IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 September 2023, accepted 21 November 2023, date of publication 24 November 2023,
date of current version 30 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3336818

RESEARCH ARTICLE

Adoption of Cybersecurity in the Chilean Manufacturing Sector: A First Analytical Proposal

FRANCISCO GATICA-NEIRA[1], PATRICIO GALDAMES-SEPULVEDA[2,3], AND MARIO RAMOS-MALDONADO[4]

[1]Department of Economics and Finance, Faculty of Business Sciences, University of Bío-Bío, Concepción 4051381, Chile
[2]Department Information System, Faculty of Business Sciences, University of Bío-Bío, Concepción 4051381, Chile
[3]Faculty of Engineering, Architecture and Design, Universidad San Sebastián, Concepción 4081339, Chile
[4]Department of Wood Engineering, Faculty of Engineering, University of Bío-Bío, Concepción 4051381, Chile

Corresponding author: Francisco Gatica-Neira (fgatica@ubiobio.cl)

This work was supported in part by FIC Project ''Sustainable Digital Transformation for Manufacturing SMEs in the Biobío region'' Innovation Fund for Regional Competitiveness, FIC-R Biobio 2021 execution 2022–2024 under Grant FIC I+D 22-79, and in part by the Internal Fund of the University of Bío-Bío (Research Directorate).

ABSTRACT This paper focuses on adopting cybersecurity procedures in Chilean manufacturing companies in the context of the Fourth Industrial Revolution's data-driven demands, which have exposed vulnerabilities in cybersecurity. This analysis is based on data from the Fifth Longitudinal Survey of Companies - ELE 5 - conducted by the National Institute of Statistics. Using the TOE adoption model, we employ binary and ordered Logit and Probit models with data from 574 companies and 17 explanatory variables. The objective is to gain insight into the factors influencing the adoption of cybersecurity processes, complementing the existing literature, which often focuses on developing specific technologies or conducting comprehensive analyses of digital transformation. The study highlights the significance of company size in explaining the adoption of cybersecurity procedures and reveals the relevance of explanatory variables as the depth of adoption increases. The findings underscore the need for public policies that facilitate the implementation of existing regulations, such as ISO 27.001, particularly for small companies. Additionally, the study emphasizes the importance of fostering a ''culture of cybersecurity'' across different sectors of society.

INDEX TERMS Adoption, cybersecurity, factory, industry 4.0.

I. INTRODUCTION

The Fourth Industrial Revolution, prominently features the implementation of sensors in processes and products, the use of cloud computing, the analysis of large volumes of data using artificial intelligence, and the Internet of Things (IoT), among other innovations [1]. These technologies are highly data-demanding and demand very high cybersecurity standards.

This paper aims to analyze the variables that explain the incorporation of cybersecurity procedures in companies in the Chilean manufacturing sector. To this end, several LOGIT and PROBIT models were built for binary dependent variables. Then, they were ordered with the information available in the Fifth Longitudinal Business Survey -ELE 5- of the National Institute of Statistics. This Survey includes a wide range of topics, which are grouped into i) Accounting and Finance, ii) Markets, Customers, and Suppliers, iii) General Management, iv) Resources, and v) Information Technologies. Our study exhaustively reviews the survey and selects 17 variables to analyze the factors explaining cybersecurity procedures' incorporation.

In this sense, the ELE 5 Survey identifies five types of internal cybersecurity procedures:

- Secure Password Authentication
- Identification and authentication of users through tokens or electronic devices (cards, USB, among others).
- Identification and authentication of users through biometric methods (fingerprint).
- Data backup (external hard drive, cloud computing) and
- Intrusion detection system (includes spam).

When reviewing the database of journals in the Web of Science Core Collection, Open Access, using the words ''cybersecurity,'' ''Adoption,'' and ''Manufacture'' to June 2023, we found that there are only sixteen publications, of which four are related to the analysis of specific technologies (IoT,

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Tsun Cheng.

3D printing, Blockchain, BWM-CRITIC-TOPSIS). The rest is associated with the advancement of digital transformation and how cybersecurity plays a vital role within this process. It is noteworthy that this group of articles particularly emphasizes the importance of professional technical secondary education and the adoption of cybersecurity standards within the manufacturing sector [2]. Furthermore, when consulting the terms ''cybersecurity,'' ''Manufacture,'' and ''Chile,'' we find only one study related to professional technical education. In conclusion, there are still few scientific publications that address, in a transversal and empirical way, with many companies, the levels of adoption of cybersecurity procedures.

The contribution of our work can be summarized in three axes:

- This research is innovative because it takes a data-driven approach to examine the adoption of cybersecurity practices in 574 Chilean companies. Our study encompasses various organizations and utilizes quantitative tools, specifically classical multivariate analysis techniques (Logit and Probit).
- Our work uses a technology adoption model to analyze the incorporation of cybersecurity practices in the company. We work on a database that addresses several company dimensions (marketing, organization, and management, among others). This allows our study to cross many different variables. Our research uses a validated and widely used model to analyze technological adoption (TOE).
- Finally, we examine the factors explaining cybersecurity adoption in a Latin American country, where digital transformation gaps are more pronounced compared to first-world countries [3]. We believe that the manufacturing reality in Chile is reflective of other developing countries.

We currently need to get information on this level of depth after COVID-19. However, manufacturing companies did not change their production practices for the most part, adjusting them according to social distancing health measures; therefore, our analysis includes structural elements that may be useful for a public policy to promote digital transformation.

II. THEORETICAL FRAMEWORK

Two main axes of analysis are developed. First, we present the concept of cybersecurity and its implications in Industry 4.0. Then, the generic technology adoption model is reviewed in a second point.

A. CYBERSECURITY AND INDUSTRY 4.0

Cybersecurity is one of the main challenges for those companies that want to become in Industry 4.0 [4].

According to Spadafora [5], manufacturing companies are the second most attacked in the USA due to the lack of security controls that protect their information assets according to the model: Confidentiality, Integrity, and Availability (CIA). Attacks through CAD files or USB disks with a malicious program or malware can affect the confidentiality and availability of data, and hackers who seek to compromise the integrity of the control interfaces employed by a human operator stand out.

The situation in Chile is the same. According to the study conducted by IPSOS in 2019 [6], 4 of 10 Chilean companies admitted to having had a cyber-attack. Furthermore, 40% of micro, 45% of small, and 56% of medium enterprises are considered vulnerable. In the cybersecurity guide of the Government of Chile of 2021, it is pointed out that Chilean companies have mainly suffered attacks of phishing, smishing, and ransomware, which have caused the temporary or permanent loss of files and access to services, the deletion of their websites or the Disruption of programs or systems.

As a result, companies have suffered from business continuity problems. Several studies highlight that the need for more awareness, training, and implementation of an adequate management system for information security are the main problems for small and medium-sized enterprises (SMEs) to be preferred to be attacked. In general, SMEs believe that investment in cybersecurity is an expense and do not see it as an ally that can mitigate business continuity problems and enhance the objectives and reputation of the organization.

In this sense, several regulations have been established to stimulate the adoption of cybersecurity in the industry, highlighting ISO 27.001 [7] and the NIST framework for cybersecurity [8]. These show the importance of maintaining adequate risk management on the company's information to continuously evaluate vulnerabilities, threats, and impact on information assets.

Another example of a standard even less known in Chile but no less relevant is the ANSI/ISA-62443, which corresponds to a series of standards for the safety of industrial control and automation systems. This standard emphasizes the application of the principle of defense in depth in the areas of plant safety, network, and system integrity. It is taking great value in the electricity sector.

In general, all the regulations, as mentioned earlier, promote the application of the following procedures [9]:

- Define the inherent vulnerabilities of systems that affect their security;
- Definition of cyber threats to systems.
- Identify risks related to cyberattacks.
- Countermeasures to address cybersecurity issues and subsequent assessment of residual risk obtained after implementation.

These steps require establishing an inventory of information assets to which a risk assessment is applied, considering confidentiality, integrity, and availability. This exercise must be updated regularly as a continuous improvement procedure, which allows an organization to have a vision of the current state of its level of maturity in cybersecurity, establish policies, procedures, improvement activities, and subsequent evaluation.

Considering the specific challenges and observations in small and medium-sized manufacturing companies regarding

cybersecurity, the facets of cybersecurity in the data-driven look can be further discussed as follows:

a) Supply chain security: It is crucial to highlight the potential consequences of data breaches or unauthorized access to shared data. Many attacks are originated from associated suppliers, vendors, or third-party partners.
b) Industrial Internet of Things (IIoT) security: The proliferation of connected devices and sensors in manufacturing environments brings new cybersecurity challenges and increases the landscape attack.
c) Employee training and awareness: Small and medium-sized manufacturing companies often have limited resources for cybersecurity personnel. Therefore, it becomes crucial to invest in comprehensive cybersecurity training and awareness programs for employees, even in companies with limited resources. Nowadays, phishing is one of the most popular attacks due to the lack of cyber awareness.
d) Incident response and business continuity: In the event of a cybersecurity incident, small and medium-sized manufacturing companies need to have effective incident response plans in place. This plan will help them to make good decisions as fast as possible and will help them to recover later quicker.
e) Compliance with industry standards: Small and medium-sized manufacturing companies may be subject to industry-specific cybersecurity standards or regulations. Complying with relevant standards, such as the NIST Cybersecurity Framework or ISO 27001, can become mandatory regulations in some industrial sectors. This involves conducting risk assessments, implementing appropriate controls, and regularly reviewing and updating security practices to align with industry requirements.

B. FACTORS THAT MAY DETERMINE THE ADOPTION OF CYBERSECURITY PRACTICES

A review of the WOS-Core Collection database for ''cybersecurity,'' ''Adoption,'' and ''Manufacture'' to June 2023 yielded 16 results. A summary of this group is the ten most relevant articles shown in Table 1. In summary, the following emphases emerge:

1) In relation to the Context: A first group of articles deals tangentially with cybersecurity, framing it within a broader theme associated with the implementation of enabling technologies for Industry 4.0. [10], [11], [12]. A second group accounts for cybersecurity and the development of some specific technologies, e. g. IoT, 3D printing, Blockchain, Digital Twin, among others. [13], [14], [15], [16], [17], [18]
2) Regarding the results: A first group proposed different methodologies or tools to detect anomalies and attacks [13], [14], [15], [18]. Meanwhile, we have a second group that identified barriers or risks in implementing Industry 4.0 enabling technologies, among which is cybersecurity. [10], [11], [12], [16], [17]. In this regard one research identifies barriers to adopting cybersecurity [19], using a survey of 258 organizations.
3) Regarding the method: In general, there is a group of articles that work with the expert consultation methodology using interpretive structural modeling (ISM), Analytical Hierarchy Process (AHP), among other methodologies. [11], [12], [16]. On the other hand, there are works oriented to explore a set of techniques or tools through simulation or cases [13], [14], [14], [14], [18]. In this sense, the works that use sustainability reports [10], surveys of organizations [19], and literature review plus cases to generate a diagnosis [17] stand out.

Our research analyzes the explanatory factors of adopting some cybersecurity practices in 574 Chilean manufacturing companies, using multivariate techniques, complements ongoing research on the subject.

Many models allow us to understand the processes of technological adoption at the level of companies and end users. Our work will use the Technology, Organization, and Environment (TOE) model, which is more focused on the Diffusion of Innovation [20] because it is commonly used to understand the adoption process in companies.

Own elaboration from the Bibliographic review

The TOE model we will use is generic and, in future research, should be adjusted to cybersecurity because it is a business decision where leadership, policies, and the perception of cyber risk are fundamental [21]. In addition, we need to include cultural factors because they are vital when analyzing the adoption level of cybersecurity practices [22]. However, despite the above, in this research, we will stay with the homogeneous TOE given the quantitative nature of our study, where 574 companies are analyzed from 17 variables, generating quantitative indicators from the information available in the Survey.

Quickly, the dimensions of the TOE model are:

- Technological: Relative advantages provided by technology due to the perception of challenges and compatibility problems.
- Organizational: Firm size, management support, and workforce qualification.
- Environmental: The level of rivalry that the adopter company has, the levels of environmental uncertainty, and the perception of logistics support.

In a quick literature review, the ability of manufacturing companies to adopt cybersecurity practices can be explained by the following generic factors:

- The size of the company determines the capacity to adopt more complex technologies through the financial and administrative power to be able to mobilize scarce resources [19], [23], [24], [25], [26].
- Skilled labor facilitates the process of adoption of new technologies. This determines the company's prospecting, evaluation, and implementation processes [28], [29]. This is especially true in the workforce specialized in digitalization [21], [30], [31], which must have a

TABLE 1. Synthesis of the main selected articles.

Article	Context	Proposal / key results	Method
[13]	Cyber-attacks and IoT use	Statistical methods of attack detection.	Simulation and use of sorting algorithms.
[10]	Industry 4.0 and sustainability reporting.	The level of presence of 4.0 technologies is broken down by type, region, and impact on processes.	Examines 1501 sustainability reports (GRI) to see the level of adoption.
[14]	Increased interconnecti on of devices increases cyber security requirements.	The neural network model allows for different types of anomaly detection models.	Deep Learning is proposed for threat detection in IoT systems.
[11]	Risks for SMEs when incorporating Industry 4.0 technologies.	Risks are identified: financial, operational, technological, business, social, supply chain, and cybersecurity (data breaches, hacking, repudiation of attacks).	Survey of industry experts in India using Analytical Hierarchy Process.
[19]	Identification of barriers to adoption around cybersecurity .	Seven barriers were identified. They include lack of expertise, little recognition in implementation, little government support, and that it is not a driver for purchasing decisions. .	258 organizations from various sectors in Australia and international organizations were surveyed. Response distribution analysis and semantic analysis.
[12]	Factors conditioning the implementati on of Information and Digital Technologies (IDT) in the smart factory.	Perception of benefits and management support is critical. Stresses the importance of having a 360° approach to cyber security.	Expert consultation, literature review, and interpretive structural modelling (ISM).
[15]	Expansion of additive manufacturin g (AM)	Implement various Machine Learning (ML) tools in additive manufacturing techniques.	Simulation and use of various algorithms.
[16]	Use of Blockchain technology in global supply chains	The blockchain is an excellent tool to improve trust in a global supply chain. Essential knowledge to generate a decision roadmap.	Literature review and interview with four project managers to discover the state of Blockchain adoption in three third-party logistics services.
[17]	Application of Blockchain technology to the automotive industry.	Guidelines and recommendations for the implementation of the Blockchain in the automotive industry.	Literature review and case study, SWOT diagnosis.
[18]	New technologies (ML, IoT) impose challenges in cyber security.	Visualize and implement an integrated platform for simulating and monitoring industrial conditions in a digital twin.	Development of multiple components based on Artificial Intelligence. Textile company case

cybersecurity culture [22], especially in the SME segment [19].

- Companies with an innovative track record are more likely to adopt new technologies for leadership, innovation culture, and organizational flexibility [25], [32], [33], [34].
- Companies with more compatible and interconnected technologies will likely adopt synergistic technologies. In digitalization ecosystems, cybersecurity is a strategic part of Industry s 4.0 [35]. The units that have a greater incorporation of 4.0 technologies and, at the same time, have a more significant presence of these in the different stages of the value chain will have a greater probability of taking advantage of new opportunities in terms of speed, production capacity, reduction of errors, costs and an improvement in the quality and differentiation of the products [36]
- The existence of young, knowledge-intensive companies based on new technological fields increases the likelihood of adopting new technologies [37]. In this sense, the type of entrepreneur is fundamental to leading the digital transformation process, which was confirmed by Maggi C. [31] and Motta [30] in manufacturing SMEs in Chile and Argentina.
- Finally, access to some markets can pressure the adoption processes of specific technologies. Openness to international trade, whether in sales or purchases, is a stimulator of adopting 4.0 technologies [38]. Even trading with other countries can force companies to have a certain cybersecurity standard [21]. Certification in compliance with cybersecurity criteria could mean an advantage when attracting new customers or maintaining current ones. This issue depends on the sensitivity of consumers to the cyber risks associated with the misuse of their information [19].

In summary, the adoption of cybersecurity practices will be positively associated with the size of the company, the qualified human capital, the innovative trajectories of the organization, the existence of compatible technologies, youth, the origin of business capital, and the presence of markets that stimulate the existence of certain key technologies.

In this sense, the CSIRT of the Chilean government published a report on manufacturing companies [39]. This study presents global data on the main cyber security threats affecting this productive sector. Some examples of affected companies are given, but Chilean companies are not included.

The Global Cybersecurity Index (ITU) [40], which considers legal, technical, organizational, development, and cooperation aspects, ranks Chile 74th worldwide. Specifically, our country ranks seventh in the Americas, following the USA, Canada, Brazil, Mexico, Uruguay, and the Dominican Republic. Chile boasts an acceptable legal framework but faces significant weaknesses in technological aspects.

Since March 2018, Chile has had a Computer Security Incident Response Team (CSIRT) operating under the Ministry of Interior and Public Security. This team is responsible for strengthening and promoting good practices, policies, laws, regulations, protocols, and cybersecurity standards throughout the State, critical infrastructure, and the entire country (https://www.csirt.gob.cl/). Additionally, the draft Framework Law on Cybersecurity and Critical Information Infrastructure is currently in the Chamber of Deputies, undergoing its second constitutional procedure. This legal framework aims to enhance the institutional framework by establishing the National Cybersecurity Agency in Chile. Lastly, Law 19.628 on the Protection of Privacy, which dates back to 1999, is currently undergoing updates.

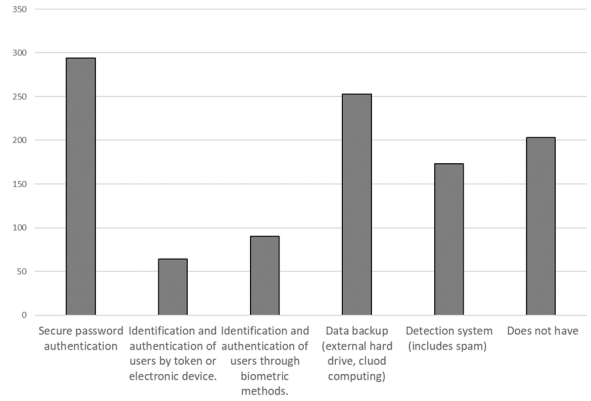

FIGURE 1. Frequency of occurrence of cybersecurity procedure. Number of enterprises = 574 (Note = a company can have multiple procedures). Own elaboration from the ELE.

Chile must urgently close the cybersecurity gaps to approach the standards of the most developed countries.

In this context, our research aims to analyze the factors influencing the adoption of cybersecurity procedures in the Chilean manufacturing sector, which contributes 9.7% to the Gross Domestic Product (GDP), ranking below mining activity (14.7%) and personal services (12.1%), according to data from the Central Bank of Chile. Within the manufacturing sector, notable industries include the food industry (31% share in manufacturing), the chemical industry (24%), and metal production (16%).

Chilean manufacturing plays a crucial role in the national export chains, serving as a strategic supplier to mining, forestry, and fishing activities. Consequently, cyber threats targeting individual manufacturing companies' operating networks can affect the entire production network, impacting both forward links (with customers) and backward links (with suppliers).

In this regard, we note an explosive increase in vulnerabilities in industrial control system (ICS) platforms [39], which increased by 49% when comparing 2020/2019. More specifically, in operational technology environments, during 2020, we have ransomware attacks (extortion software), which account for 33% of cases, remote access Trojans (RATs), which account for 15%, and internal incidents (associated with malicious insiders and negligence) account for 13% of the total.

Our work aimed to study cybersecurity as a critical link for national economic growth. With our study we sought to provide information necessary for new public policies, in the context of a new institutional framework f for promoting and developing cybersecurity at the national level.

Next, a pre-data review will be carried out to contextualize the quantitative analysis.

III. PRELIMINARY REVIEW OF DATA

About 35% (n = 203) of the companies analyzed need built-in cybersecurity procedures. This percentage is high considering the type of companies being analyzed, where manufacturing companies should have a minimum cybersecurity standard due to the more significant addition of value in their production processes.

The most frequent procedures are strong password authentication, present in 51% of companies (n = 294); data backup on external disks or the cloud is present in 44% of companies (n = 253); and intrusion detection systems (including SPAM) were found in 30% of companies (n = 173).

In the range of the least frequent procedures, we have the identification and authentication of users through biometric methods, present in 16% of manufacturing companies (n = 90), and the identification and authentication of users by a token or an electronic device available in 11% of companies (n = 64).

A review of Table 1 shows that the Survey prepared by the National Institute of Statistics (INE) distinguishes different sizes of companies based on sales revenue. According to our tabulation, 33% of the companies are classified as significant (n = 187), and the medium ones represent 6% of the total analyzed (n = 37). Furthermore, in the group of small companies, the INE separates this segment into two sections, explaining 42% of the total (n = 243). Finally, the microenterprise segment represents 19% of the analyzed group (n = 107).

In another area, we see that, on average, companies are 24 years old. 40% of the units analyzed (n = 227) are family businesses. 29% of the organizations analyzed (n = 164) have invested in computer equipment in the last two years. Only 11% of all companies (n = 66) have invested in software in the last two years. The primary customer is the domestic market accounting for 60% of sales. While the international market explains an average of 7%, and sales to the State or public sector explain 3.9%. In the last two data, the dispersions are high from the coefficient of variation (301% and 345%, respectively).

Regarding its innovative dimension, 25% of the companies analyzed (n = 144) declare to participate in a trade association with a university and the productive development system. In this line, 26% of companies (n = 151) declare to participate in an R + D + i project. On average, companies hire 1,713 workers annually with a high dispersion (coefficient of variation of 474%); in monthly terms, the average number of workers is 142. However, only 29.7% are qualified as specialized workers, understood as managers, professionals, technicians, and qualified operators.

Finally, we have the technological variable. On average, companies use software other than traditional office software. In addition, 78%, equivalent to 449 units, use the Internet to interact with customers. However, 34% of these manufacturing companies (n = 194) use social networks, and only 36% of the organizations (n = 208) perform e-commerce operations (purchase or sales).

IV. METHODOLOGY

Our database comes from the Longitudinal Survey of Companies [44], which is carried out by the National Statistics Institute (INE) of the Ministry of Economy of the Government of Chile. This instrument aims to characterize the

TABLE 2. Presentation of the variables.

Variable	Variable type	Sum	Average	Deviation	C. variation
Company size					
Large company	Binary	187			
Median	Binary	37			
Small 1	Binary	77			
Small 2	Binary	166			
Microenterprise	Binary	107			
Antiquity	Numerical		24,7	14,6	59%
Family businesses	Binary	227			
Invested in computer equipment in the last two years	Binary	164			
Invested in software in the last two years	Binary	66			
% national sale	Numerical		59,9	42,6	71%
% foreign sales	Numerical		7,0	21,0	301%
% sale to the State	Numerical		3,9	13,3	345%
Number of major suppliers	Numerical		29,1	162,1	557%
Participation in Promotion System	Binary	144		EE	
Amount of complex software (excluding office)	Numerical		0,9	1,2	128%
Does R+D+i	Binary	151			
The annual number of workers	Numerical		1713	8121	474%
% Skilled workers	Numerical		29,7	31,9	107%
Use the Internet to interact with customers	Binary	449			
The company uses RRSS.	Binary	194			
The company buys and sells using the Internet	Binary	208			

NOTE: OWN ELABORATION FROM THE ELE

TABLE 3. Distribution of the dependent variable.

Dependent variable	Number of companies	%
Has cybersecurity procedure	371	65%
No cybersecurity procedure	203	35%
Overall total	574	100%

	Number of companies	%
Null incorporation (0 procedure)	203	35%
Basic incorporation (1 procedure)	124	22%
High incorporation (2,3,4,5 procedures)	247	43%
Overall total	**574**	**100%**

Note: own elaboration from the ELE

country's companies and uses the database of the Internal Revenue Service (SII) as an input to determine the target population. To classify economic activities, it uses the International Standard Industrial Classification (ISIC4.cl.2012). The survey is answered by the owner or manager of the company and is a validated instrument, which has been applied since 2009, being a very relevant input for public policies in Chile.

Our model uses 17 explanatory variables from different company domains (Xn). The dependent variable (Yn), related to the adoption of cybersecurity procedures, arises from the same ELE 5 survey and is related to question J.III, on ICT security, and reads: "Does your company use one of the following internal security facilities or procedures? The respondent could tick more than one of the following alternatives:

a) "Secure password authentication".
b) "User identification and authentication via token or electronic device (e.g. USB card). "
c) "Identification and authentication of users through biometric methods (fingerprint)".
d) "Data backup (external hard disk, cloud computing).
e) "Intrusion detection systems (including spam)".
f) "Does not have "

The analysis assumes this database as a limitation of the field study. Since the survey was taken by the National Institute of Statistics, it is forbidden to reveal the name of the companies that provided the information (Organic Law 17.374). This limits the depth of the data of the surveyed enterprises within a specific subgroup. In the future, the quality of the measurement of cybersecurity in the company can be improved, which would be the subject of further research. Scales were generated from the responses.

We chose to binary the dependent variable based on the presence of cybersecurity procedures (0/1), considering that 35% of the companies do not have any procedures.

To better measure the depth of the adoption process, three scales of adoption were identified. From the results, a distinction was made between a) No adoption (0 procedure), b) Basic adoption (1 procedure) and c) High adoption (2 to 5 procedures). These scales are consistent with the cut-off points detected in the ordered Logit models and especially in the ordered Probit (see Table 5).

Measuring adoption from the sum of the procedures present in a company can be a basic proxy for technological depth. However, it is a first step to identify interrelationships between different technologies present in an organization [41]. This will be the subject of future research.

Four models were generated to identify the variables that best explain the level of adoption of cybersecurity procedures:

- Two binary models (Logit and Probit) to identify the factors that explain the presence or absence of cybersecurity procedures.

- Two ordered models (Logit and Probit) to identify the factors that explain the depth of the adoption process.

Regression models have the following formulation:

TABLE 4. Presentation of variable and hypothetical relationships.

TOE	Variable	Var. type	Explanation and hypothetical relationship
Technology	Invested in computer equipment. Last two years	Binary	The company invested in assets during the previous year. Si=1; No =0 Positive hypothetical ratio (+) [32], [33], [25], [34]
Technology	Invested in software. Last two years	Binary	The company invested in assets during the previous year. Si=1; No =0 Positive hypothetical ratio (+) [32], [33], [25], [34]
Technology	Amount of complex software (excluding office)	Numerical	Total number of software (ERP; Sales, marketing, and customer management software; Turn-specific software, cloud computing, others) Positive hypothetical ratio (+) [35], [36]
Technology	Use the Internet to interact with customers	Binary	The company declares to use the Internet to interact with its customers. Si=1; No =0 Positive hypothetical ratio (+) [35] [36]
Technology	The company uses RRSS.	Binary	The company declares to use social networks. Si=1; No =0 Positive hypothetical ratio (+) [35] [36]
Technology	The company buys and sells using the Internet	Binary	During the year, the company performed buying and selling operations online (at least one). Si=1; No =0 Positive hypothetical ratio (+) [35] [36]
Organization	The annual number of workers	Numerical	The total number of people employed during the year (Jan+Feb+...+Dec). Direct contract (written or fee) included Positive hypothetical ratio (+) [23], [27], [24], [25], [26]
Organization	Company size	Categorical.	The survey distinguishes the Large, Medium, Small 1, and Small 2 companies. Positive hypothetical ratio (+). [23], [27], [24], [25], [26] [19]
Organization	% Skilled workers	Numerical	=(Sum (managers + professionals + technicians) / total workers)*100% Positive hypothetical relationship. [29], [30], [31], [21], [28], [19]
Organization	Antiquity	Numerical	Years of the company's existence from initiating activities in the Internal Revenue Service. Negative hypothetical ratio (-) [37]
Organization	Family businesses	Binary	A family or household owns more than 51%. Si=1; No =0 Negative hypothetical ratio (-) [37]
Environment	% national sale	Numerical	The percentage declared by the company of its income sold to domestic companies. Positive hypothetical ratio (+) [38], [21], [19]
Environment	% foreign sales	Numerical	The percentage declared by the company of its revenue sold to international companies. Positive hypothetical ratio (+) [38], [21], [19]
Environment	% sale to the State	Numerical	Percentage declared by the company of its income that is sold to the public sector. Positive hypothetical ratio (+) [38], [21], [19]
Environment	Number of major suppliers	Numerical	The number of suppliers declared by the company as relevant to the production process. Positive hypothetical ratio (+) [38]
Environment	Participation in Promotion System	Binary	The company currently participates in trade associations with universities and productive development systems. Si=1; No =0 Positive hypothetical ratio (+) [32], [33], [25], [34]
Environment	Does R+D+i	Binary	During the last two years, the company has carried out basic, applied, and experimental research (at least one). Si=1; No =0 Positive hypothetical ratio (+) [32], [33], [25], [34]

Own elaboration from the Bibliographic review.

Adoption level = f (size; seniority; family businesses; investment in computer equipment; investment in software; % of national sales; % of foreign sales; % sale to the State; the number of significant suppliers; participation in trade associations, universities, and development system; the amount of complex software; doesR +D+i; the annual number of workers, % skilled workers; use of the Internet to interact with customers; use of Social Networks; carrying out buying and selling transactions, (θ)

Appendix A presents the nonparametric correlation matrix where Spearman's Rho coefficient and Kendall's Tau correlation coefficient are calculated from the nature of the data [42]. It can be verified that no very high correlation generates suspicions of multicollinearity. On the other hand, the Variance Inflation Factor (VIF) is calculated, yielding results below 10.0, ruling out collinearity problems.

The original database of the Longitudinal Survey of Companies (ELE) registered 656 companies in the filtering process; companies that had incomplete and erratic data were excluded, reaching 574 units, equivalent to 87.5% of the original base.

Regarding the size restrictions to run the Logit and Probit models, Freeman's formula was used: $[n = 10 * (k + 1)]$ [43], where k are the independent variables used ($k = 17$), then $n = 10^*(17+1)$; $n = 180$ companies required, our database reached 574, exceeding what was necessary.

Along with the ordered Logit and Probit models, marginal effects were also calculated to clearly identify each independent variable's impact when changing each dependent variable's tranche. Finally, the econometric analyses were done with the free software Gretl [45]. For the estimation of marginal effects, an lp-mfx package add-on, version 1.0, was downloaded.

V. FIELD STUDY

Now, we will present the results ordered by TOE dimension from Table 3. For each dimension and variable, we will offer the following:

1. Binary Coefficient Logit (Blb).
2. Binary Probit coefficient (Bpb).
3. Ordered Logit coefficient (Blo).
4. Ordered Probit coefficient (Bpo).

For each variable, the confidence level is presented with an asterisk. The rates of correctly predicted cases exceed 68%, indicating excellent models' good explanatory capacity (Table 4).

A. TECHNOLOGY

In all the regressions, companies that invested in computer equipment during the previous year have a greater probability of having cybersecurity procedures (Blb = 0.68**, Bpb = 0.395**; Blo = 0.775***; Bpb = 0.441***), confirming our initial hypothesis. However, the result was not as expected when we analyzed the investment in software. In all four regressions, this variable did not turn out to be significant, which rejects our preliminary hypothesis.

The technological variable "the number of complex software" is significant and positive when explaining adoption, which is tangible in all regressions (Blb = 0.46**; Bpb = 0.249**; Blo = 0.643***; Bpo = 0.365***). The above confirms the technological compatibility with our initial working hypothesis.

In binary regression models, the Internet use to link with customers is not a significant variable (Blb = 0.28; Bpb = 0.18), which contradicts our working hypothesis. However, when we analyze the ordered models, using the Internet to link with customers is a positive and significant variable, confirming our initial assumptions (Blo = 0.421*; Bpo = 0.301**). Furthermore, the variable use of the Internet to link with customers shows its importance when we identify different stages of adopting cybersecurity procedures.

The use of social networks in all models explains the adoption of cybersecurity procedures (Blb = 0.84***; Bpb = 0.475***; Blo = 0.901***; Bpo = 0.503**). This relationship is positive and significant, confirming our working hypothesis.

Finally, we have the results of performing buying and selling operations online. Generally, this variable has a positive and significant relationship with adopting cybersecurity procedures (Blb = 0379*; Blo = 0.421*; Bpo = 0.179∗). However, the results are not as strong as the previous variables. It is striking that in the Probit binary model, the purchase and sale over the Internet is not a significant variable to explain the adoption of cybersecurity practices.

B. ORGANIZATION

The first variable is the number of workers who behaved differently in our regression models. In the case of the binary Logit and Probit models, it is not observed that this variable is explanatory of adopting cybersecurity procedures. However, when we relate the variables in the ordered models, the number of workers becomes a vital indicator adjusting to our initial hypothesis (Blo = 0.00**; Bpo = 0.00***).

When the size of companies is analyzed, we verify that large companies have a high probability of adopting cybersecurity procedures (Blb = 1,599***, Bpb = 1,007***; Blo = 1,351***; Bpo = 0.81***). With a lower weight, medium-sized companies have an explanatory impact on adoption in all the regressions analyzed (Blb = 1. 152**, Bpb = 0.78***; Blo = 1. 12**; Bpo = 0. 69**). When we examine the upper end of small businesses, there is still a probability of adoption of a lower significance (Blb = 0.609*, Bpb = 0. 37*; Blo = 0.54∗), and even for the ordered Probit model, the small business is no longer significant. Finally, smaller companies have no bearing on adoption. This gradient confirms the initial working hypothesis where the company size is unbalanced when explaining the adoption.

Contrary to our initial hypothesis, the variable percentage of specialized workers is insignificant in any of the four regressions. Something similar happens with the family condition of the company, where we do not see a significant impact on adoption in the four models built. Finally, although the age variable has a negative slope, it was non-significant.

C. ENVIRONMENT

Interestingly, in both models, the percentage of national sales presents a positive and significant result when explaining the adoption of cybersecurity procedures (Blb = 0.007***, Bpb = 0.004***, Blo = 0.008***, Bpo = 0.004***), which confirms our hypothesis. Contrary to expectations, sales to foreign customers are not explanatory when adoption is worked as a binary variable. However, when we distinguish the depths of the adoption process, openness to international trade is a significant variable (Blo = 0.013**, Bpo = 0.008**), which allows us to confirm our initial hypothesis. Finally, when analyzing the dynamic capacity of sales to the public sector or the State, we find no significant impact on adopting cybersecurity procedures.

From the four regression models, we found that the variable ''number of important suppliers'' is insignificant in explaining adoption, which rejects our original hypothesis. Similarly, participation in trade associations, university consortia, and productive development systems is insignificant, rejecting our original hypothesis.

Finally, there is a significant and positive impact of those companies that carry out R + D + i and the adoption of cybersecurity practices (Blb = 0.892***, Bpb = 0.495***, Blo = 0. 714***, Bpo = 0.391***), which proves our initial hypothesis.

Complementing the previous analysis, marginal effects are presented (Table 5) to identify any change in significance or slope in each depth section in adoption: a) Null incorporation, b) Basic incorporation, and c) Advanced incorporation. Next, the main changes for each dimension of the TOE model will be presented.

- **Technological dimension:** The investment in computer equipment in the last two years, the amount of complex software in the previous two years, customer service through the Internet, the purchase and sale by the Internet, and the use of the RRSS are positively and significantly associated when the level of adoption is advanced. However, consistent with previous results, investment in software in the last two years does not explain the adoption level.
- **Organizational Dimension:** The number of workers has a differential effect when the company is at an advanced incorporation level. Something similar happens with large and medium-sized companies where their condition is positively and significantly associated with high levels of incorporation of practices. Interestingly, in small companies, in the ordered Probit model, in none of the sections analyzed, any significant relationship is observed. Something different is the Logit-ordered model, where the incidence of small companies in the upper section shows that the advanced incorporation is very weak. In the case of smaller companies in this section, the relationship is nil. As previously concluded, the percentage of specialized workers, seniority, and family business status is not significantly related to the level of incorporation in any of its analyzed sections.
- **Environment Dimension:** The percentage of national sales, the percentage of sales abroad, and the realization of R+D have a positive and significant relationship

TABLE 5. Logit and probit regressions N = 574.

		(A) Binary logit (βlb)	(B) Binary probit (βpb)	(C) Logit Ordered (βlo)	(D) Probit Ordered (βpo)
TOE	Constant	-1,850 (***)	-1,064 (***)		
T	Investment in computer equipment. Last two years (Binary)	0,683 (**)	0,395 (**)	0,775 (***)	0,441 (***)
	Software Investment. Last two years (Binary)	-0,203	-0,132	-0,313	-0,154
	Amount of complex software (office software excluded)	0,4618 (**)	0,249 (**)	0,643 (***)	0,365 (***)
	Uses the Internet to link with clients (binary)	0,2831	0,187	0,421 (*)	0,301 (**)
	The company uses the RRSS (binary)	0,8406 (***)	0,475 (***)	0,901 (***)	0,503 (***)
	Buy and sell online (binary)	0,379 (*)	0,198	0,345 (**)	0,179 (*)
O	The annual number of workers	0,0004	-0,0002	0,0004 (**)	0,0002 (**)
	Large enterprise (binary)	1,599 (***)	1,007 (***)	1,351 (***)	0,811 (***)
	Medium Business (Binary)	1,152 (**)	0,785 (***)	1,120 (**)	0,691 (**)
	Small Business 1 (binary)	0,609 (*)	0,370 (*)	0,544 (*)	0,281
	Small Business 2 (binary)	0,354	0,221	0,100	0,052
	Percentage of skilled workers.	0,00002	-0,0001	0,001	0,0004
	Antiquity	-0,006	-0,004	-0.007	-0,005
	Family business (Binary)	0,362	0,201	0,197	0,105
E	% National sale	0,007 (***)	0,004 (***)	0,008 (***)	0,004 (***)
	% Foreign sales	-0,004	0,003	0,013 (**)	0,008 (**)
	% Sale to the state	-0,002	-0,001	0,002	0,00084
	Number of major suppliers	0,001	0,0006	0,001	0,0007
	Participation in Trade Associations, Universities, and Productive Development Systems (Binary)	0,301	0,179	0,183	0,114
	Does R+D+i	0,892 (***)	0,495 (***)	0,714 (***)	0,391 (***)
	Cut-off points			C1=1,8(***) C2=3,5(***)	C1=1,0(***) C2=2,0 (***)
	Adjustment quality indicators	Number of correctly predicted cases = 79% R_2 corrected=0.27 Chi^2.=0000	No. of correctly predicted cases = 78% R_2 corrected=0.27 Chi^2.=0000 Null hip (the error has normal distribution); Chi^2=1.30 p=0.520	Núm.de correctly predicted cases = 69% Chi^2.=0000	No. of correctly predicted cases = 68% Chi^2.=0000 Null hip (the error has normal distribution); Chi^2=1.53 p=0.46

(*) 90% confidence; (**) 95% confidence and (***) 99% confidence.

Own elaboration from the ELE

in the section of companies with advanced incorporation. In both regression models ordered, the variables' percentage of the sale to the State, the number of suppliers, and participation in trade associations do not present a significant relationship in any of the sections analyzed.

From the slopes of marginal effects, we can conclude that the differentials in technological, organizational, and environmental variables are only clearly seen when companies have advanced incorporation. The analysis of marginal effects also shows us that in the face of changes in independent variables, the segment of null and basic incorporation companies has the same sensitivity.

VI. DISCUSSION OF RESULTS

From the results, we can conclude that:

- Companies implementing a digital ecosystem [35], [36] will be more likely to adopt cybersecurity procedures. The above is visible in investment in computer equipment, complex software, relationships with customers through the Internet, electronic buying and selling, and the use of social networks. Moreover, this group of companies already knows the profitability of having a certain technological synergy, being more likely to implement or add new digital technologies by better visualizing the benefits, more excellent technological compatibility, and an innovative trajectory.
- A second strongly endorsed dimension is the size of companies as a determinant of adopting cybersecurity procedures. Our results align with those indicated by [19], [23], [24], [25], [26], and [27]. The number of workers hired, and the company's size from tranches derived from sales revenue show that large and medium-sized companies are more likely to mobilize financial, human, and organizational resources to implement new adoption processes.
- Contrary to expectations, the percentage of specialized workers turned out to be a variable that was not very significant, contradicting what was initially indicated by

TABLE 6. Marginal effects for ordered logit and ordered probit.

		Logit Ordered			Probit Ordered		
TOE		Null incorporation of practices (dp/dx)	Basic incorporation of practices (dp/dx)	Advanced incorporation of practices (dp/dx)	Null incorporation of practices (dp/dx)	Basic incorporation of practices (dp/dx)	Advanced incorporation of practices (dp/dx)
T	Investment in computer equipment in the last two years (Binary)	-0.077 (***)	-0.105 (***)	0.182 (***)	-0.089 (***)	-0.080 (***)	0.170 (***)
	Software Investment in the last two years (Binary)	0.038	0.039	-0.077	0.036	0.024	-0.06
	Amount of complex software (office software excluded)	-0.07 (***)	-0.085 (***)	0.157 (***)	-0.081 (***)	-0.062 (***)	0,144 (***)
	Uses the Internet to link with clients (binary)	-0.051	-0.052 (**)	0.104 (*)	-0.07 (**)	-0.04 (**)	0,119 (**)
	The company uses the RRSS (binary)	-0.091 (***)	-0.120 (***)	0.212 (***)	-0.103 (***)	-0.090 (***)	0,194 (***)
	Buy and sell online (binary)	-0.038 (**)	-0.046 (**)	0.084 (**)	-0.040 (*)	-0.030 (*)	0,070 (**)
O	The annual number of workers	-0.0005 (***)	-0.0006 (**)	0.00012 (**)	-0.0006 (***)	-0.0004	0,0001 (**)
	Large enterprise (binary)	-0.129 (**)	-0.176 (***)	0.306 (***)	-0.156 (**)	-0.147 (***)	0,303 (***)
	Medium Business (Binary)	-0.087 (**)	-0.151 (***)	0.238 (***)	-0.108 (***)	-0.137 (***)	0,246 (***)
	Small Business 1 (binary)	-0.052 (*)	-0.075 (*)	0.127 (**)	-0.056	-0.052	0,108
	Small Business 2 (binary)	-0.011	-0.01	0.024	-0.011	-0.009	0,020
	Percentage of skilled workers.	-0.0001	-0.002	0.0003	-0.0001	0.0007	0,0001
	Antiquity	0.0008	0.001	-0.0019	0.0012	0.0009	-0.002
	Family business (Binary)	-0.021	-0.026	0.048	-0.023	-0.018	0.041
E	% National sale	-0.0009 (***)	-0.001 (***)	0.002 (***)	-0.001 (***)	-0.00084 (***)	0,0019 (***)
	% Foreign sales	-0.001 (**)	-0.001 (**)	0.003 (**)	-0.001 (**)	-0.0014 (**)	0,003 (**)
	% Sale to the state	-0.0002	-0.0003	0.006	-0.0001	-0.0001	0,0003
	Number of major suppliers	-0.0001	-0.00017	0.0003	-0.0001	-0.0001	0,0003
	Participation in Trade Associations, Universities, and Productive Development Systems (Binary)	-0.019	-0.024	0.044	-0.024	-0.020	0,044
	Does R+D+i	-0.070(***)	-0.097 (***)	0.168 (***)	-0.07 (***)	-0.072 (**)	0,151 (***)

(*) 90% confidence; (**) 95% confidence and (***) 99% confidence
Own elaboration from the ELE.

[21], [28], [29], [30], and [31]. Our study has not yet captured the importance of the workforce specialized in digitalization, especially those with cybersecurity training [19].

- The results reject the initial hypotheses concerning seniority and family business variables. One explanation for these results is that manufacturing companies that already have a level of complexity are being analyzed. Therefore, the type of firm does not contribute to the variety when explaining the dependent variable.
- The variable ''percentages of national sales and international sales'' are explanatory of the level of adoption, confirming the importance of the ''pull of the markets'' when explaining the adoption, which follows the line of what was identified by [21] and [38]. However, it is worrying that sales to the State do not stimulate the adoption of cybersecurity procedures. This result shows a ''gap'' that must be covered by public policies where the State can promote processes of technical change in the companies that provide them as a strategy to boost the national productive fabric [19].
- In the environmental elements, it is striking that participation in Trade Associations, Universities, and Productive Development Systems does not explain the probability of adopting cybersecurity procedures. In this case, participation in these instances does not stimulate the implementation of cybersecurity procedures in manufacturing processes.

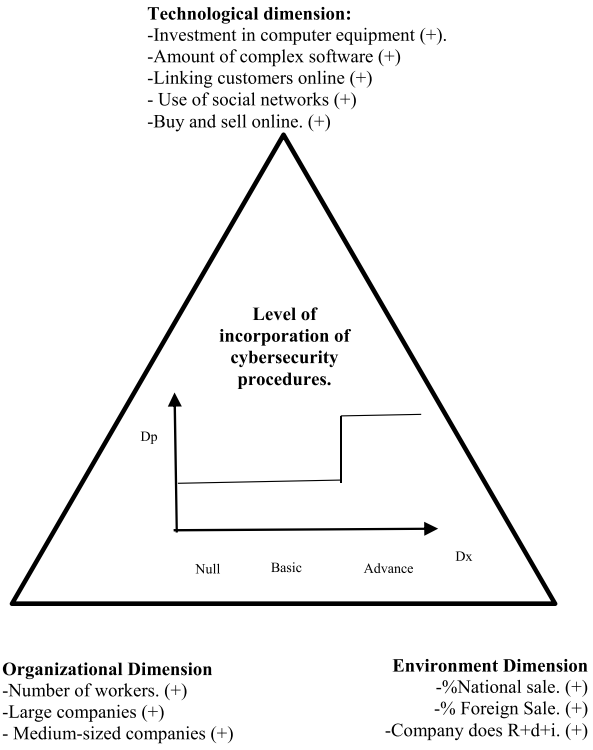

FIGURE 2. Variables explaining the level of incorporation by dimension TOE. Source: own elaboration based on the results.

- A very different case is the companies that carry out R + D + i presenting high levels of incorporation of cybersecurity procedures. This significant and positive relationship shows the importance of innovative trajectories and having an organizational culture prone to technical change, which aligns with what is indicated in the theoretical framework.

The new enabling technologies of Industry 4.0 will continue to increase across different national productive sectors, owing to their numerous business benefits. The implementation of these new 4.0 technologies offers opportunities in six key areas [36]: a) enhanced flexibility through small batch production, b) accelerated prototyping, c) reduced set-up costs and fewer errors, d) minimized downtime, e) improved product quality and reduced rejected production, and f) better customer feedback on products. Howeve it is essential to note that these digital technologies, being highly data-intensive, are also more vulnerable to various cyber-attacks [39].

A significant part of the drivers of adoption of cyber security procedures identified in our study are replicated with other Industry 4.0 enabling technologies. Therefore, we will have a ''co-evolution'' of adoption trajectories between new digital production technologies and cyber security procedures.

In this context, manufacturing businesses must recognize the advantages of integrating digital technology into their production processes while also appreciating the benefits it brings to their company and the entire production network. Securing data from the threats of cyber-attacks should be a top priority. Entrepreneurs must view cyber security not only as a necessity but also as a competitive advantage over their rivals.

The acceleration of co-evolution between industrial process enhancements and a higher standard of cyber security for company databases will be influenced by two key factors: firstly, the pressure from public policies in establishing standards, and secondly, the demands from larger companies acting as customers. These factors will play a significant role in adopting robust cyber security measures across the industry.

VII. CONCLUSION

The conclusions will be divided into three parts: regarding the methodology, regarding public policies, and regarding a new adoption model for cybersecurity.

A. THE METHODOLOGY AND LINES OF FUTURE RESEARCH

The first conclusion we can obtain is associated with the research limits. Agreeing with what was proposed by [21], the generic TOE model by itself does not allow us to understand the adoption of cybersecurity procedures because there are qualitative elements associated with the perception of those responsible for ICTs about the existing risks either by unknown, hypothetical and intangible threats and secondly, to the political dimension by establishing mandatory cybersecurity procedures, which must be respected by the different actors, which implies coordinating, educating, raising awareness or punishing if they are not fulfilled promptly.

It is pertinent that the surveys better record some critical elements in the cyber security of companies, for example: a) the existence of staff training in cyber security, b) the level of knowledge of ISO 27001 cyber security standards, c) the existence of procedures before, during and after cyber-attacks, d) the presence of ''risk maps'' where the threat and impact of cyber-attacks on key assets is assessed, e) the frequency of backups, among other aspects.

Although the ELE 5 survey evaluates certain cyber security aspects such as the adoption of technologies to reinforce access control to the buildings of a company, in no case, did this survey asked if an organization carries out cybersecurity awareness and training for its workers. Nor does it address prevention aspects that would diagnose if workers can identify possible attempts at phishing, smishing, and ransomware attacks (the most reported attacks in Chile). Moreover, the survey does not determine whether manufacturing companies are interested in including cybersecurity standards and good practices beyond those regulated in their sector.

Upon reviewing the existing literature, we observed a scarcity of studies analyzing the adoption of cybersecurity among a group of companies. We believe that our research makes a significant contribution in this field for several reasons: i) Our study examines explanatory factors based on a comprehensive sample of 574 companies, utilizing classical

multivariate analysis methodologies (Logit and Probit), ii) It addresses the cybersecurity challenge by employing a well-established adoption model (TOE), providing valuable insights into the adoption process y iii) furthermore, our research delves into the cybersecurity concerns specific to a developing country, which faces technological gaps in comparison to more developed nations. This aspect adds a valuable dimension to understanding cybersecurity practices in diverse socio-economic contexts.

We identify the following lines of future research:

- It is necessary to look at the links between companies to identify the extent to which a large company (e.g., an exporter) puts pressure on an SME to adopt specific cybersecurity standards. Knowledge of the productive fabric will make it possible to estimate the diffusion speed of new technologies and cybersecurity procedures.
- It is relevant to know the interrelationships between technologies within companies. This implies identifying for each specific technology (e.g., SCADA, IoT; PLC, EWS, etc.) the level of risk of cyber-attack. Due to their high interoperability, it is interesting to identify how new 4.0 technologies can be a ''gateway'' for cyber attackers, affecting the entire operational network of the manufacturing company and its production environment.
- It is necessary to visualize where the SME can start to strengthen its cybersecurity (procedures and facilities). In our opinion, an interesting topic to address is the ''technology trajectories'' for each type of company, distinguishing the size, industrial sector, and strategic content of its production.

It is essential to establish international research networks focused on studying cybersecurity in the industry from a global perspective, aiming to: i) develop specific tools for identifying the current state of cybersecurity in manufacturing (e.g., surveys, incident reports, among others), ii) identify new common patterns in cyberattacks, and iii) determine new protocols for prevention, response, and business continuity.

Currently, various international organizations are involved in cybersecurity efforts, such as the United Nations (UN), the International Telecommunication Union (ITU), the Cybersecurity Center in Madrid (CCMAD), the National Institute of Cybersecurity in Spain (INCIBE), the Open Web Application Security Project (OWASP), the CSIRT of Chile, among others. There is a need to establish a global research network since cyber attackers do not respect traditional national boundaries.

B. REGARDING PUBLIC POLICIES AND ISO 27001

In the Chilean context, there is an emerging institutional framework for cybersecurity. Notably, the Computer Security Incident Response Team (CSIRT) was established in 2018, and currently, there are ongoing discussions in the Chamber of Deputies to enact the first Framework Law on Cybersecurity. Given this landscape, it becomes paramount to foster a ''cybersecurity culture'' [22] by promoting the dissemination of procedures within organizations, integrating them into the fabric of production processes, and particularly among citizens. Citizens, in their roles as customers, can play a vital role in encouraging companies to enhance their security standards. Simultaneously, they can exert pressure on the State to improve regulatory frameworks that involve fines and sanctions. Instilling such a cybersecurity culture across different levels of society will create a more robust and secure digital environment, benefitting both the private and public sectors in Chile.

The State can also help disseminate and encourage the use of cybersecurity standards at the company level (e.g., tax incentives, public procurement systems, etc.) as a condition for accessing key customers in international markets, which is especially necessary for SMEs [19].

In this regard, the government, in collaboration with other key stakeholders including businesses and universities, should implement a National Cybersecurity Plan for manufacturing Small and Medium-sized Enterprises (SMEs). This initiative should commence with a comprehensive survey of the sector during its diagnostic phase and should culminate in public policies aimed at strengthening cybersecurity. This entails enhancing incident monitoring through the establishment of a new Manufacturing CSIRT (Computer Security Incident Response Team), fostering the development of new technology providers, providing training, implementing certification of standards (ISO 27001 and NIST), and raising awareness within each company.

Finally, ISO 27001 presents several guidelines for implementing an information security management system to manage risks and establish control measures to protect an organization's information assets, including the TOE model's dimensions.

- Technology. According to the standard, the use of technology is intended to support critical activities and that it will be able to allow the organization to meet its objectives. The standard promotes using cryptography for storing data in transit and at rest, using semi-automated technological equipment, processes, and physical security monitoring mechanisms. The use of good practices and the use and development of software are promoted, as well as establishing protocols that direct the continuity and recovery of an organization in the event of a security incident.
- Organization**:** ISO 27001 advises that the risk management process be wholly aligned with the culture, processes, structure, and strategy of the organization. Each member of the organization must have clear roles and accountability. There must be clear policies, standards, guidelines, and documented models known and practiced by its members. For this, senior management must demonstrate an exemplary and committed attitude, encouraging the continuous improvement of all the resources that support the organization.
- Environment**:** The standard highlights the importance that the organization knows the needs and expectations

of its stakeholders (employees, customers, suppliers, investors, etc.) and the social, cultural, legal, financial, and competitive environments at national and international levels where it operates. Must identify critical aspects of the business and trends that impact the organization's goals.

Although some aspects indicated by ISO 27001 were analyzed in this article, as future lines of work, we hope to deepen under its eaves in the study of the Chilean manufacturing industry according to the dimensions of the TOE model.

C. REGARDING AN APPROPRIATE ADOPTION MODEL

We believe the generic TOE (Technology, Organization, and Environment) model can adopt cybersecurity procedures when the following key factors are included:

1. **Technological factors** encompass the availability, maturity, and effectiveness of cybersecurity technologies and solutions. This includes the existence of robust security tools, frameworks, and standards that can be leveraged to protect an organization's technology infrastructure, systems, and data. The presence of advanced threat detection and prevention mechanisms, encryption technologies, and secure communication protocols can significantly influence the adoption of cybersecurity procedures.
2. **Organizational factors** affect an organization's internal structures, processes, and capabilities. These factors include dedicated cybersecurity teams, well-defined roles, responsibilities, and allocating sufficient resources and budget for cybersecurity initiatives. Additionally, the organization's commitment to creating a cybersecurity culture and fostering awareness among employees plays a vital role in determining the success of adopting cybersecurity procedures.
3. **Human factors** refer to the knowledge, skills, and attitudes of individuals within the organization. This includes the level of cybersecurity awareness, training, and education provided to employees. The willingness and motivation of employees to adhere to cybersecurity best practices, such as strong password management, regular updates, and vigilant behavior, greatly impact the successful adoption of cybersecurity procedures.
4. **Regulatory and compliance factors** encompass the legal and regulatory requirements that organizations must adhere to regarding cybersecurity. These may include industry-specific regulations, privacy laws, data protection requirements, and international standards such as ISO 27001. The need to comply with these regulations provides a strong incentive for organizations to adopt cybersecurity procedures
5. **Environmental factors:** consider the external influences on an organization's cybersecurity posture. This includes the evolving threat landscape, emerging cybersecurity risks, and the overall security climate within the organization's industry or geographical region. High-profile cyber incidents and public awareness of cybersecurity issues can influence organizations to adopt cybersecurity procedures to protect against potential threats and reputational damage.
6. **Economic factors:** pertain to the financial aspects of cybersecurity adoption. This includes the cost of implementing cybersecurity measures, the return on investment (ROI) associated with cybersecurity investments, and the cost of potential breaches or incidents. Organizations must evaluate the financial viability and long-term benefits of adopting cybersecurity procedures about their overall business goals and risk tolerance.

Considering these factors within the TOE model, we believe organizations can assess their readiness and capacity to adopt cybersecurity procedures effectively. The interaction and alignment of technological, organizational, human, regulatory, compliance, environmental, and economic factors determine the level of cybersecurity maturity and the extent to which cybersecurity procedures can be adopted and integrated into an organization's operations.

APPENDIX A
CORRELATION MATRIX FOR NONPARAMETRIC VARIABLES

Kendall's tau correlation coefficient

	a)	b)	c)	d)	e)	f)	g)	h)	i)	j)	k)	l)	m)	n)	o)	p)	q)	r)	s)	t)	u)	v)
a)		0,0	0,1	0,0	0,0	0,2	0,1	0,1	0,2	0,2	0,1	0,3	0,0	0,0	0,0	0,0	0,3	0,0	0,0	-0,2	**0,1**	**0,1**
b)	0,0		0,0	0,0	0,0	-0,1	0,0	0,0	0,0	0,0	0,0	0,0	-0,1	0,0	0,0	0,0	0,0	0,0	0,1	-0,1	**0,0**	**0,1**
c)	0,1	0,0		0,4	0,1	0,2	0,2	0,2	0,2	0,4	0,2	0,2	0,1	0,2	0,2	0,1	0,3	0,0	-0,1	-0,2	**0,4**	**0,3**
d)	0,1	0,0	0,4		0,0	0,1	0,1	0,2	0,2	0,3	0,2	0,2	0,1	0,2	0,1	0,1	0,3	0,0	-0,1	-0,1	**0,2**	**0,2**
e)	0,0	0,0	0,1	0,0		-0,2	-0,1	0,0	0,0	0,1	0,1	0,1	0,1	-0,1	0,0	0,1	0,1	-0,1	0,0	**0,2**	**0,2**
f)	0,3	-0,1	0,2	0,2	-0,2		0,1	0,3	0,3	0,4	0,3	0,4	0,1	0,1	0,1	0,0	0,5	0,0	-0,1	-0,2	**0,3**	**0,3**
g)	0,1	0,0	0,2	0,1	-0,1	0,1		0,1	0,1	0,1	0,1	0,0	0,1	0,1	0,1	0,2	0,0	0,1	0,0	0,0	**0,1**	**0,1**
h)	0,1	0,0	0,2	0,2	0,0	0,3	0,1		0,2	0,3	0,2	0,3	0,1	0,1	0,1	0,1	0,3	0,1	0,0	-0,2	**0,3**	**0,2**
i)	0,2	0,0	0,2	0,2	0,0	0,3	0,1	0,3		0,4	0,2	0,3	0,1	0,2	0,1	0,2	0,4	0,0	-0,1	-0,2	**0,3**	**0,3**
J)	0,3	0,1	0,4	0,3	0,2	0,4	0,1	0,4	0,4		0,3	0,6	0,2	0,2	0,2	0,1	0,6	0,1	-0,1	-0,4	**0,5**	**0,4**
k)	0,1	0,0	0,2	0,2	0,1	0,3	0,1	0,2	0,2	0,3		0,2	0,2	0,2	0,1	0,2	0,3	0,0	-0,1	-0,1	**0,3**	**0,3**
l)	0,4	0,0	0,3	0,2	0,1	0,5	0,0	0,4	0,4	0,7	0,3		0,1	0,2	0,1	0,1	0,6	0,1	0,0	-0,4	**0,5**	**0,4**
m)	0,0	-0,1	0,2	0,1	0,2	0,2	0,1	0,1	0,1	0,2	0,2	0,1		0,2	0,0	0,1	0,1	0,0	0,0	0,0	**0,2**	**0,1**
n)	0,0	0,0	0,2	0,2	0,2	0,1	0,1	0,2	0,2	0,3	0,2	0,2	0,2		0,2	0,2	0,2	0,1	0,0	-0,2	**0,3**	**0,3**
o)	-0,1	0,0	0,2	0,1	-0,1	0,1	0,1	0,1	0,1	0,2	0,1	0,1	0,0	0,2		0,3	0,1	0,0	-0,1	0,0	**0,3**	**0,2**
p)	0,0	0,0	0,1	0,1	0,0	0,0	0,2	0,1	0,2	0,1	0,2	0,1	0,1	0,2	0,3		0,0	0,1	0,0	0,0	**0,2**	**0,2**
q)	0,4	0,0	0,3	0,3	0,1	0,5	0,0	0,4	0,4	0,7	0,3	0,7	0,1	0,2	0,1	0,0		-0,2	-0,3	-0,4	**0,5**	**0,4**
r)	0,0	0,0	0,0	0,0	0,1	0,0	0,1	0,1	0,0	0,1	0,0	0,2	0,0	0,1	0,0	0,1	-0,2		-0,1	-0,2	**0,1**	**0,1**
s)	0,0	0,1	-0,1	-0,1	-0,1	-0,1	0,0	0,0	-0,1	-0,2	-0,1	0,0	0,0	0,0	-0,1	0,0	-0,3	-0,1		-0,3	**-0,1**	**-0,1**
t)	-0,2	-0,1	-0,2	-0,1	-0,1	-0,3	0,0	-0,3	-0,2	-0,4	-0,1	-0,4	0,0	-0,2	0,0	0,0	-0,4	-0,2	-0,3		**-0,3**	**-0,2**
u)	**0,2**	**0,0**	**0,4**	**0,2**	**0,2**	**0,4**	**0,1**	**0,3**	**0,3**	**0,6**	**0,3**	**0,6**	**0,2**	**0,3**	**0,3**	**0,2**	**0,6**	**0,1**	**-0,1**	**-0,3**		**0,8**
v)	**0,1**	**0,1**	**0,3**	**0,2**	**0,2**	**0,3**	**0,1**	**0,3**	**0,3**	**0,5**	**0,3**	**0,5**	**0,2**	**0,3**	**0,2**	**0,2**	**0,4**	**0,1**	**-0,1**	**-0,2**	**0,9**	

Spearman's correlation coefficient

(a) Seniority
(b) Family business (Binary)
(c) Investment in computer equipment (Binary)
(d) Investment in software (Binary)
(e) % Domestic sale
(f) % Foreign sale
(g) % Sale to the state
(h) Number of major suppliers
(i) Participation in Trade Associations, Universities, and Productive Development Systems (Binary)
(J) Number of complex software (office software is excluded)
(k) Does R+D+i
(L) Total number of workers
M) Percentage of skilled workers.
(n) Uses the Internet to link with clients (binary)
(o) The company uses the RRSS (binary)
(P) Buy and sell online (binary)
(q) Large company (binary)
(r) Medium-sized enterprise (binary)
(s) Small Business 1 (binary)
(t) Small Business 2 (binary)
(u) Discreet security practices
(v) Binary security practices

Own elaboration from the ELE.

APPENDIX B

- CIA: Security model, Confidentiality, Integrity, and Availability

- IoT: Internet of Things
- SCADA: Supervisory Control and Data Acquisition
- BWM: Best-Worst Method
- CRITIC: CRiteria Importance Through Intercriteria Correlation
- TOPSIS: Technique for Order of Preference by Similarity to Ideal Solution
- IPSOS: Independent Polling System Of Society
- ISO: International Organization for Standardization
- NIST: National Institute of Standards and Technology
- ANSI/ISA: American National Standards Institute Instrument Society of America
- TOE: Technology, Organization, and Environment model
- PLC: Programmable Logic Controller
- EWS: Exchange Web Services
- CSIRT: Computer Security Incident Response Team
- ROI: Return on Investments

REFERENCES

[1] H. Lasi, *Industry 4.0. Business & Information Systems Engineering*, no. 6. Cham, Switzerland: Springer, 2014, pp. 239–242.
[2] M. Castillo-Vergara, A. Álvarez-Marín, E. V. Pinto, and L. E. Valdez-Juárez, "Technological acceptance of industry 4.0 by students from rural areas," *Electronics*, vol. 11, no. 14, p. 2109, Jul. 2022.
[3] M. Dini, N. Gligo, and A. Patiño, "Transformación digital de las mipymes: Elementos para el diseño de políticas," Comisión Económica para América Latina y el Caribe (CEPAL), Documentos de Proyectos (LC/TS.2021/99), Santiago, CL, USA, Tech. Rep. 99, pp. 1–61, 2021.
[4] A. Corallo, M. Lazoi, and M. Lezzi, "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," *Comput. Ind.*, vol. 114, Jan. 2020, Art. no. 103165.
[5] A. Spadafora. (2019). *Industry 4.0 is Suffering Major Security Issues*. [Online]. Available: https://www.techradar.com/news/industry-40-suffering-major-security-issues
[6] Tecnova. (2019). *Ciberseguridad: Están protegidas las empresas en Chile?* [Online]. Available: https://www.tecnova.cl/2019/12/05/ciberseguridad-estan-protegidas-las-empresas-en-chile/
[7] *Norma Chilena NCh-ISO 27001*, Standard ISO 27001, 2013.
[8] A. Mahn. (2021). *Primeros Pasos de NIST Marco de Ciberseguridad: Guía de Inicio rápido*. [Online]. Available: https://doi.org/10.6028/NIST.SP.1271es
[9] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for industry 4.0 in the current literature: A reference framework," *Comput. Ind.*, vol. 103, pp. 97–110, Dec. 2018.
[10] A. Calabrese, R. Costa, L. Tiburzi, and A. Brem, "Merging two revolutions: A human-artificial intelligence method to study how sustainability and industry 4.0 are intertwined," *Technol. Forecasting Social Change*, vol. 188, Mar. 2023, Art. no. 122265.
[11] J. P. Tamvada, S. Narula, D. Audretsch, H. Puppala, and A. Kumar, "Adopting new technology is a distant dream? The risks of implementing industry 4.0 in emerging economy SMEs," *Technol. Forecasting Social Change*, vol. 185, Dec. 2022, Art. no. 122088.
[12] M. Ghobakhloo, "Determinants of information and digital technology implementation for smart manufacturing," *Int. J. Prod. Res.*, vol. 58, no. 8, pp. 2384–2405, Apr. 2020.
[13] M. Amin, F. Al-Obeidat, A. Tubaishat, B. Shah, S. Anwar, and T. A. Tanveer, "Cyber security and beyond: Detecting malware and concept drift in AI-based sensor data streams using statistical techniques," *Comput. Electr. Eng.*, vol. 108, May 2023, Art. no. 108702.
[14] G. Bravos, "Cybersecurity for industrial Internet of Things: Architecture, models and lessons learned," *IEEE Access*, vol. 10, pp. 124747–124765, 2022.
[15] G. D. Goh, S. L. Sing, and W. Y. Yeong, "A review on machine learning in 3D printing: Applications, potential, and challenges," *Artif. Intell. Rev.*, vol. 54, no. 1, pp. 63–94, Jan. 2021.
[16] S. Tiwari, "Blockchain and third-party logistics for global supply chain operations: Stakeholders' perspectives and decision roadmap," *Transp. Res. E, Logistics Transp. Rev.*, vol. 170, Feb. 2023, Art. no. 103012.
[17] P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17578–17598, 2019.
[18] E. Maia, S. Wannous, T. Dias, I. Praça, and A. Faria, "Holistic security and safety for factories of the future," *Sensors*, vol. 22, no. 24, p. 9915, Dec. 2022.
[19] N. Sun, C.-T. Li, H. Chan, M. Z. Islam, M. R. Islam, and W. Armstrong, "How do organizations seek cyber assurance? Investigations on the adoption of the common criteria and beyond," *IEEE Access*, vol. 10, pp. 71749–71763, 2022.
[20] E. Rogers, *Diffusion of Innovations*. New York, NY, USA: The Free Press, 1995.
[21] S. Wallace, K. Y. Green, C. M. Johnson, J. T. Cooper, and C. M. Gilstrap, "An extended TOE framework for cybersecurity adoption decisions," *Commun. Assoc. Inf. Syst.*, vol. 47, pp. 338–363, 2020.
[22] B. Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, "Developing a cyber security culture: Current practices and future needs," *Comput. Secur.*, vol. 109, Oct. 2021, Art. no. 102387.
[23] C. Arnold, J. Veile, and K. Voigt, "What drives industry 4.0 adoption? An examination of technological, organizational, and environmental determinants," in *Proc. Int. Assoc. Manag. Technol. (IAMOT)*, 2018, pp. 1–19.
[24] M. Ingaldi and R. Ulewicz, "Problems with the implementation of industry 4.0 in enterprises from the SME sector," *Sustainability*, vol. 12, no. 1, pp. 1–18, Dec. 2019.
[25] D. Horváth and R. Z. Szabó, "Driving forces and barriers of industry 4.0: Do multinational and small and medium-sized companies have equal opportunities?" *Technol. Forecasting Social Change*, vol. 146, pp. 119–132, Sep. 2019.
[26] I. Brambilla, "Digital technology adoption and jobs: A model of firm heterogeneity," World Bank Policy Res., Working Paper 8326, Jan. 2018. [Online]. Available: https://ssrn.com/abstract=3115833
[27] L. S. Dalenogare, G. B. Benitez, N. F. Ayala, and A. G. Frank, "The expected contribution of industry 4.0 technologies for industrial performance," *Int. J. Prod. Econ.*, vol. 204, pp. 383–394, Oct. 2018.
[28] P. M. Reyes, S. Li, and J. K. Visich, "Determinants of RFID adoption stage and perceived benefits," *Eur. J. Oper. Res.*, vol. 254, no. 3, pp. 801–812, Nov. 2016.
[29] C. Günther and M. Prause, "Technology diffusion of industry 4.0: An agent-based approach," *Int. J. Comput. Econ. Econometrics*, vol. 9, nos. 1–2, p. 29, 2019.
[30] J. Motta, H. Moreno, and R. Ascúa, "Industria 4.0 en MIPYMES manufactureras de la Argentina," Documentos de Proyectos (LC/TS.2019/93), Santiago de Chile, Comisión Económica para América Latina y el Caribe (CEPAL), Tech. Rep. 93, pp 1–68, 2019.
[31] C. Maggi, M. Ramos, and R. Vergara, "Adopción de tecnologías digitales 4.0 por parte de pequeñas y medianas empresas manufactureras en la región del biobío (Chile)," Documentos de Proyectos (LC/TS.2020/133), Santiago de Chile, Comisión Económica para Amórica Latina y el Caribe (CEPAL), Tech. Rep. 133, pp 1–65, 2020.
[32] F. E. G. Neira and M. A. R. Maldonado, "Políticas públicas y redes para el desarrollo delas tecnologías 4.0 en Chile," Paakat, Revista de Tecnología y Sociedad, Universidad de Guadalajara," México, 2020, vol. 10, no. 19, doi: 10.32870/Pk.a10n19.475.
[33] L. Agostini and R. Filippini, "Organizational and managerial challenges in the path toward industry 4.0," *Eur. J. Innov. Manage.*, vol. 22, no. 3, pp. 406–421, Jun. 2019.
[34] C. Rojas-Córdova, B. Heredia-Rojas, and P. Ramírez-Correa, "Predicting business innovation intention based on perceived barriers: A machine learning approach," *Symmetry*, vol. 12, no. 9, p. 1381, Aug. 2020.
[35] R. Berger, "España 4.0. El reto de la transformación digital de la economía," Tech. Rep., 2016.
[36] G. Büchi, M. Cugno, and R. Castagnoli, "Smart factory performance and industry 4.0," *Technol. Forecasting Social Change*, vol. 150, Jan. 2020, Art. no. 119790.
[37] F. Malerba and M. McKelvey, "Knowledge-intensive innovative entrepreneurship integrating schumpeter, evolutionary economics, and innovation systems," *Small Bus. Econ.*, vol. 54, no. 2, pp. 503–522, Feb. 2020.
[38] M. Kossaï, M. L. L. de Souza, Y. B. Zaied, and P. Nguyen, "Determinants of the adoption of information and communication technologies (ICTs): The case of Tunisian electrical and electronics sector," *J. Knowl. Economy*, vol. 11, no. 3, pp. 845–864, Sep. 2020.

[39] M. Bendel, *Ciberamenazas en Redes Industriales*. Santiago, CL, USA: CSIRT-Chile, 2021.
[40] *Global Cybersecurity Index. Measuring Commitment to Cybersecurity*, ITU Publications, Geneva, Switzerland, 2020.
[41] E. Battistoni, S. Gitto, G. Murgia, and D. Campisi, "Adoption paths of digital transformation in manufacturing SME," *Int. J. Prod. Econ.*, vol. 255, Jan. 2023, Art. no. 108675.
[42] S. Siegel and N. J. Castellan, *Estadística no Paramétrica*, vol. 437. México: Editorial Trillas, 1998.
[43] M. Ortega-Calvo and A. Cayuela-Domínguez, "Regresión logística no condicionada y tamaño de muestra: Una revisión bibliográfica," *Revista Española de Salud Pública*, vol. 76, no. 2, pp. 85–93, 2002.
[44] *National Institute of Statistics*, Longitudinal Survey of Companies ELE, Ministry of Economy, Government of Chile, Santiago, CL, USA, 2019. [Online]. Available: https://www.economia.gob.cl/2019/03/12/quinta-encuesta-longitudinal-de-empresas-ele5.htm
[45] Gretl. *Gretl: Gnu Regression, Econometrics and Time-Series Library for Microsoft Windows*. Accessed: Nov. 27, 2023. [Online]. Available: http://gretl.sourceforge.net/win32/index_es.html

FRANCISCO GATICA-NEIRA received the Ph.D. degree in economics and management of innovation and technology policies from the Complutense University of Madrid and the degree in commercial engineering from the University of Bío-Bío. He is currently an Associate Professor with the Department of Economics and Finance, University of Bío-Bío. He is a bachelor's and master's Professor at various universities. He has participated in Fondecyt, FNDR, FIC GORE Bío-Bío projects, and various technology transfer initiatives. He has published articles in national and foreign journals. He was a member of the Board of Directors of the Science and Technology Park of the Regional Government of Bío-Bío and the University of Concepción (Pacyt) and the Board of Directors of the Corporation for the Regionalization of Bío-Bío (Corbiobio). He has been the Director of Finance, the General Director of Institutional Analysis, and the Vice-Chancellor of Economic Affairs of the University of Bío-Bío. He belongs to the Research Group on Intelligent Industry and Complex Systems (Giscom). He also participates in the panel of experts of the Regional Development Strategy of Bío-Bío. He is also a Researcher of the FIC Project "Sustainable digital transformation for manufacturing SMEs in the Bío-Bío industry 4.0, industrial analysis, and local economy."

PATRICIO GALDAMES-SEPULVEDA received the B.S. degree in electrical engineering from Universidad de Chile, in 1998, and the M.S. and Ph.D. degrees in computer science from Iowa State University, Ames, IA, USA, in 2008 and 2012, respectively.

Since 2023, he has been a part-time Lecturer with Universidad San Sebastian, Chile. He has published many research articles in several international journals and has participated in international research conferences and technology transfer projects in Chile. He was a full-time Faculty Member of the Department of Information Systems and a member of the Research Group on Intelligent Industry and Complex Systems (Giscom), University of Bío-Bío. He is currently a Researcher of the FIC Project "Sustainable digital transformation for manufacturing SMEs in the Bío-Bío industry." His research interests include mobile computing, machine learning, and data privacy and security.

MARIO RAMOS-MALDONADO received the degree in mechanical civil engineering from Universidad Técnica Federico Santa María, and the D.E.A. and Ph.D. degrees in production automation from Université Henri Poincaré Nancy I, France. He has been an Academician with the University of Bío-Bío (UBB), since 1988. He has developed his activity with the Faculty of Engineering, in intelligent industry, operations management, and automation with applications in the manufacturing and process industry. He teaches undergraduate and graduate courses, with several publications in scientific journals and presentations at national and international conferences. He has led and participated in research and development projects Fondecyt, FONDEF, FIC Regional, CYTED, and CORFO, and various consultancies to companies. He has experience in industrial policies, innovation management, and higher university management. He has been the General Director of Research, Development and Innovation (DGI) and the Vice Rector of Research and Graduate Studies. He currently participates and directs research projects with industry, CORFO, and the Ministry of Science, in the field of artificial intelligence, manufacturing, and processes. He teaches in several careers and master and doctoral programs. He is a part of the editorial committee of the journal *Maderas Ciencia y Tecnología* and a member of the Chilean Institute of Operations Research (ICHIO). He coordinates the Intelligent Industry and Complex Systems Research Group. He is currently the Director of the Department of Wood Engineering, UBB, and directs the FIC projects: "Digital transformation for SMEs in the Bío-Bío region" and Fondef [National Agency for Research and Development (ANID)]: "Prescriptive analysis and machine learning for the high productivity plywood industry."