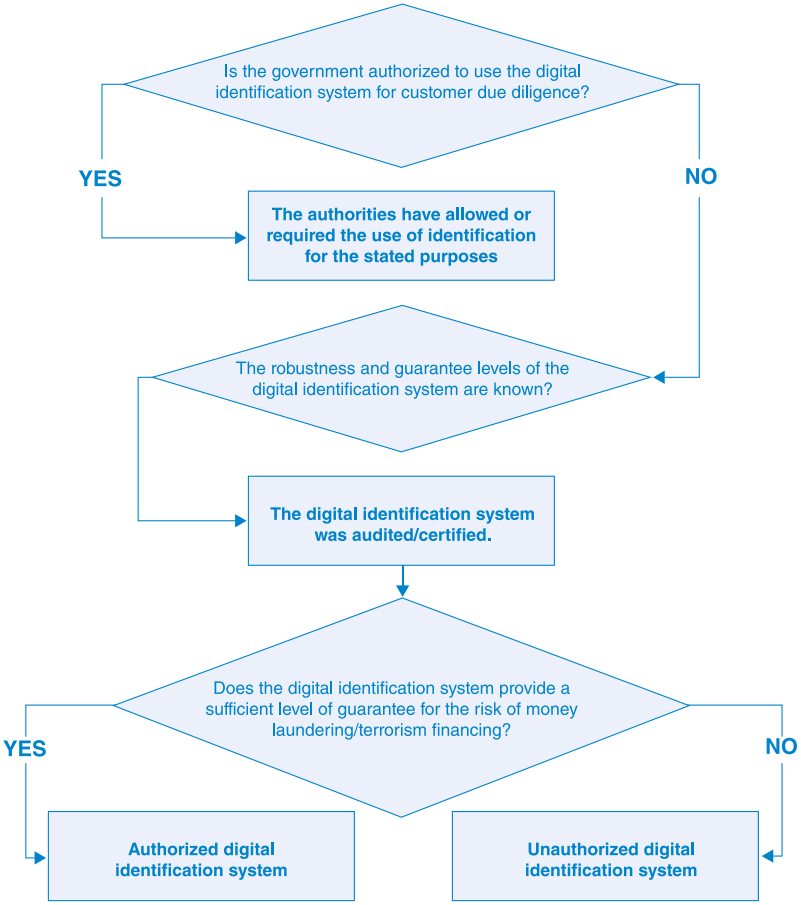
In the case of individuals, digital identity allows, among other services, the application of cryptographic mechanisms to the content of a message or document to prove to the message recipient that the sender of the message is real (authentication), that the sender cannot deny sending the message (non-repudiation), and that the message has not been altered since its issuance (integrity).

Consequently, Digital Identity is a fundamental element for the implementation, among many other services, of digital signatures, whether in the form of advanced electronic signatures, qualified electronic signatures, or what has been called "simple" electronic signatures.

6. 1 About Digital Identity Systems

An identity system provides the requirements that allow for selecting a level of assurance in terms of identification, authentication, and authorization. Identity systems must verify the legitimacy of an identity by combining authenticators, credentials, and assertions, among others. The definition of assurance levels corresponds to regulation. The recognition or classification of a digital identity system must be regulated. The following figure illustrates the generalized phases that a digital identity system must go through for its use at the governmental level (ECLAC, 2022).

The levels of assurance or security determine the processes of identity verification, authentication, or federation. In addition, digital signatures can be integrated into identity verification processes in different forms, for example: simple electronic signature, advanced electronic signature, and qualified electronic signature.



Electronic Signature

Sometimes also called e-signature, it is a legal concept that is the electronic equivalent of a handwritten signature, where a person accepts and validates the content of an electronic message through any legitimate and permitted electronic means. Examples:

***Using a biometric signature.**

***Signing with an electronic pen.**

***Using a credit or debit card at a store.**

***Checking a box on a computer, or typewriter, or applying with a mouse or even the user's finger on a touch screen.**

***Using a digital signature.**

***Using a system that requires establishing a username and password.**

***Using a coordinate card.**

The electronic signature can also have different techniques for signing a document, as follows:

→Secret code or password: the need for a specific combination of numbers or letters, known only by the owner of the document, or what we all use, for example, at ATMs, the well-known PIN (Personal Identification Number).

→Methods based on Biometrics: access to the document is allowed through mechanisms of physical or biological identification of the user or owner of the document; the identification method in this case consists of comparing physical characteristics of each person with a known pattern stored in a database. Biometric readers identify the person by their hands, eyes, fingerprints, and voe.

→Advancement in message encryption, known as cryptography, consists of a system of encoding a text with confidential character keys and complex mathematical processes so that for a third party, the document is incomprehensible if they do not know the decoding key, which allows viewing the document in its original form. This is where two types of cryptography arise:

***Secret key or symmetric:** the parties in both the encryption and decryption processes share a previously agreed common key; it should only be known by both parties to prevent a third party unrelated to the operation from decrypting the transmitted message and thus compromising the security of the system.

***Asymmetric key or public key:** This system has two keys: a private key and a public key. One of them is only known by the author of the document, and the other can be known by anyone; although these two keys are mathematically related through an algorithm, it is not possible to determine the private key through the public key, at least in current technological standards.

An electronic signature creates an audit trail that includes verification of who sends the signed document and a seal with the date and time.

The electronic signature offers security and legal support. In the case of advanced and qualified electronic signatures, in addition to uniquely identifying the signer, they guarantee the integrity of the information contained in the message or document.

The validity of a signature is based on the impossibility of falsifying any type of signature, as long as the signer's key remains secret. In the case of handwritten signatures, the secret is constituted by graphological characteristics inherent to the signer and therefore difficult to forge. On the other hand, in the case of digital signatures, the signer's secret is the exclusive knowledge of a (secret) key used to generate the signature. To ensure the security of digital signatures, they must be:t

***Unique:** Signatures must be able to be generated only by the signer and therefore cannot be forged. Therefore, the signature must depend on the signer.

***Unforgeable:** To forge a digital signature, the attacker must solve math problems of very high complexity, meaning that signatures must be computationally secure. Therefore, the signature must depend on the message itself.

***Verifiable:** Signatures must be easily verifiable by the recipients and, if necessary, also by judges or competent authorities.

***Non-repudiable:** The signer must not be able to deny own signature.

***Feasible:** Signatures must be easy to generate by the signer.

Advanced Electronic Signature

An electronic signature that meets the following requirements:

*It is uniquely linked to the signer;

*It allows for the identification of the signer;

*It has been created using signature creation data that the signer can use, with a high level of confidence, under their exclusive control;

*It is linked to the signed data in such a way that any subsequent modification of the data can be detected.

Qualified Electronic Signature

An advanced electronic signature is created using a qualified electronic signature creation device and is based on a qualified electronic signature certificate.

What is the main difference between an advanced electronic signature and a qualified electronic signature?

Considering the definitions of the eIDAS regulation, the main difference between an advanced electronic signature and a qualified electronic signature are two:

*The qualified electronic signature must be created with a qualified electronic signature creation device.

*The qualified electronic signature must be based on a qualified electronic signature certificate.

What is a qualified electronic signature creation device?

Qualified electronic signature creation devices must comply with the requirements of qualified electronic signature creation devices established in Annex II of Regulation 910/2014.[43]

Requirements for qualified electronic signature creation devices

1. Qualified electronic signature creation devices shall ensure, at least by appropriate technical and procedural means, that:

a) The confidentiality of the electronic signature creation data is reasonably guaranteed;

b) The electronic signature creation data used for the creation of an electronic signature can only appear once in practice;

c) There is reasonable assurance that the electronic signature creation data used for the creation of an electronic signature cannot be deduced and that the signature is protected against forgery by the technology available at the time;

d) The electronic signature creation data used for the creation of an electronic signature can be reliably protected by the legitimate signatory against its use by others.

2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being displayed to the signatory before signing.

3. The generation or management of the electronic signature creation data on behalf of the signer can only be carried out by a qualified trust service provider.

[43] "Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 , relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE" EUR-Lex, European Union. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:32014R0910

4. Without prejudice to point 1, qualified trust service providers that manage the electronic signature creation data on behalf of the signer may duplicate the creation data solely to create a backup of said data, provided that the following requirements are met:

a) The security of the duplicated data sets is at the same level as the original data sets;

b) The number of duplicated data sets does not exceed the minimum necessary to ensure the continuity of the service.

For practical purposes, a qualified device is a hardware device that must be able to guarantee that electronic signatures made with said device are secure and protected against possible counterfeiting. To do this, these devices must be able to use appropriate cryptographic algorithms, key lengths, and hash functions.

What is a qualified electronic signature certificate?

A qualified electronic signature certificate, as defined in Regulation 910/2014 of the European Union, is a certificate issued by a qualified trust service provider that meets the requirements of qualified electronic signature certificates established in Annex I of Regulation 910/2014.

Requirements for qualified electronic signature certificates

Qualified electronic signature certificates shall contain:

*An indication, at least in a format suitable for automatic processing, that the certificate has been issued as a qualified electronic signature certificate;

*A set of data that unequivocally represents the qualified trust service provider issuing the qualified certificates, including at least the Member State in which the provider is established, and

*For legal persons: the name and, where applicable, the registration number as recorded in official registers,

*For natural persons, the name of the person;

*At least the name of the signer or a pseudonym; if a pseudonym is used, it shall be indicated;

*Electronic signature validation data corresponding to the electronic signature creation data;

*Data relating to the start and end of the certificate's validity period;

*The certificate's identity code, which must be unique to the qualified trust service provider;

*The advanced electronic signature or advanced electronic seal of the issuing trust service provider;

*The location where the certificate supporting the advanced electronic signature or advanced electronic seal referenced in point g) is available free of charge;

*The location of the services that can be used to check the validity status of the qualified certificate;

*When the electronic signature creation data related to the electronic signature validation data are stored on a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automatic processing.

The objective of electronic certificates is to validate and certify that an electronic signature corresponds to a specific person or entity, and it can do so because it contains the data of the individual or entity in question: name, ID number, algorithm and signature keys, expiration date, and issuing organization.

To obtain an electronic certificate, it is necessary to personally present oneself at the issuing entity so that it can verify the identity of the person who will be the user of said certificate. A classic example of a digital certificate is the one contained in the National Identity Document (DNI), although there are also digital certificates that are stored in software files.

Advantages of advanced electronic signature compared to qualified signature

Due to the requirements that an electronic signature must meet to be considered qualified - it must be created using a qualified electronic signature creation device and be based on a qualified electronic signature certificate - it is difficult to use this type of signature to identify the user in those procedures or transactions where ease, immediacy, and above all, mobility are paramount.

Currently, the majority of the population does not have a qualified device or a qualified signature certificate, so requiring their use to sign contracts, documents, or user registrations is a clear barrier that can interrupt the course of any type of transaction.

For all these reasons, the use of qualified electronic signatures is more restricted to the public administration sphere. Most companies that use electronic signatures opt for the advanced solution, as it allows them to operate with total security in the online environment and identify their customers or users with all legal guarantees.

Base features of advanced electronic signature

→Allows to identify the signer, as we collect a series of data that are unequivocally associated with the signer during the signing process: email, geolocation, and biometric data of the graph when the device allows it, among other data.

→It is possible to detect any changes made to the signed document, thanks to the use of a public/private key system for both the signed document and the probative document, which allows us to encrypt all the generated documentation and guarantees the integrity of the data at all times.

→Links the generated documentation to the signer and their data, providing a hash system and unique key that is directly related to the signer.

→It is created through means that are under the control of the signer: the signature is generated directly from the signer's device and can only be accessed through private accounts.

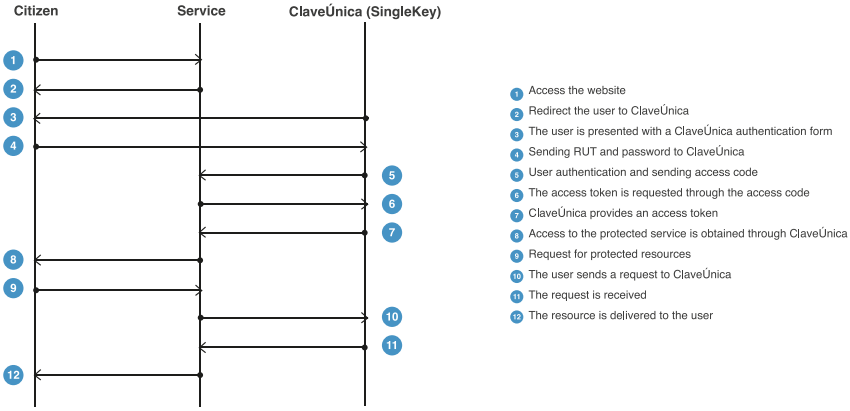
6.2 National context and international use cases

According to Law 19.477, we understand that the civil identity of individuals can be accredited by a centralized public body called the Civil Registry and Identification Service. However, interoperability includes not only natural persons but also legal persons or entities, as well as international identities. Furthermore, interoperability integrates digital processes to expand the exchange of information between multiple local and global actors (Naser, 2020).

Thus, Laws 19.799 and 10.886, which regulate the use of electronic signatures, such as the digital processing of judicial procedures, are not designed for international or cross-border exchange. From the perspective of Law 19.799, the principle of non-repudiation is provided by an advanced electronic signature where multiple cryptographic elements participate, such as a digital certificate, and private and public key. Now, as can be seen, the advanced signature has been directed towards the exchange of electronic documents specific to the State Administration. Thus, the simple electronic signature is implemented as a mechanism to establish sufficient security interactions: user and password, or Unique Key (SEGPRES, 2004; SEGPRES, 2005).

The unique key (Claveúnica) system is based on OpenID Connect technology, which is a standard protocol that allows for authenticating and/or authorizing identities to obtain a protected resource. It allows for three flows for authentication, of which the Authorization Code Flow is used. After the user is identified in the Civil Registry and Identification, it associates an access code that can be changed for a logical access token that has an expiration time. The following sequence diagram summarizes the authentication and authorization process of the Unique Key.

ClaveÚnica

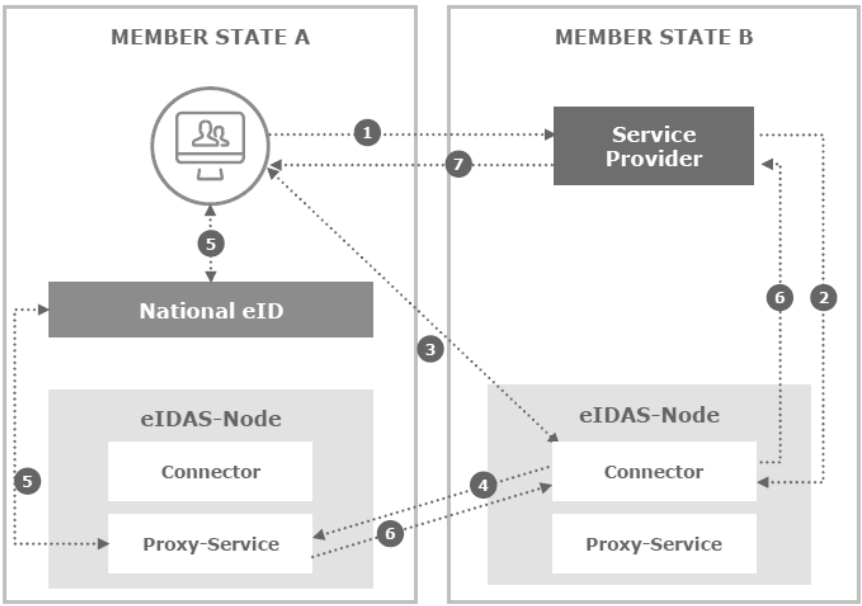


European Case

The European Union (EU) is an international community made up of 27 member states and was established in 1992. The EU is founded on a democratic and representative model, with separate powers in legislative, judicial, and executive entities. The projected growth rate of the EU's gross domestic product is 4.3% for 2022.

The framework for Electronic Identification and Trust Services, eIDAS (EU/910/2014), began its adoption in 2014. The objective of the eIDAS regulation is to securely interoperate among the multiple member states and thus achieve the benefits of a unified digital economy. By 2030, it is expected that eIDAS will provide a digital identity for 80% of all EU citizens.

The implementation of eIDAS involves a single point of contact per member state (national eID), and consequently, cross-border interoperability occurs in a network of eIDAS nodes, complementarily. Each node (eIDAS-node) consists of a connector and a proxy or middleware service. In the following figure, we note that a citizen of Member State A requests an electronic document from Member State B, and does so through a certain service provider who must verify if the applicant's identity is legitimate. The associated node in locality B receives the request and interacts with a node in locality A that redirects the query to the corresponding national node. Finally, it is the national node that is the central entity and custodian of the identity that directly confirms with the applicant and citizen authorizing the request from another Member State.



national eID node scheme allows for mutual recognition among members, and therefore, each state proposes a scheme in line with the technical specifications defined by the ENISA Cybersecurity Agency (526/2013/EC), which are published by the technical committee of ETSI TC ESI. By 2019, 77% of all participating countries had fully implemented eIDAS in their national legislation, which came into effect in 2018.

The identity validation process establishes a relationship of trust that is built on an interoperable public key infrastructure (PKI), which consists of a set of technical standards and services that facilitate the use of encryption or asymmetric cryptography. PKI management includes the issuance of digital certificates, key management, certificate renewal and revocation, and registration of authority, among others.

The framework aligns with the regulation of personal data processing to provide levels of assurance or security according to the risk of the data being accessed (REGULATION (EU) 2016/679 Art. 32). This level (Level of Assurance, LoA) defines three levels of electronic identification: Low, Medium or Substantial, and High (ISO/IEC 29115:2013).[44] The certification of each level encompasses the processes of authentication, verification, and proofing, with the highest level being equivalent to the highest degree of certainty and credibility.

Finally, the European legal framework associates each type of electronic signature with a different level of security.

*Simple electronic signature: does not allow for unique identification of the signer.

*Advanced electronic signature: allows for unique identification of the signer.

*Qualified electronic signature: allows for unique identification of the signer, but requires a qualified electronic signature certificate and a qualified signature creation device.

Due to this hierarchy of signatures based on their levels of security, it is assumed that electronic signatures according to European regulations also comply with US laws, as long as a North American federal law does not impose specific technical characteristics beyond what is defined in the UETA Act and the E-Sign Act.

Estonia Case

Principles of Estonian Identity

*The state is solely responsible for identifying individuals.

*Management is centralized.

*Each person must have one and only one legal identity.

*The link between the physical document and the digital certificate is unambiguous and publicly verifiable through a fundamental element in the Estonian system: the Personal Identification Code (PIC), which was implemented in 1992.

The PIC is an 11-digit number. It contains personal information (gender and date of birth), unlike other countries where the identity number is completely sequential and therefore does not contain any personal information. The PIC is assigned when a person registers in the Population Register.

Digital identity systems or schemes are grouped into three types: low-level security, based on public key infrastructure (PKI), and blockchains.

[44] ISO/IEC 29115:2013, Joinup, Interoperable Europe. European Commission. Disponible en: https://joinup.ec.europa.eu/collection/ict-standards-procurement/solution/isoiec-291152013-information-technology-security-techniques-entity-authentication-assurance

Low-level security digital identity systems use means such as password cards and PIN calculators. Despite the insecurity of these schemes, they are the ones that prevail in the digital world. Name and password authentication prevails in social networks. Unfortunately, many countries and large service providers only offer schemes of this type.

PKI-based digital identity systems are built using asymmetric cryptography. A pair of cryptographic keys are used: the public and private keys. The public key is managed by the identity provider. Systems differ in the methods of storing private keys. The most common are schemes in which the private key is stored on the chip of a digital identity document or on a SIM card of a mobile phone (these schemes are used in Estonia). This ensures the protection of the key by its owner.

Canada Case

In summary, the minimum requirements established by the Canadian model to establish levels of identity assurance are shown in the following table.

Requerimiento	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Unicidad	o Definir información de identidad o Definir contexto			
Evidencia de identidad	No hay restricción sobre lo que se proporciona como evidencia	Un ejemplo de evidencia de identidad	Dos casos de evidencia de identidad (al menos uno debe ser una prueba fundamental de identidad)	Tres casos de evidencia de identidad (al menos uno debe ser una prueba fundamental de identidad)
Precisión de la información de identidad	Aceptación de la autoafirmación de la información de identidad por parte de un individuo	La información de identidad coincide aceptablemente con la afirmación de un individuo y la evidencia de identidad, y Confirmación de que la evidencia de identidad proviene de una autoridad apropiada	o La información de identidad coincide aceptablemente con la afirmación de un individuo y de todos los casos de evidencia de identidad Y, o Confirmación de la evidencia fundamental de la identidad, utilizando una fuente autorizada, y o Confirmación de que la evidencia de identidad de apoyo proviene de una autoridad apropiada, utilizando una fuente autorizada Siempre que no se pueda aplicar nada de lo anterior:	
			o inspección por parte del examinador capacitado	
Vinculación de la información de identidad con la persona	Sin Requerimiento	Sin Requerimiento	Al menos uno de los siguientes: o confirmación basada en el conocimiento o confirmación biológica o de características de comportamiento o confirmación del árbitro de confianza o confirmación de posesión física	Al menos tres de los siguientes: o confirmación basada en el conocimiento o confirmación biológica o de características de comportamiento o confirmación del árbitro de confianza o confirmación de posesión física

6.3 Criteria of a Digital Identity System

We know that a digital signature is derived from cryptographic mechanisms that are applied to the content of a message or document to demonstrate to the recipient of the message that the sender of the message is real (authentication), and that they cannot deny sending the message (non-repudiation), and that the message has not been altered since its issuance (integrity).

The digital signature is therefore a fundamental part of advanced electronic signatures and qualified electronic signatures, but not of simple signatures. The digital signature is also legal, although it does not have a legal nature, in the sense that its objective is not to attest to an act of will on the part of the signer, but only to encrypt the data of a document to provide it with greater security.

With the advent of the digital economy, interactions and transactions that until now were only carried out in person are beginning to be executed through interconnected information systems. Hence the need to take into account the digital identity of each person so that they can be identified and authenticated, obtain permissions to access certain information or physical resources (for example, access to an area), and carry out transactions through the Internet or private networks.

In the digital economy, it is necessary to identify people remotely, without physical interaction, in most cases without prior knowledge of the other party, and often with a computer being responsible for executing the process. As a result, identity management entails challenges in terms of privacy, data protection, and new fraud risks, as well as the need to review and adjust governance schemes, legal frameworks, and technologies that may be becoming obsolete.

Digital identity can be classified into two categories:

***Legal Digital Identity:** needs to be linked to the legal identity of a natural or legal person. It is necessary, for example, to carry out transactions with the government or regulated financial institutions.

***Simple Digital Identity:** does not need to be linked to a physical legal identity. It is used, for example, to connect to social networks.

Legal Digital Identity

It is reflected in what is known as fundamental identity documents (birth certificates for natural citizens, immigration records for legal citizens or residents, or national identity documents in both cases). From these documents, functional identity documents (passport, driver's license, etc.) and legal digital identities can be generated.

One of the most common forms of digital identity is a username. In the case of legal digital identity, it is this username that is linked to a physical identity. The linking occurs at the time of enrollment.

Every identity system has three basic types of actors (Deloitte, 2016):

*Service users, who obtain an identity to comply with regulations and carry out transactions.

*Identity providers, who capture and store the attributes of users' identities, ensure that they are true, and complete transactions on their behalf of them.

*Service providers (basically, companies and the government), who rely on identity providers to comply with the KYC requirement (know your customer), in all cases where best practices advise it or regulations require it.

Identity Systems Management

Combines processes and technologies that enhance the use of people's identifying data, and requires:

*a governance model and a business model;

*an appropriate and up-to-date legal framework;

*simplification and standardization of processes and systems;

*establishment of interoperability mechanisms that facilitate coordination between different organizations;

*and promotion and coordination of the identity usage ecosystem.

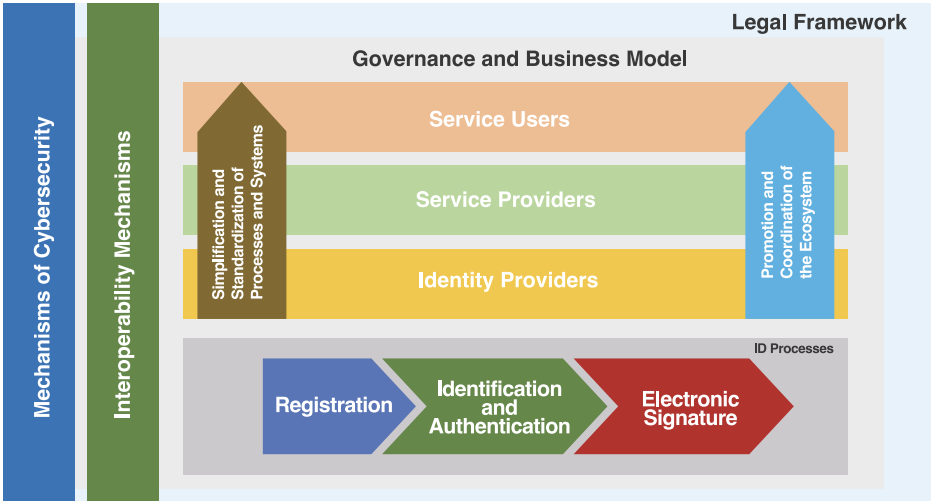
Identity Systems Processes

***Registration in a digital identity system.** A user is created in the system and assigned a digital credential. Enrollment can be done in person or online. In the first case, a commitment of responsibility for the use of digital identity is usually signed. In the second case, it is common to include a confirmation step through a link or a code sent to the user's email or phone.

***Identification and authentication.** This takes place when attempting to access an information system. People are identified using a physical or digital credential, and through authentication, it is verified that the person is who they claim to be.

***Electronic signature.** It is a computer mechanism that allows demonstrating the authenticity of a document or message.

Management of Digital Identity System



Authentication is a key process in the digital world. Historically, it has been based on three elements (factors) that are used to improve the robustness and security of the method, namely:

*Something the person knows: a password or the answer to a personal question.

*Something the person is: fingerprint, iris, face, or voice biometrics.

*Something the person has: an identification card or credit card, a digital certificate.

A digital certificate is a digital file that serves similar functions to a physical identification card in the digital world, including the person's signature. Therefore, the file contains the person's identification and their public key. It is part of the mechanism that the owner can use to sign information packages (documents).

Best practices indicate that, for high-risk operations, a combination of at least two of these elements should be used. Among the most recent innovations in authentication, the adoption of complementary adaptive security mechanisms can be mentioned for some online services, based on the users' history (their browsing profile, geolocation, social media usage profile, etc.).

Digital signatures are performed through digital certificates and not only allow consent to the content of a document or message but also ensure its integrity and non-repudiation of the signature.

In the public sector of Latin America and the Caribbean, the level of development of online transactions is very low. Among the main causal factors for this low level of development, the following can be mentioned:

*The limited possibilities of using certificates, due to the low supply of services that accept digital signatures and the relatively small number of use cases where a digital signature with a certificate is necessary;

*The cost for the user (considerable at the beginning);

*The inconvenience for the user of having to have a reader for the device where the certificate is stored (smartcard, USB token, or other), and

* Various regulatory frameworks that may have been approved to emulate advanced countries, following a trend, rather than taking into account the local situation or realistically managing adoption expectations.

Digital Identity Costs

The main components of the cost of managing digital identity are as follows:

*Implementation and maintenance of the technological support, consisting of databases, the PKI (Public Key Infrastructure) platform, identity data management software, and other cybersecurity measures.

*Enrollment and revocation of certificates. Due to their criticality, in many cases, it is an in-person procedure, with the consequent high cost for both the institution and the citizens.

*Acquisition and maintenance of devices that store certificates (tokens, cards, readers, dynamic key generators, etc.).

*User support (for example, when they forget their password).

6.4 The Chilean case

Chile has a national identification mechanism for citizens and legal entities based on the Unique National Role (RUN) and Unique Tax Role (RUT), defined in the early 1970s. The operating model contemplates that the assignment and administration of RUNs correspond to the Civil Registry and Identification Service (SRCeI), and in the case of RUT, to the Internal Revenue Service (SII).

The model, in general, is a strength of the country, as it allows for a multisystem identification mechanism, used in multiple industries, and being part of the country's daily life. While it facilitates the identification of citizens in both public and private operations, it has some aspects that require improvement in terms of its application and extension.

Some aspects that require improvement to the national identification mechanism are:

*The numbers are not reusable, which can lead to future availability problems (review availability and distribution model among institutions).

*There are challenges related to privacy, a topic that is addressed in legislative proposals under discussion in parliament, related to the Personal Data Protection Law.

Authentication Models

Due to the increasing use of digital services over the Internet, various service providers, both public and private, have had to incorporate identification mechanisms (in many cases based on the National Identifier, the RUN/RUT) and a secret key, in an authentication model based on a single factor (secret key).

In some industries and public services, these authentication models have been extended to models based on the national identifier (RUN/RUT) and two factors (secret key and token, secret key and biometrics, secret key and mobile phone). However, all mechanisms are proprietary to the institution providing the service and have their own enrollment and administration models.

In the case of the public sector, the Chilean government has developed a unique authentication model called Clave Única, which is being incorporated into all government services, with approximately 14 million active citizens to date. The service is made available to the public based on identity certified by the Civil Registry and Identification Service and operated by the Digital Government Division of the General Secretariat of the Presidency.

Currently, it follows a single-factor authentication model (secret key), technologically integrated into an OpenID 2.0 model.

Clave Única has proven to be an important support for the implementation of procedures in the relationship with citizens, especially in their relationship with the government, allowing for the implementation of legally supported procedures. So far, the use of Clave Única by private operators who take advantage of Clave Única services is very incipient, even though there are no technical restrictions on its use.

The situations described above explain the existence of multiple authentication mechanisms specific to each industry and organization (public or private), which are not connected.

This means that users are obliged to manage multiple "digital identities" and "authentication mechanisms". In particular, a hypothesis to be validated is whether the extension or depth of the use of digital services in Chile is hindered by the operation and extension of these authentication mechanisms. And, by the way, having to manage multiple digital identities compromises certain security criteria (unique keys, non-repetition, periodic updates, etc.).

"Unofficial" identities for "non-Chileans"

Being the RUN/RUT the basic identifier for individuals in the various systems in operation in Chile, there are industries that, due to their own operational needs, have generated workarounds or exceptional procedures to address the availability problem of a national identifier (RUN/RUT) for individuals who do not possess said official identifier. This situation applies to individuals not born in Chile (since the current operating model automatically assigns a RUN to every person born in the national territory by SRCeI).

Examples of these industries:

→Public education: Assigns "temporary RUNs" to children of immigrants who make use of the national public education system.

→Public health: Assigns "temporary RUNs" to non-Chilean individuals who require the use of public health services.

→Private pension: Assigns "temporary RUNs" to individuals who work without yet obtaining their Chilean RUN/RUT and require an identifier for the allocation of their pension funds.

Additionally, there is a specific requirement from the Investigations Police (PDI) and services related to immigration and foreign affairs, who have identified and declared the need to have identification and control mechanisms for temporary visitors to Chile.

General needs

Given the background, a national need for a National Identification Strategy is therefore identified, which allows for mechanisms that solve needs at two levels, both for traditional operations and for digital economy operations

→ Identification (that can be used by multiple systems)
→ Authentication (that can be shared among multiple actors)
→ Simple user experience)
→ Various levels of security
→ Multifactor options (two or more factors)
→ Interoperability across multiple industries
→ Compatible with the National Identification Model

Additionally, based on international use cases, it is considered necessary to analyze in detail use cases that justify extending the identification and storage technological capabilities contained in the National Identity Card. Therefore, it is necessary to define a Unique National Identification Model. Along with this, there is a consensus that the basis of the Chilean identification model and repository of public faith in identity management is the Civil Registry and Identification Service.

However, it is necessary to design a "Digital Identity" model that complements it, resolves homogeneously and consistently the requirements of various industries, and meets the needs of the national ecosystem, both public and private actors.

Additionally, the "Digital Identity" model must incorporate an authentication model that allows its extended use by multiple industries in a collaborative model.

A good implementation option for the national authentication mechanism is to extend the Clave Unica (Unique Key) model, incorporating multifactor mechanisms (two or more factors). To do this, it is recommended to explore the models of Estonia, Spain, and Uruguay.

For those industries that have not yet implemented authentication mechanisms in their systems, it is also proposed to extend the use of this Unique Key model at least to implement basic service levels, restricting the model of state responsibility (on operations).

Need for a National Governance Model

Given the previous criteria, the main issue to be resolved is to design a National Digital Identity Governance model that defines:

→Who manages it
→Who uses it, giving authority to whom
→What is the level of responsibility
→What are the technological standards that support it
→What is the underlying infrastructure that supports it
→ Who contributes, finances, and operates said infrastructure

Expansion of the use of the National Identity Card

As part of the National Digital Identity Governance model, the creation of a specific space for discussion on the use of the National Identity Card is proposed, and these definitions should be included in the new bidding bases for the identity system of the Civil Registry and Identification Service.

Some aspects that can be considered in this discussion space are:

→Issuance of "Temporary" Identification Cards
→Exploring the use of the Chip as a Personal Wallet
→Potential frauds that can be carried out through the disabling of security mechanisms and exception handling.

7. GENERATION OF VALUE THROUGH INTEROPERABILITY AND DIGITAL IDENTITY

7.1 Considerations for technical criteria

The provision of the majority of public services requires different government bodies to collaborate to meet the needs of end users in an integrated manner. For this purpose, services must have operational governance that guarantees this integration, uninterrupted exchange of information, reuse of services and data, and the development of new services.

The organizational governance at which institutional processes exchange information, services, and components that support the provision of integrated services must be defined according to legislation, user needs, and new technologies. In this organizational structure of processes and their enabling technologies, formal agreements must be incorporated on topics such as interoperability service levels, change management procedures, operational continuity plans, and data quality.

The Technical Criteria for generating the technology that supports State interoperability are described below:

Basic Infrastructure:

a) Determine the computational requirements of State organizations to manage and exchange information.

b) Assess if the State's computer infrastructure is capable of supporting interoperable services.

*Available services
*Enabled Data Network
*Bandwidth and Quality of Service

c) Considerations regarding the type of Architecture (how the State's digital service network is structured)

*Centralized, Distributed, Federated
*Cloud, Organization-specific servers, etc.

d) Ownership rights over State services at the regulatory level

*Public good (in-house developments)
*Licenses
*Turnkey systems/proprietary.

Infrastructure: Considerations of strategic basals for interoperability

e) Standardization: Definition of standards to be used

*Syntactic Standard
*Semantic standards (thesaurus, standard taxonomy)
*Organizational standards.

f)Identification of Enablers

*Terminology Services
*Object Identification Services and their models (OID: Object Identifier)
*Repositories for specific services defined in the value proposition
*General Identification Services

The above implies having a definition and criteria to determine one of the two options:

1) Criteria for assigning a single interoperability platform
2) Criteria for defining regulations for local system developments or purchases to interoperate based on defined standards and architectures

g) Generation of a model for updating technical criteria

7.2 Value Generation Model

The conception of a modern State where its processes are computerized and the information required from one unit to another can be made available to improve process efficiency, both internally and to facilitate the management of requirements that the population must execute. The above generates value in several dimensions that are those that we name below:

a) Public Value: The services provided by the State are favored in different aspects, highlighting the following:

***Efficiency:** The State improves its ability to execute processes, as the flow of information is continuous. This enables better capacity to make timely decisions, save time in searching, collecting, and analyzing information, and reduce waiting times for services, both for State users and for the general public.

***Quality:** Quality can be measured in two dimensions: quality in the management of information (data); and quality in the service that is delivered. Interoperability allows for avoiding data duplication, double or triple tabulation, and transcription errors, which naturally lead to information damage. On the other hand, having services that provide timely and error-free information improves the quality of processes and therefore the services that the State provides.

***Citizen Satisfaction:** Satisfaction refers to the ex-post impact obtained in response to a request. Another way is to evaluate the user's perception during the journey of their request. Citizens are interested in not wasting time navigating through different government services to find information that allows them to complete a single procedure. In addition, the loss of continuity in the processes that are part of government services significantly affects the perception of the quality of government services. Interoperability shortens process times and makes the citizen's journey in requesting a service simpler and shorter, improving the perception of satisfaction.

b) Social Impacts

***Cohesion and equity:** The OECD (2014) defines the benefits that society can see from the perspective of different actors as the public value that results from the exercise of certain state strategies. One of these values, when the State interoperates, is equity and social cohesion, as it allows the efficiency of the State to reach the entire population equally, reducing the costs of procedures and perceiving a fairer State.

***Security and trust:** By making information interoperable, the principle of transparency begins to be guaranteed, it becomes more difficult not to inform, and it is simpler to compare information, as it can be obtained from various sources. The State becomes more transparent in its processes and before the citizens.

c) Trust and legitimacy: One of the challenges of the State is to gain legitimacy among the population. Security and transparency as a valuable object for the State entail generating trust and legitimacy among the population, which indirectly allows for improving the quality of life of the population and advancing politically and socially in strategies that are more legitimized by the citizens.

d) Perceived value by the population: For the population, value is manifested in the following elements, which are more qualitative than quantitative.

*Cost reduction and better organization for services to people

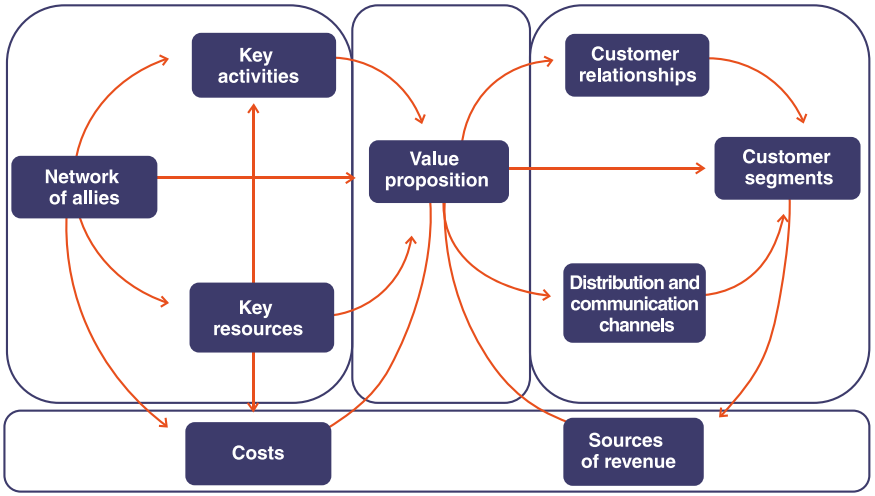
*Greater transparency

*Ease of maintenance and technological evolution

*More organized technological evolution

7.3 Proposal to Generate a Value Model

Considering the reports issued by the following entities: ECLAC, "Digital Governance and Government Interoperability," Alejandra Naser; OECD; Homeland Security, "Communications Interoperability Performance Measurement Guide," 2018; Ministry of the General Secretariat of the Presidency, "Characterization Study of Interoperability in the State of Chile," 2017; IDB (Inter-American Development Bank) (2019), The ABC of Social Services Interoperability: Conceptual and Methodological Framework [online]; European Commission (2020), "The Digital Economy and Society Index (DESI)." The value model proposed by ECLAC is indicated in divisions of the CANVAS model.



Canvas Model of Division, for interoperability value. (Source: "Digital Governance and Government Interoperability, ECLAC)

The model revolves around determining the value proposition, which is not necessarily everything that can be achieved through interoperability, but rather a specific objective that the State determines.

The model must be based on the fact that each organization belonging to the State must define its institutional value proposition, which must be based on the functions it performs and which are weighted by government guidelines.

Then, the value proposition must be nuanced in such a way that it fulfills:

1) Understanding by the citizens of this proposition

2) Identification of strategic services or products

3) Clarity in processes and where technological transformation should be generated

4) Organizational structure following it.

If the mechanisms for strengthening this institutional value proposition are added, and aligned with those of the other organizations that coexist in the State ecosystem, interoperability becomes relevant and contributes to the value of digital government.

7.4 Measurement Indicators

The European experience indicates the criticality of developing measurement indicators within local regulations. In this experience, the following types of indicators are determined:

1) Performance Indicators: Indicate the performance of interoperability strategies (Inputs, Processes, Outputs, Results, and Impacts)

2) Capability Indicators: Measure whether the implementation of interoperability is feasible or not

3) Performance Indicators: Technical, they determine whether the collected data is usable or not.

8- CHANGE MANAGEMENT: KEY TO SUCCESS

In any organizational change process, especially those involving technological components, there are barriers to achieving success in this transformation. That is why it is necessary to address these barriers, analyze them, and take action to prevent them.

It is also necessary to identify the change facilitators, those traits, characteristics, people, and/or situations in the organization(s) that can accelerate or implement the desired change. Most of these barriers or resistance forces come from individuals or organizational cultures.

Through a Change Management Strategy operationalized through an Implementation Plan, it is possible to contribute to reducing this resistance and empowering facilitators to create more favorable conditions for the implementation of projects such as Digital Government, Interoperability, Digital Identity, and Cybersecurity. This strategy should cover both the actors in government institutions, companies, and citizens, to promote a cultural change that is suitable for this new digital way of interacting among the different actors in the country.

Organizations usually make adjustments in terms of personnel, refocusing, training, and integrating new resources that meet the required competencies to manage, administer, and master a change associated with the implementation of the Digital Transformation of the State, resulting in a Digital Government.

The citizen community is more demanding, and the obstacles are not in the technology or its functionality, but in the practices and culture it has. Therefore, that is where the work should be focused.

[45] https://www.cisa.gov/sites/default/files/publications Communications%2BInteroperability%2BPerformance%2BMeasurement%2BGuide_0.pdf

8.1 Need for Change Management

Change Management focuses on the human factor. Its continuous monitoring, evaluation, and improvement in motivational quality generate one of the strongest competitive advantages in any industry.

The implicit objective of Change Management is to increasingly involve the organization's personnel in the entire transformation process, maintain the level of adherence, and increase the level of involvement, facilitating the definition of the best solutions for the realization of the project and achieving the assimilation of the improvements it will bring.

In short, Change Management reduces the risk of failure, accelerates the realization of benefits, and ensures the sustainability of the change over time.

The synergy between the organization's strategy and its capacity for change makes the difference between successful projects and failures.

It is possible to argue that skills are central in the fast-paced world we live in and constitute the way to translate knowledge into effective actions. Building trust in work teams, along with efficient management of networks and commitments, are core aspects to ensure an increase in value.

One relevant aspect to consider in a change process is that resistance to change is not inherently negative; it is a natural predisposition of human beings to move within the security provided by what is known.

Resistance to change is a relationship between the quality of the proposal and the characteristics of those affected by it. We only resist change when we interpret it as a mixture where threats prevail over opportunities.

There is an important responsibility to develop, which is to show the advantages that the change brings to those involved.

8.2 Background for Successful Change Management

Interaction

In any change process, different actors interact, each fulfilling different roles that must be considered in the design. Among these, the following stand out:

* Change sponsors. Their responsibilities include evaluating the consequences of the transition, identifying adaptive requirements, and deciding on changes to implement.

*Change agents. They are responsible for managing the change process, forming the responsible team, and handling the different variables of change.

*Personnel affected by the change. These are the individuals who experience and undergo changes in knowledge, attitudes, and behaviors.

Key aspects

From a component perspective, change management in modernization projects associated with Digital Government involves five key elements that must be present in a change management strategy, namely:

*Communicated Vision: regarding the underlying arguments for this change (modernization, citizen focus, remote service, public value in service, etc.).

*Trained Skills: ensuring that the universe of actors involved in the change (internal and citizen) have the sufficient skills, knowledge, and training required to make use of the resulting change.

* Resources: ensuring the availability of the economic, personnel, and infrastructure means required for the proper implementation and use of the change.

*Incentives: providing motivation that translates into recognition, not necessarily financial, towards the team and the involved citizens (in the latter case, extended service hours, extended deadlines for submission, shorter deadlines for recovery, among others).

*Action Plan: establishing the activities, milestones, responsible parties, and products associated with the implementation project.

Not having any of these components generates some degree of impact on the people involved.

Change in the bureaucratic culture

At the governmental level, with Digital Government, there is talk of a cultural change in public services and their officials, in terms of:

*Putting the citizen at the center.
*Collaborating with other Public Services.
*Generating new capabilities.
*Becoming aware and taking responsibility for the fact that internal tasks and performance affect others (the citizens).
*Modifying the way of working and relating to others for this purpose.

From the cultural dimension, that is, from the dimension of people, it means changes in work practices, and doing things differently. This aspect must be taken into account as another element of the change management plan given its magnitude and effect on the organization and its immediate environment.
Change management must be approached from three key perspectives and/or pillars:

Organizational Impact (Containment)

Assessing the level of impact that a technological initiative will have requires identifying the factors that will hinder and/or facilitate the change, as well as the impacts it will have on the organization(s) and the people involved in its implementation.

The need to follow the following steps to obtain a good situation diagnosis is proposed:

1. Identification of the target group: includes segmenting the audiences impacted by the change project, their stakeholders, and the management level, establishing commitments with the counterpart carrying out the change project. It also seeks to identify those individuals who can become agents of change for the project.

2. Evaluation of organizational climate and culture: includes conducting a diagnosis of the organization(s), understanding the problem, organizational knowledge, and identifying drivers of change, applying tools for measuring work climate, conducting interviews and focus groups to determine the starting point from a cultural perspective.

3. Evaluation and assessment of requirements and gaps: Analysis of the information generated by the change project to understand the existing gaps in the organization(s) between what the project presents and the reality of the organization(s), companies, and citizens in terms of processes, people (roles and profiles), and technology. Identification of new roles and competencies needed for the staff towards the new institutional framework identified by the change project.

4. Identification of internal barriers to change, as well as the skills and competencies (present and absent) required in the team carrying out the change project, to provoke the desired strategic and technological change.

5. Identification of external factors that can facilitate or hinder the development of the change strategy to be implemented in the organization. Political cycles, changes in the leadership of key institutions.

6.Identification of facilitators and detractors that can support or hinder the development of the change strategy to be implemented in the organization. It is crucial to identify the level of impact and influence of the facilitators/detractors of change by the project.

7. Generation of containment actions (detractors) and promotion actions (facilitators).

Knowledge Transfer (Training)

People are considered the main agents of change. If we want them to think, feel, and do something differently, we must address the fear, skepticism, insecurity, mistrust, resistance, ambition, and confusion that may arise in the officials of participating institutions and the users/beneficiaries of the services provided by these institutions when faced with the unknown. In this sense, the field of knowledge transfer must not only address the technical knowledge associated with new tools and processes but also the adaptive components involved in change.

Based on the previous diagnosis, this field takes into account the need to acquire new knowledge, skills, and abilities by the individuals impacted by the Digital Government Project.

The methodological approach should focus on "Knowing How" and "Learning by Doing".

Communication and Dissemination

These should promote the appropriate involvement of all stakeholders in the project (internal and external) and necessarily facilitate the integration of the desired changes into the processes and functions that will be impacted. This is particularly relevant when a technological change is proposed that involves conceptual and practical changes.

A communication and project dissemination plan must be formulated and implemented, which should include at least the following components:

*Identification of stakeholders and construction of Communication Treatment Matrices (strategy)
*Segmentation of stakeholders
*IDefinition of Content (narrative) for each target group
*Mediation of Content
*Design, definition, and enablement of communication channels.
*Definition of Risk Management Strategy.
*Design of Communication Plan
*Execution and Control of the Plan according to Change Triggers.

Each of these components (Containment, Training, and Communication) must be addressed together and as complements from the conception of change projects.

Within the resistances that people frequently present in the face of change processes, at least three categories of groups of people are identified, which in turn make up three Pillars of Change Management:

***Those who do not know** that a change is coming and what it consists of, therefore there is resistance due to ignorance. For these situations, the **Diffusion and Communication Plan** is defined.

***Those who do not want the change**, are those who oppose it for personal, professional, political, cultural, or other reasons, express their dissatisfaction, or discontent, and will not support it. For these situations, the Containment and Case Follow-up Plan is defined.

***Those who cannot**, mainly due to a lack of knowledge, skills, and abilities. For these situations, the **Training and Training Plan** is defined.

8.3 Considerations for a Successful Change Management

The success factor for introducing a successful digital transformation, in which Interoperability and Digital Identity are key, lies not so much in the technological solutions that can be acquired in the market, but 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 relevant to consider some key precepts for this:

***Establish discipline from the origins of projects involving changes**

***Establish adaptive competence as a requirement in the ADP[46]**

***Manage the acquisition of adaptive competencies for change projects in institutions, companies, organizations, and citizens**

***Establish user experience as a hygiene factor in every change project**

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:

[46] ADP: Alta Dirección Pública

Detection of the need for change

Both internal and external factors provoke the need for change, which are detected and analyzed by the change management team, generating a strategy that materializes in support projects. The probable factors of change come from social, regulatory, internal organization, technological (Digital Government), strategic, and political variables.

Initial analysis (diagnosis)

A position is established concerning the desired situation. Specific profiles and situations that may facilitate or hinder a transformation process must be detected and identified. The current state, change projects, and the desired future state are identified. An important aspect to consider is Demand Management, which refers to the efforts that the projects will require from the organization and its team. It should be taken into account that specific efforts will be demanded from certain actors in the organization, who are usually the ones with the most knowledge and the least time available, and who will have to dedicate some hours of their day to the project involving the change.

Stakeholders and Roles

The importance of the commitment of all actors, especially those leading the change process, and their impact on the success or failure of organizational change should be reinforced. Positive/negative leadership characteristics can be mentioned, and two sets of stakeholders can be identified:

***Network of leaders directly involved in the project:** directors, assistant directors, and middle managers related to the change initiatives. Identify collaborators who need to be involved in the leadership of the change process. Establish individual goals, specific objectives, and rewards.

***Stakeholder map:** generated by the Processes department to identify collaborators who need to be involved, ranked according to the impact their participation may have on the process.

Planning:

A plan is identified for each Pillar of Change Management.

→**Communication and Dissemination Plan:** Plans designed for each specific project that the organization is carrying out and that involve changes in actions, roles, and profiles of individuals. They ensure the proper understanding of the projects by the collaborators. They contribute to aligning the organization with change initiatives. They keep the entire organization informed promptly. They contribute to and reinforce the learning process of those involved. The components of this plan include at least:

***Communication Objectives**
***Segmentation**
***Media (Magazine; Flash; Cascades; Meetings; Conventions; Intranet)**
***Messages**
***Frequency**
***Monitoring and Control**
***Feedback**

→Training Plan: includes the planning, implementation, and control of training initiatives. The plan should respond to identifying the training needs of the team that will be impacted by the change in terms of training programs that address both new processes, new tools, and new roles (it should provide both technical and adaptive competencies). The components of this plan include at least:

*Involved Units: Identification - Coordination - Communication - Support
*People: Identification - Recruitment - Control - Monitoring
*Courses: Definition - Validation - Assembly - Control - Monitoring - Data
*Time: Training periods - Key dates - Scheduling
*Technical Aspects: Rooms - Hardware and Software - Presentations - User Manuals

→Containment and Monitoring Plan: The plan must cover, starting from the identification of the team's containment needs that need to be addressed due to the divergence generated regarding the change project, to align them through concrete actions such as mentoring, coaching, or peer support, so that they can integrate into the change process and contribute to its implementation. It includes at least the following actions:

***Proactive Monitoring:**

*Training Plan: Evaluation of the experience, and evaluation of the learning.
*Communication Plan: Evaluation of the means and penetration of the messages.
*Leadership: Monitoring the participation of the organization's leaders.

***Reactive Monitoring:** Analysis and segmentation of incidents or situations reported by the collaborators.

***Maturation Monitoring:**

*Assimilation level: Evaluation of the degree of application of processes and new knowledge.
*Productivity level: How much work has improved due to new knowledge and skills.

***Coaching, Reprogramming, and Retraining.**

9- FUTURE CHALLENGES

9.1 Technological Criteria:

Regarding the criteria for evaluation, design, selection, and implementation of technological mechanisms that account for the aforementioned definitions and work plans, these should consider:

*Maintaining the principle of technological neutrality in the State, in the sense that both the design and implementation of underlying technological solutions should not favor specific brands or technologies from specific providers, tending to prefer technologies that are publicly accessible, based on open standards, and have diverse providers that support their implementation.

*Without prejudice to the above, the scope of dependence that a technological decision may imply and its impact on national security should be duly considered.

*Prioritizing models of technological solutions that allow the national industry to acquire new knowledge, and develop its own capabilities and comparative advantages, strengthening Chile's competitive capacity in a global context.

*Establishing formal and regular mechanisms for reviewing the decisions and designs established in the standards defined for these issues, contrasting the definitions with the state of the art in technological development. For this purpose, periodic and formal reviews (maximum every 18 months) will be established to verify that the technological decisions and criteria taken remain valid and in line with the development of the local and global industry.

*Considering that the technological standards or definitions included in the designs are in line with Chile's technical and human capabilities to incorporate such technologies, verifying the technological absorption capacity by the agents included in each ecosystem.

9.2 Interoperability

Improving the efficiency of the State by simplifying its response to the population, and meeting their requirements, is possible by implementing Interoperability.

In summary, it is a powerful management tool that puts the citizen at the center, promoting best practices and regulations for the development of technologies and technological enablers. Implementing Interoperability involves a political decision, which is supported by the State Modernization Law[47] and the associated timelines for compliance.

[47] Tercera consulta pública Ley N° 21.180, de Transformación Digital del Estado. Norma Técnica de Interoperabilidad. 2021. Gobierno Digital. Gobierno de Chile. Disponible en: https://digital.gob.cl/biblioteca/regulacion/tercera-consulta-publica-ley-n-21180-de-transformacion-digital-del-estado-norma-tecnica-de-interoperabilidad/

There have been multiple attempts at Interoperability in our country, but they have followed their development models, and there is a significant dispersion of systems, policies, and laws that hinder interoperability. We should strive for a universal model, which should be adopted with the conviction that it is the best solution in terms of dimensions, techniques, security, and change management. (See: experience in Uruguay[48] and Colombia,[49] challenges in Argentina,[50] recommendations from ECLAC[51], and X-Road, Interoperability in Nordic countries).[52]

Short-Term Actions

*Identify existing instances where the proposed Governance classifications can be adjusted and operated during a transition period, incorporating governance issues into the specific agenda of the instance and coordinating them with concrete objectives and actions, to generate the necessary practice and culture. In the meantime, the permanent installed capacities can be utilized.´

*Promoting a National Interoperability Law that generates the administrative tools and resources to promote an Interoperability model for the State of Chile, considering an Interoperability architecture based on internationally proven standards, and considering aspects of foreign policy to facilitate cross-border interoperability. This law will regulate the administrative aspects related to the exchange of information between state institutions in a digital and real-time manner, strictly adhering to Data Protection and Cybersecurity laws.

*Creation of the National Interoperability Agency, under the Ministry of Interior, which will articulate Interoperability, assuming the necessary governance to manage the change processes and the generation of norms and regulations.

*Establish a process to disseminate the changes to be faced by Interoperability, and the rethinking of internal management processes in institutions.

*Establish an interoperability adoption schedule aligned with the Modernization of the State law.

*Promote the interoperability standard for its application in both the public and private sectors. Encourage the development of APIs (Application Interfaces) as private developments.

[48] "Qué es la Plataforma de Interoperabilidad" disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/que-es-la-plataforma-de-interoperabilidad

[49]"Marco de interoperabilidad para Gobierno Digital. Agosto de 2019", Gobierno de Colombia. Disponible en https://www.mintic.gov.co/arquitecturati/630/articles-9375_recurso_4.pdf

[50]"Interoperabilidad en Gestión Pública" tesis Claudia Sánchez, maestría en gestión de servicios tecnológicos y telecomunicaciones, Universidad de San Andrés, Argentina, 2018. Disponible en https://repositorio.udesa.edu.ar/jspui/bitstream/10908/16162/1/%5BP%5D%5BW%5D%20T.%20M.%20Ges.%20S%C3%A1nchez%2C%20Claudia.pdf

[51]"Desde el gobierno digital hacia un gobierno inteligente", Biblioguías, Biblioteca CEPAL. Disponible en https://biblioguias.cepal.org/gobierno-digital/interoperabilidad

[52]"Nordic Institute for Interoperability Solutions - NIIS. Disponible en: https://www.niis.org/

Medium and Long-Term Actions:

*Manage the State's Interoperability system, adapting to new requirements arising from technological changes and increasing volumes of interoperated information.

9.3 Digital Identity

Considering the following benefits associated with the establishment of digital identity[52]:

*Those directly derived from the digitization of existing processes that were previously only offered in person (for example, identity verification), and

*Those associated with the emergence of new services and economic activities as a result of the use of digital identity.

To advance in the field of digital identification and trusted services for electronic transactions carried out both in the Chilean and international markets, allowing for legal certainty in countless transactions between individuals, companies, and the State; from a regulatory perspective, the existing systems that not only electronically identify, but also authenticate identity through two factors, must be strengthened, so that those who interact digitally are truly who they claim to be.

Short-Term Actions:

*Strengthen the existing public authentication mechanisms: ClaveÚnica and Clave Tributaria.

*Establish robust legislation on digital identity, with the issuance and management of digital identity in Chile being the responsibility of the Civil Registry and Identification Service. This legislation should include the "digital address" of each citizen, where communication between the State and each citizen will take place.

*Include in this legislation clear rules for the use of Digital Identity by private entities, under the Data Protection Law, currently in the legislative process, as well as Law No. 21.180 on State Modernization.

*This legislation should consider aspects such as technological dependence on providers and national interests, which could be compromised in implementation decisions.

[53] "Identidad digital como habilitante estratégico de la transformación digital del país", 2019, OCDE. Gobierno de Chile. Disponible en https: //digital.gob.cl/biblioteca/estudios/identidad-digital-como-habilitante-estrategico-de-la-transformacion-digital-del-pais/

*For advanced electronic signature, the construction of a national registry of procedures and processes for various industries is proposed, which allows interaction between public and/or private agents, recommends and regulates the gradual and progressive use of digital signature mechanisms, starting from the incorporation of intermediate digital signature to advanced digital signature, depending on the required coverage, technological reality, complexity, availability, and state of the art of the involved processes.

Medium and Long-Term Actions

*Promote an identification and authentication mechanism compatible at a Latin American level, as Europe has been advancing through the eIDAS[53] Regulation. This change would require the regulation of interoperability, as recommended in the point related to this topic.

[54] eIDAS: Reglamento europeo de identificación digital", Electronic Identification (Signicat company). Disponible en https://www.electronicid.eu/es/blog/post/eidas-nuevo-reglamento-de-firma-electronica-en-europa/es

REFERENCES

Grassi Paul A., Garcia Michael E., and Fenton James L. (2017). Digital Identity Guidelines. NIST Special Publication 800-63-3. tu, Estonia. Available on: https://doi.org/10.6028/NIST.SP.800-63-3 (acc. 17/11/2022).

European Union (2017). European Interoperability Framework, Promoting seamless services and data flows for European public administrations. Available on: https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf (acc. 07/08/2022).

Ministerio Secretaría General de la Presidencia (2018). Ley 21.096, Consagra el Derecho a Protección de los Datos Personales. Disponible en: https://www.bcn.cl/leychile/ (acc. 11/08/2022).

Statista (2022). Value of data economy in EU and UK 2016-2020 and 2025. Value of direct, indirect, and induced impacts on the economy. Available on: https://www.statista.com/statistics/1134993/value-of-data-economy-eu-uk/ (acc. 11/08/2022)

IDSA - Identity Defined Security Alliance (2022). Whitepaper: 2022 Trends in Securing Digital Identities. Disponible en: https://www.idsalliance.org/white-paper/2022-trends-in-securing-digital-identities/ (acc. 07/08/2022).

NIIS, Nordic Institute for Interoperability Solutions (2022). European Interoperability Landscape Report. University of Tartu, Estonia. Available on: https://www.niis.org/publications (acc. 11/08/2022).

CEPAL, "Gobernanza Digital e Interoperabilidad Gubernamental", Alejandra Naser

OCDE Homeland Security, "Communications Interoperability Performance Measurement Guide", 2011

Ministerio Secretaría General de la Presidencia, "Estudio de Caracterización de la Interoperabilidad en el Estado de Chile", 2017

BID (Banco Interamericano de Desarrollo) (2019), El ABC de la interoperabilidad de los servicios sociales: marco conceptual y metodológico [en línea]

Comisión Europea (2020), "The Digital Economy and Society Index (DESI)" [en línea].

*Chapter 8_*

National Cybersecurity Forum

PARTICIPANTS IN THE ELABORATION OF THIS TEXT:

- Senator Kenneth Pugh, Michael Heavey, Carolina Muñoz, Julio Cámara, Raimundo Roberts and Tania Yovanovic.

INTRODUCTION

Cyberspace is an ecosystem entirely created by human ingenuity, and it has had a rapid evolution. It is not a reality that replicates the laws of the physical world, as in this environment, rules of coexistence can be built in the face of new situations and challenges, as well as dangers that go beyond virtuality, whose potential effects can severely affect our physical world, our way of life, human rights, and of course, democracy, and freedom.

The concept of cybersecurity arises from how to handle these dangers and challenges, a term that encompasses security within this new ecosystem.
The right to make safe and reliable use of cyberspace and contribute to building digital trust is a shared responsibility among all public and private actors and society as a whole.

In this context, during the year 2022, the Senate of Chile, through the Committee on Future Challenges, Science, Technology, and Innovation, convened over 140 professionals from the academic world, providers, industry, and related experts to form a Cybersecurity Work Team, to analyze and make visible aspects of cybersecurity in our country. The Said work table was organized and worked on 7 relevant topics for several months, and the result is included in this document entitled: "Building Cybersecurity in Chile" which also feeds into the actions of the Digital Transformation Strategy **"Chile Digital 2035."**

Cybersecurity is one of the cornerstones in the processes of Digital Transformation, being a **shared responsibility**, and all measures that lead to necessary cooperation for common security must be promoted.

Its guiding principle is to establish itself as a public-private collaboration environment where knowledge about opportunities and challenges for cybersecurity in cyberspace is shared, generated, and disseminated. The Forum brings together the Academy, the State, Armed Forces, Police, civil organizations, providers, and specialists, who, in an open, transparent, and voluntary participation, will analyze and promote initiatives that allow for the improvement of national cybersecurity in all areas.

To respond to the doubts and concerns associated with a safe digital environment and to articulate a broad collaboration environment in our country, the aforementioned Cybersecurity Task Force suggests creating an entity called the **"National Cybersecurity Forum"**, which will organize experts to address concerns and initiatives in this field, and which will be based in the Senate of Chile.

The advisory role of the Forum will allow for expert opinions to continuously improve legal and regulatory frameworks, supporting the updating of policies and strategies in this field, and serving as a reference for national cybersecurity institutions, as well as permanent support for the Country's Digital Transformation.

In its dissemination role, the Forum will promote Cybersecurity at a national level, supporting and coordinating the development of promotional and educational activities, as well as national participation in international forums on the subject. Promoting a culture of cybersecurity is a necessary process, as is supporting R&D and the creation of a national industry that provides appropriate solutions to our needs.

The creation of this Forum is inspired by the experience of Spain (https://foronacionalciberseguridad.es), whose forum plays an important role as part of the cybersecurity governance in that country.

OBJECTIVES OF THE NATIONAL CYBERSECURITY FORUM

1. Create a permanent public-private collaboration environment to share and generate knowledge about opportunities and challenges for cybersecurity in cyberspace.

2. Propose initiatives to the Executive and Legislative powers to enhance and create public-private synergies in cybersecurity and/or cyber defense, as well as in the Digital Transformation of the State.

3. Analyze, review, comment, and propose draft laws sponsored by a parliamentarian or the Executive, which are processed in the National Congress and require the informed opinions of experts in cyberspace, cybersecurity, and digital transformation.

4. Review, evaluate, and propose updates to the National Cybersecurity Policy.

5. Contribute to identifying the needs of the industry and research centers regarding cybersecurity.

6. Promote R&D and the national cybersecurity industry.

7. Conduct and formulate proposals on the regulatory and normative framework with an impact on cybersecurity, also considering other related disciplines that should be harmonized, such as the Digital Transformation of the State.

8. Support the future National Cybersecurity Agency as an advisory body.

9. Promote proactive studies and reports on new and emerging technologies and analyze their impact on national cybersecurity and digital transformation of the country.

10. Develop initiatives that promote a National Cybersecurity culture.

11. Promote Chile's projection and participation in Latin America in cybersecurity, cyber defense, and digital transformation.

12. Sponsor national and international cybersecurity activities, especially those to be carried out during October of each year, the month of Cybersecurity (Law No. 21.113).

FORMALIZATION OF THE FORUM

In recent years, various initiatives on cybersecurity have been generated both from the public and private sectors. However, it is important to recognize the special concern that the Senate of the Republic has had in these matters.

Unlike the Spanish Forum, which is part of the cybersecurity architecture and is supported by an executive structure that convenes public-private participation, our country is just creating its cybersecurity governance and it is necessary to take steps to articulate collaboration, facilitate legislation, and give a prospective meaning to cybersecurity, as well as to the digital transformation processes of the State.

In cybersecurity matters, the Senate has historically been a promoter and articulator of these issues. Cybersecurity Month originated from a parliamentary motion presented in the Senate, which led to Law No. 21,113 of 2018, declaring October of each year as the national cybersecurity month. Since its creation, this activity has traditionally been inaugurated at the beginning of each October with a special session of the Senate, led by its President.

It is worth highlighting the experience gained by the Senate's Committee on Future Challenges, which has had an important capacity to convene, thus making many significant topics visible beyond politics. In it, they think about the Chile of tomorrow and unite wills for the future of the nation. This is how initiatives such as neural rights, space research, developments in various specialties and their impacts, and certainly a very powerful prospecting tool have emerged.

It is also important to highlight the role of the Senate's Commission on Transport and Telecommunications, which, recognizing the importance of digital transformation, has created instances of participation that go beyond the parliamentary sphere, and have generated an important vision for the future, reflected in the document Chile Digital 2035.

The Cybersecurity Task Force of the Senate's Challenges of the Future Committee has been a remarkable experience, bringing together discussions, and sharing visions and concerns unrelated to political avatars, in a changing reality that demands and requires the attention of specialists.

The logical evolution of the Task Force is the National Cybersecurity Forum.

The Senate could promote the formalization of a voluntary entity, of a public-private nature, that brings together academia, civil society, the State, and trade organizations, among others, that represent interests in cybersecurity, to contribute to a healthy discussion and dissemination of knowledge that becomes a national reference in the field.

EXECUTIVE FORMATION OF THE FORUM

The Forum will be convened by the President of the Senate and will have a permanent Director appointed by him, who will be responsible for coordinating and facilitating the participation activities of the members, as well as promoting the activities of the Forum and representing it in public or private events.

It will have a permanent council composed of 12 members: two Senators appointed by the President of the Corporation; 4 representatives will be designated by institutions selected by the Transport and Telecommunications and Future Committees; 4 will be representatives elected by the institutions represented in the forum; one representative from the National Cybersecurity Agency and another from the National Data Protection Agency (considering that both entities are still subject to legislative process, the positions will remain vacant and will only be filled once these agencies are established).

FORUM MEMBERSHIP

The President of the Senate, in his capacity as President of the Forum, will extend a broad invitation to academia, civil society, trade organizations, non-governmental organizations, professional associations, and individuals related to the field of cybersecurity.

Institutions will be invited to have permanent representatives in the Forum, who must register with the respective formality, and they cannot exceed 5 representatives, preferably from diverse areas of each institution. Considering that Cybersecurity must be approached with a multidisciplinary and preferably holistic approach, it is important to have the participation of different sensitivities that are involved or affected by cybersecurity.

A regulation of participation and commitment of the members of the Forum will be established, considering the possibility of recognizing membership for personal or institutional promotion, in case of permanent participation. This condition will be evaluated based on their quarterly participation.

Participation in the forum is free of charge; however, considering the importance of the commitment assumed by the participating institutions, nominated members commit to support the activities with their time and knowledge, without implying exclusive dedication, similar to participation in professional or related activities.

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. Institutions may participate in more than one working group but with only one representative per group.

The Forum excludes the individual representation of companies that market or promote cybersecurity solutions, digital services of any kind, communications, data storage, equipment providers, search engines, and others related or similar, to maintain the necessary transparency and technical neutrality in the analysis and recommendations made by the Forum.

ABOUT WORKING TABLES

Once the Permanent Council is established, work tables will be proposed according to affinity, but following the Spanish model and our own current National Cybersecurity Policy. The following are initially proposed:

1) Cybersecurity culture. Seeking to:

***Promote** the dissemination of cybersecurity culture as a good business practice and recognize the involvement of companies in improving collective cybersecurity as corporate social responsibility.

***Raise** awareness among organizational executives so that they enable the necessary resources and promote cybersecurity projects that their entities may need.

***Promote** cybersecurity awareness and education at an educational level.

***Promote** a critical spirit in favor of accurate and quality information that contributes to the identification of fake news and misinformation.

***Seek** and recognize the collaboration and participation of media outlets in promoting cybersecurity.

***Support** and promote associations of institutions grouped on cybersecurity issues with their international counterparts.

2) Promotion of the cybersecurity industry and R&D&I. Seeking to:

***Stimulate** the increase in supply and demand for cybersecurity products and services from the national industry and their internationalization.

***Generate**, promote, and articulate entrepreneurship ecosystems in cybersecurity and R&D&I within a framework of public-private collaboration.

***Drive** the adoption of cybersecurity improvement measures in SMEs and micro-enterprises.

***Stimulate** the development of the cyber defense industry in coordination with national defense institutions.

3) Talent and training in Cybersecurity. Seeking to:

***Identify** the need for professional cybersecurity capabilities, fostering collaboration with educational and training institutions by promoting continuous training, employment training, and university education, and promoting systems of accreditation and professional certification systems.

***Promote** the inclusion of cybersecurity professional profiles in state institutions.

***Detect,** promote, and retain cybersecurity talent through programs and activities coordinated with academia.

4) Regulatory Framework in Cybersecurity

***Provide** analysis and proposals in regulatory and strategic matters.

***Systematize** public-private collaboration in initiatives with significant cross-sectoral impact during all phases of the legislative process.

***Contribute** to the situational awareness of the main national and international trends, objectives, and regulatory lines of action.

***Contribute** to the evaluation, simplification, harmonization, and alignment of existing regulations.

5) Digital Transformation

***Identify** the main challenges in Change Management in the Digital Transformation of the State and its relationship with citizens, and propose action paths to facilitate their resolution.

***Promote** the search for both conceptual and practical solutions to problems involving change management in a digital society.

***Contribute** to promoting societal changes towards a simple and secure use of information technology in the citizen-state relationship.

***Support** the development of Interoperability in Chile as a mechanism for continuous improvement in the citizen-state relationship.

6) Disruptive Technologies

***Identify** disruptive technologies in cyberspace.

***Assess** the positive and negative effects that the identified technologies may have, as well as their impact on the digital ecosystem and other areas of the country.

***Propose** control and mitigation measures for the adverse effects and risks that may affect the security of individuals, human rights, and democracy.

***Contribute** to the dissemination of the risks associated with the use of disinformation tools, fake news, deep faking, and others.

7) Online Disinformation

***Identifying** the techniques used to promote the dissemination of false information and inaccurate information (Disinformation, misinformation), Deep Fake, digital harassment, sextortion, phishing, cyberbullying, and similar.

***Prospecting** the effects and forms of influence of disinformation mechanisms, generation of disinformation campaigns, and manipulation of information in key processes for Democracy, the Rule of Law, and freedom of expression.

***Propose** strategies for control, mitigation, and evidence gathering to counteract effects contrary to the safety of individuals and their interpersonal relationships, the Rule of Law, and Democracy.

***Contribute**, based on international experience, to propose alternatives to address these issues, and develop control and oversight regulations without affecting human rights and the Rule of Law, pillars of democracy.

Other working groups will be established in case of more specific needs according to the Permanent Council.

OPERATION OF WORK TABLES

The work tables will be initially led by a team of Directors/Co-Director (chair-cochair) who will have the function of coordinating the activities; initially, they will be appointed by the Permanent Council and then ratified or replaced by the absolute majority of each table.

The tables will work on specific topics that are requested of them or address their initiatives that are considered relevant and on which it is important to form an opinion, generating documents and conclusions that represent their positions, following the rules that they establish for their operation, and according to standardized formats that will be agreed upon with the Permanent Council.

Foro Nacional de Ciberseguridad

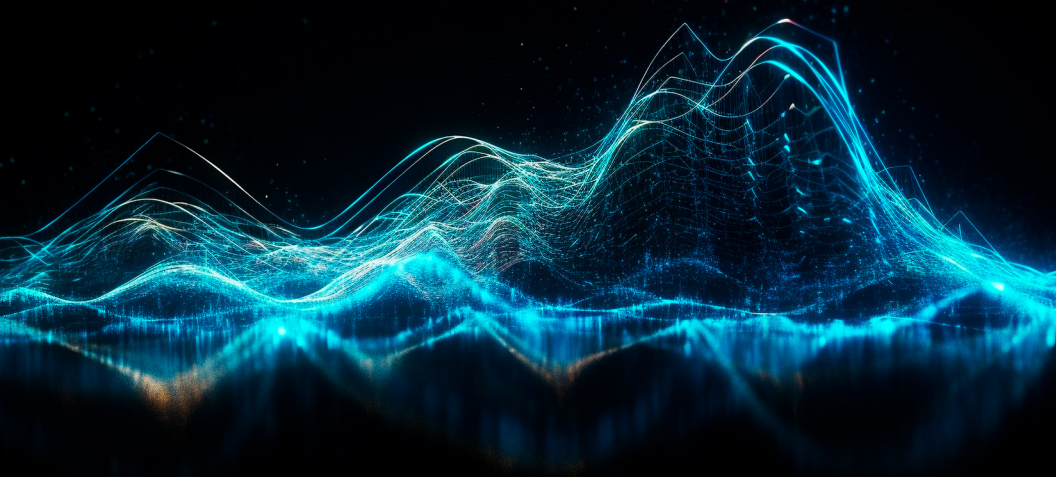
The National Cybersecurity Forum, under the Presidency of the Senate, was officially launched on October 2, 2023, at an event in the Hall of Honor of the Former National Congress in Santiago, attended by about 400 guests.

Participation in its working groups will be entirely online, and it will meet in person three times a year to report on its activities.

Access the website **www.forociber.cl** to learn more and participate in the National Cybersecurity Forum.

REPÚBLICA DE CHILE
SENADO

BUILDING CYBERSECURITY IN CHILE



COMITEE FUTURE CHALLENGES, SCIENCE, TECHNOLOGY, AND INNOVATION

Biblioteca del Congreso Nacional de Chile / BCN