ISSN 1680-8754

SERIES

PRODUCTION DEVELOPMENT 228

State of cybersecurity in logistics in Latin America and the Caribbean

Rodrigo Mariano Díaz

UNITED NATIONS

ECLAC

Thank you for your interest in this ECLAC publication

Please register if you would like to receive information on our editorial products and activities. When you register, you may specify your particular areas of interest and you will gain access to our products in other formats.

Register

UNITED NATIONS

ECLAC

www.cepal.org/en/publications

facebook.com/publicacionesdelacepal

www.cepal.org/apps

SERIES

PRODUCTION DEVELOPMENT | 228

State of cybersecurity in logistics in Latin America and the Caribbean

Rodrigo Mariano Díaz

UNITED NATIONS

ECLAC

This document was prepared by Rodrigo Mariano Díaz, a consultant with the Division of Production, Productivity and Management of the Economic Commission for Latin America and the Caribbean (ECLAC), under the coordination of Georgina Núñez, Economic Affairs Officer in the Unit on Investment and Corporate Strategies of the same Division, and Ricardo Sánchez, Chief of the Infrastructure Services Unit of the International Trade and Integration Division of ECLAC.

The coordinators and the author would like to thank Felipe Harboe, a lecturer in data protection in the Diploma course in Compliance and Good Corporate Practices of the Pontifical Catholic University of Chile, for his comments on the final draft of this document.

The views expressed in this document, which has been reproduced without formal editing, are those of the author and do not necessarily reflect the views of the Organization or the countries it represents.

United Nations publication
ISSN: 1680-8754 (electronic version)
ISSN: 1020-5179 (print version)
LC/TS.2021/108
Distribution: L

Printed at United Nations, Santiago
S.21-00687

This publication should be cited as: R. Díaz, "State of cybersecurity in logistics in Latin America and the Caribbean", *Production Development series*, No. 228 (LC/TS.2021/108), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC), 2021.

Contents

Summary 5
Introduction 7
I. Cybersecurity incidents in logistics chains 11
II. The evolution of ransomware 23
III. Analysis of the causes of incidents 25
IV. The situation in logistics organizations 27
V. A technical overview of the current situation 31
VI. Cyberresilience practices 33
VII. Cyberimmunity, a cybersecurity strategy for post-pandemic recovery 35
Bibliography 39
Annexes 41
Annex 1 42
Annex 2 45
Annex 3 48
Annex 4 51
Annex 5 54
Annex 6 57
Annex 7 60
Annex 8 63
Annex 9 66
Issues published 69

Table

Table 1 Incidents in Latin America, by area of activity and country, 2020 12

Figures

Figure 1 Growth in Internet users, 2010–2020 8
Figure 2 Number of logistics incidents recorded, 2016–2020 11
Figure 3 Countries affected, by number of incidents 21
Figure 4 Impact on organizations 21
Figure 5 Average ransom demands by quarter, third quarter 2018–third quarter 2020 23
Figure 6 Causes of incidents 25
Figure 7 Age of exploited vulnerabilities 26
Figure 8 Incidents by organization size 27
Figure 9 Incident recovery time 28
Figure 10 Formalization of cybersecurity management 29
Figure 11 Organizational structure for security management 29
Figure 12 Level of confidence in cybersecurity controls implemented 31
Figure 13 Concerns by type of threat and target of attack 32
Figure 14 Organizations with a DRP 33
Figure A1 Situation in Argentina 42
Figure A2 Situation in Brazil 45
Figure A3 Situation in Chile 48
Figure A4 Situation in Colombia 51
Figure A5 Situation in Ecuador 54
Figure A6 Situation in Mexico 57
Figure A7 Situation in Panama 60
Figure A8 Situation in Peru 63
Figure A9 Situation in Uruguay 66

Summary

The dizzying changes that have been brought about by technologies of the fourth industrial revolution in the transition to logistics 4.0 will have an impact on countries, businesses, industries and society as a whole.

The COVID-19 pandemic has reduced production, exports and imports in Latin America and the Caribbean. At the same time, it has become a catalyst for digitization, accelerating the transition process and making it possible for operations to continue during lockdowns and enabling them gradually to recover, while also reducing interaction among people. In order to maintain their operational base, organizations have opened virtual branches in homes, allowing work to continue in home office mode.

In this context, powerful pre-existing cybersecurity threats are a reality. Since the beginning of the pandemic, in addition to the operational problems that have affected logistics centres, cyberattacks have increased, and logistics continues to be one of the hardest-hit economic sectors. Evidence shows an increase in cyberattacks in the last year, although complete information on critical infrastructure and logistics chains is not available.

Introduction

The main objective of this study is to carry out an assessment of the cybersecurity-related events that have occurred in the last five years, especially during the COVID-19 pandemic, in Latin America and the Caribbean in order to analyse technical trends in the region and thus be able to devise an action plan to support the recovery of the logistics sector, which is strongly linked to disruptive technologies of the fourth industrial revolution.

To that end, information has been collected in three ways. First, research was conducted, using secondary information collected from public and private organizations involved in preventing, detecting and fixing cybersecurity gaps in Latin America and the Caribbean. In addition, an inventory was compiled of known cybersecurity incidents in the region in the last five years that affected and have had an impact on the infrastructure of logistics chains or organizations. Finally, 46 directors and managers of logistics-related organizations in the region were surveyed about cybersecurity events during the last year and asked about their concerns and strategies for the next 12 months. For this purpose, a 23-question questionnaire was distributed to collect information on incidents in the last year and their impact, on the general preparedness of the directors' and managers' organizations and on their concerns for the next 12 months. The results are assessed in general for the Latin American and Caribbean region as a whole in chapter IV of this document. At the same time, the variations in the responses across the countries in which the organizations surveyed operate have been analysed individually and are presented in the annexes.

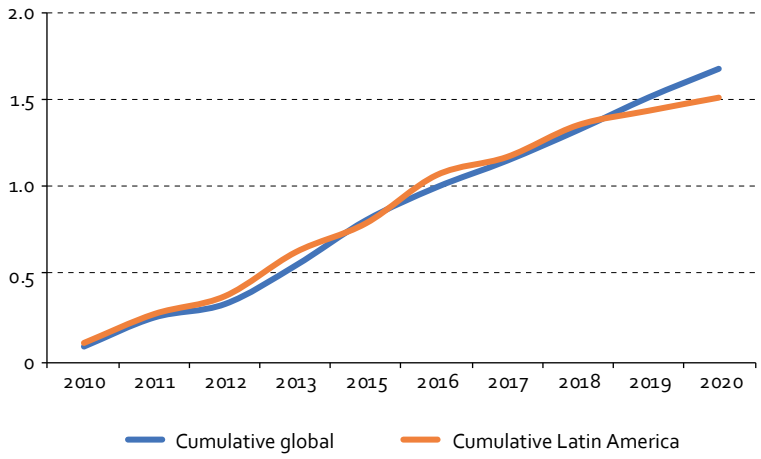
Logistics 4.0 during the COVID-19 pandemic and cybersecurity.

Key technologies of the fourth industrial revolution, such as the Internet of Things (IoT), automation, blockchain, big data and cloud computing, are driving logistics globally towards logistics 4.0, making it essential to address issues such as digital literacy, cost and speed of Internet access and cybersecurity. A study conducted by Barleta, Pérez and Sánchez (2019) explored the use and exploitation of data as a differentiator between businesses that have taken advantage of the digital transformation and those that, by not doing so, will face a serious risk to their survival, raising the question of whether this transformation will be the key to the new way of operating within the logistics sector.

COVID-19 has been an important catalyst for the digital transformation process, accelerating the pace and expanding the scale of adoption in response, in some cases, to the need to keep organizations running during the lockdown period that began in the region in March 2020. In other cases, digital technology

has allowed organizations to continue operating under strict protocols in order to reduce contagion. But in addition to the changes that have occurred over recent months, a strategic change is being seen in organizations with respect to technology. According to the International Data Group (IDG), an organization dedicated to strengthening the proper use of technology, the three priorities for organizations over the next 12 months are to lead the digital transformation, improve the experience of remote work for their organizations' personnel and upgrade cybersecurity to boost corporate resilience (IDG Communications, 2020). Alongside the acceleration of the digital transformation and the global economic depression, the cybercrime industry has grown in complexity, as a result of the use of machine learning and artificial intelligence tools, and in volume, through the malware-as-a-service (MaaS) market on the deep web. At the same time, the pandemic has led to a 1.5% annual increase in total Internet traffic and has changed usage habits, as evidenced by the fact that online transactions rose by 26.7% over the same time period (Clement, 2021). Meanwhile, the number of Internet users in the region has grown by 150% since 2010, as shown in figure 1, virtually matching the upward trend seen in the rest of the world (Johnson, 2020).

Figure 1
Growth in Internet users, 2010–2020
(Percentages)



Source: Prepared by the author, on the basis of data from Internet World Stats [online] www.internetworldstats.com.

Both the growth of supply in the cybercrime market and the increased use of technology in terms of number of Internet users and transactions, partly motivated by the continuation of human activities, resulted in a year-on-year increase of 67% in ransomware attacks, 71% in malware transmitted via secure web pages and 510% in attacks on the Internet of Things devices for the month of October 2020 (SonicWall, 2020).

This emerging scenario found the various countries in the region with differing degrees of maturity with regard to cyberdefence, and this was true in both the private and the public spheres. The phenomenon of cybercrime entails a complex process for communities, which begins with building awareness of the stark evidence of the scope and damaging effects of cyberattacks. In order to tackle this problem organically, in 2018 the International Telecommunication Union (ITU), a division of the United Nations, together with other organizations, drafted the *Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity*, which describes the role of the State in the development of a national cybersecurity strategy (NCS) (ITU, 2018). The NCS establishes national priorities and drives the allocation of resources, which is important for the discussion and formulation of appropriate legislation to fight and punish these crimes, on which the law in many cases is weak or absent.

The Budapest Convention, which was signed on 23 November 2001 in Budapest, Hungary, and entered into force on 1 July 2004, is the first international treaty conceived with the aim of **protecting society against cybercrime and Internet crime** through the development of appropriate laws, improved investigative techniques and increased international cooperation. It has served as a reference, first in the European Union and then elsewhere around the world, for the drafting of national laws to protect against cybercrime. The Convention has now been ratified by more than 50 nations globally. In Latin America and the Caribbean, Argentina, Chile, Colombia, Costa Rica, the Dominican Republic, Panama, Paraguay and Peru are Parties to this convention.

Once the strategic and legal stages have been addressed, countries enter the "possible" stage of implementing regulatory frameworks that will help mitigate the impact of cybercrimes on institutions, the economy and the lives of individuals in each country. Local cybersecurity regulations and standards thus become an essential element in managing cyberincidents, supported by the operational capacity of enforcement agencies, "operational capacity" being understood to mean the capacity to minimize the time that elapses between when an incident is detected and when action is taken to manage it.

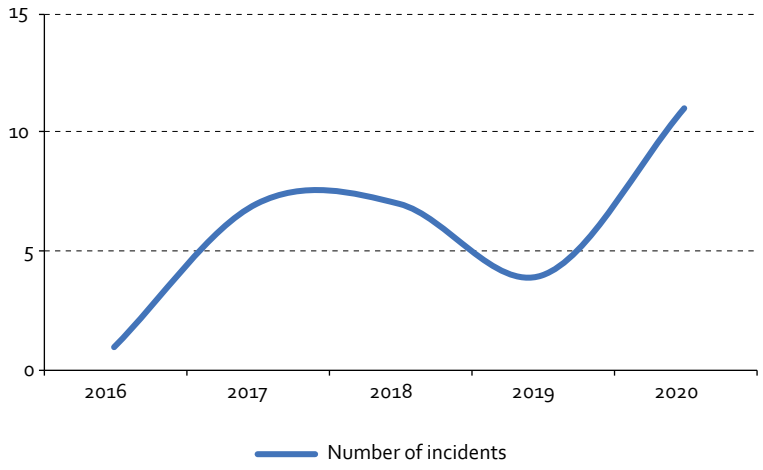
Alongside the NCS, cybersecurity incident response teams (CSIRTs), which may be formed in the academic, governmental, military or private spheres, serve as key operational hubs on which a state relies to minimize and control damage in the event of a cyberattack. At the same time, they advise, respond and restore normal operations and prevent the occurrence of future incidents (Cichonski and others, 2012).

I. Cybersecurity incidents in logistics chains

Based on the statistics mentioned in the previous section, and continuing work begun by ECLAC and published in December 2020 in *FAL Bulletin* No. 382 (Díaz, 2020), an inventory of reported and publicly disclosed cybersecurity incidents was compiled. The results are presented below.

According to the research conducted on organizations related to the logistics chain or whose activities may directly affect it, 30 publicly known incidents have been recorded over the last five years, 11 of which occurred during 2020. As can be seen in figure 2, that number is 57% higher than the number recorded in 2017 and 2018 —during which the spread of WannaCry and NotPetya ransomware strongly impacted on all types of industry, with highly publicized incidents occurring in the logistics and transport sector, such as the attack on the Maersk company, which suffered a loss of US$ 300 million— and 175% higher than in 2019. In other words, the number of incidents almost tripled from 2019 to 2020.

Figure 2
Number of logistics incidents recorded, 2016–2020



Source: Economic Commission for Latin America and the Caribbean (ECLAC).

Table 1
Incidents in Latin America, by area of activity and country, 2020

Date of incident 1	Argentina	Brazil	Chile	Colombia	Ecuador	Dominican Rep.	Mexico	Panama	Peru	Uruguay	Organization	Port name	Main activity	Pillar affected A: Availability C: Confidentiality I: Integrity			Type of incident	Description of incident	Impact		Note No.
														D	C	I			Qualitative	Quantitative (Dollars)	
20/5/2016					X						Banco del Austro		General banking			X	Zero-day vulnerability in the SWIFT network	Money transfers through the SWIFT network Control failures on the part of the network operator	Bank weakened by not keeping the network in question up to date	9 000 000	(1)
13/5/2017							X				Airports and auxiliary services		Airport management and operation	X			Wanna Decryptor ransomware	Server access blocked	No information available		(2)
13/5/2017		X									Petrobras		Producer, distributor and marketer of petroleum and petroleum products	X			WannaCry ransomware	Server access blocked	Various refineries		(3)
31/5/2017	X										Nidera – Puerto San Martín	Port of San Martín	Vegetable oil production and shipment	X			Ransomware	Commercial and logistics applications blocked	Truck unloading, oil production and shipment, merchandise purchases and transaction payments paralyzed		(4)
26/6/2017							X				APM Terminals México	Lázaro Cárdenas	Containers	X			GoldenEyes virus	Server access blocked	Operations had to be carried out manually; only unloading of containers could be done	900 000	(5)
27/6/2017	X	X	X	X			X	X	X	X	Maersk		Containers	X			Petya ransomware	Server access blocked	Affected all business units at Maersk: container shipping, port and tugboat operations, oil and gas production, drilling services and oil tanker services	300 000 000	(6)

Table 1 (continuation)

Date of incident 2	Argentina	Brazil	Chile	Colombia	Ecuador	Dominican Rep.	Mexico	Panama	Peru	Uruguay	Organization	Port name	Main activity	Pillar affected A: Availability C: Confidentiality I: Integrity			Type of incident	Description of incident	Impact		Note No.
														D	C	I			Qualitative	Quantitative (Dollars)	
27/6/2017									X		APM Terminals Callao	Callao	Containers General cargo Passengers	X			Petya ransomware	Server access blocked	Affected all business units: container shipping, port and tugboat operations		(7)
29/6/2017	X										Cofco Intl.	Timbues	Bulk cargo	X			Ransomware	Commercial and logistics applications blocked	Truck unloading, merchandise purchases and transaction payments paralyzed		(8)
28/12/2017		X									Clarkson Plc		General services		X		Password theft	Server access blocked	2% drop in the firm's stock		(9)
24/5/2018			X								Banco Estado (1)		General banking	X			Killdisk/ KillMBR malware	Inability to restart equipment	9000 PCs and 500 servers (on various platforms)		(10)
24/5/2018			X								Banco Estado (2)		General banking			X	Zero-day vulnerability in the SWIFT network	While the institution was engaged in resolving the malware affecting the computers, the attackers were making money transfers through the SWIFT network.	Bank weakened by not keeping the network in question up to date	10 000 000	(11)
17/7/2018	X	X	X	X			X	X	X	X	TNT Express		Logistics Courier and parcel delivery	X			Petya ransomware	Server access blocked	Initial downtime and subsequent delays in delivery service that impacted billing	300.000.000	(12)
24/7/2018	X	X	X					X	X	X	Cosco Shipping		Containers	X			Malware/ Ransomware	Email servers blocked	According to the company, this attack did not impact business continuity		(13)

Table 1 (continuation)

Date of incident 3	Argentina	Brazil	Chile	Colombia	Ecuador	Dominican Rep.	Mexico	Panama	Peru	Uruguay	Organization	Port name	Main activity	Pillar affected A: Availability C: Confidentiality I: Integrity			Type of incident	Description of incident	Impact		Note No.
														D	C	I			Qualitative	Quantitative (Dollars)	
17/8/2018									X		Asociación de Bancos del Perú (Asbanc)		General banking	X			SamSam ransomware	Server access blocked	The attack was detected while in progress at several institutions, so the impact, both generally and specifically in each institution, was not known		(14)
24/1/2019	X										Cooperativa 16 de Octubre		Company providing electric power, drinking water and sanitation services in the towns of Esquel and Trevelin (Chubut).	X			WannaCry ransomware	Access to billing, customer claims management and employee payroll applications blocked	Services provided by the company not affected, but the company lost control over them, incurring a major financial loss	3 000	(15)
2/7/2019			X								T.P.A. S.A.	Terminal Portuaria Arica	General	X			Malware	Websites, emails, billing and all Internet services had to be inactivated for virus detection	Operations had to be performed manually		(16)
2/7/2019			X								Puerto Angamos S.A.	Angamos	Minerals Containers	X			Malware	Websites, emails, billing and all Internet services had to be inactivated for virus detection	Operations had to be performed manually		(17)

Table 1 (continuation)

Date of incident 4	Argentina	Brazil	Chile	Colombia	Ecuador	Dominican Rep.	Mexico	Panama	Peru	Uruguay	Organization	Port name	Main activity	Pillar affected A: Availability C: Confidentiality I: Integrity			Type of incident	Description of incident	Impact		Note No.
														D	C	I			Qualitative	Quantitative (Dollars)	
2/7/2019			X								Terminal Pacifico Sur Valparaiso S.A.	Vaparaiso	Containers General cargo Passengers	X			Malware	Websites, emails, billing and all Internet services had to be inactivated for virus detection	Operations had to be performed manually		(18)
2/7/2019			X								Ultramar / Ultraport		Shipping agency	X			Malware	Websites, emails, billing and all Internet services had to be inactivated for virus detection	Operations had to be performed manually		(19)
10/11/2019							X				Pemex		Producer, distributor and marketer of petroleum and petroleum products.	X			Sodinokibi ransomware	Access to 5% of equipment blocked	Core processes (extraction, logistics, refining and marketing) were not affected	50 000 000	(20)
11/3/2020		X									Cosan Limited		Fuel producer, distributor and marketer	X			Nefilim ransomware	Server access blocked	All processes affected		(21)

Table 1 (continuation)

Date of incident 5	Argentina	Brazil	Chile	Colombia	Ecuador	Dominican Rep.	Mexico	Panama	Peru	Uruguay	Organization	Port name	Main activity	Pillar affected A: Availability C: Confidentiality I: Integrity			Type of incident	Description of incident	Impact		Note No.
														D	C	I			Qualitative	Quantitative (Dollars)	
30/3/2020						X					Autoridad Portuaria de la República Dominicana		Port authority			X	Strong	Alteration of the web page of the Port Authority of the Dominican Republic, injecting on it generic protest messages and a 404javascript.js file with the hacker's alias	Cyber-weakness affecting the organization's reputation		(22)
10/4/2020	X										Mediterranean Shipping Company Argentina	Port of Buenos Aires	Containers	X			Malware	Downtime on web platforms residing on headquarters servers (in Geneva)	When the headquarters servers went down, the Argentine subsidiary implemented contingency measures, providing services by alternative means.		(23)
8/6/2020		X									Light Energía S.A.		Electric power distributor	X			Sodinokibi ransomware	Server access blocked	Not reported	14 000 000	(24)
30/6/2020		X									CPFL Energía		Generation and distribution of electric power		X		Ransomware Maze	Server access blocked	Theft of sensitive information (estimated to have occurred from May to June 2020)		(25)

Table 1 (continuation)

Date of incident 6	Argentina	Brazil	Chile	Colombia	Ecuador	Dominican Rep.	Mexico	Panama	Peru	Uruguay	Organization	Port name	Main activity	Pillar affected A: Availability C: Confidentiality I: Integrity			Type of incident	Description of incident	Impact		Note No.
														D	C	I			Qualitative	Quantitative (Dollars)	
30/7/2020	X	X	X	X	X	X	X	X	X	X	Garmin		GPS manufacturing and support GPS for civilian use, mainly for land transit, but also for maritime and air traffic	X			WastedLocker ransomware	Server access blocked	For 5 days all users were left without geographic location support		(26)
3/8/2020							X				CIBanco		General banking		X		Sodinokibi ransomware	Server access blocked	Not reported		(27)
28/9/2020	X	X	X	X	X	X	X	X	X	X	CMA CGM		Containers	X	X		Malware	CMA CGM reported an alleged data breach following a cyberattack on its peripheral servers on Monday, 28 September, which prevented customers and users from accessing the shipping company's website and making use of its software applications	E-commerce site offline for 12 days		(28)

Table 1 (continuation)

Date of incident 6	Argentina	Brazil	Chile	Colombia	Ecuador	Dominican Rep.	Mexico	Panama	Peru	Uruguay	Organization	Port name	Main activity	Pillar affected A: Availability C: Confidentiality I: Integrity			Type of incident	Description of incident	Impact		Note No.
														D	C	I			Qualitative	Quantitative (Dollars)	
30/7/2020	X	X	X	X	X	X	X	X	X	X	Garmin		GPS manufacturing and support GPS for civilian use, mainly for land transit, but also for maritime and air traffic	X			WastedLocker ransomware	Server access blocked	For 5 days all users were left without geographic location support		(26)
3/8/2020							X				ClBanco		General banking		X		Sodinokibi ransomware	Server access blocked	Not reported		(27)
28/9/2020	X	X	X	X	X	X	X	X	X	X	CMA CGM		Containers	X	X		Malware	CMA CGM reported an alleged data breach following a cyberattack on its peripheral servers on Monday, 28 September, which prevented customers and users from accessing the shipping company's website and making use of its software applications	E-commerce site offline for 12 days		(28)

Table 1 (continuation)

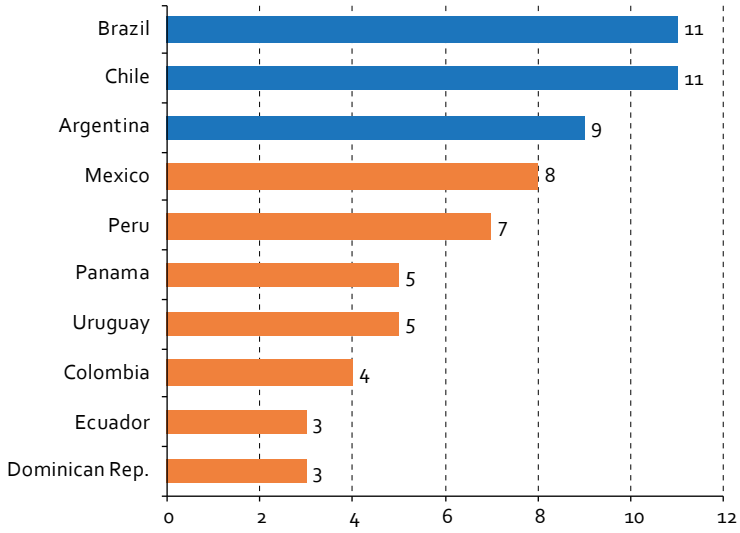
Date of incident 7	Argentina	Brazil	Chile	Colombia	Ecuador	Dominican Rep.	Mexico	Panama	Peru	Uruguay	Organization	Port name	Main activity	Pillar affected A: Availability C: Confidentiality I: Integrity			Type of incident	Description of incident	Impact		Note No.
														D	C	I			Qualitative	Quantitative (Dollars)	
28/9/2020	X	X	X	X	X	X	X	X	X	X	CMA CGM		Container transport	X	X		Ransomware Ragnar Locker	E-commerce servers	As soon as the security breach was detected, external access to the applications was suspended to prevent the malware from spreading		(29)
4/10/2020		X									Braskem		Petrochemicals Resins and other derivatives	X			Sodinokibi ransomware	Server access blocked	Delays in the delivery of products that impacted 45% of turnover during the disruption		(30)

Source: Prepared by the author, on the basis of information published on websites.Notes: (1) Hipertextual, "Banco ecuatoriano cae víctima de los cibercriminales", 20 May 2016 [online] https://hipertextual.com/2016/05/hackeo-banco-del-austro [accessed in November 2020].
(2) Xataca, "Wanna Decryptor, el ransomware que aterrorizó al mundo también llega a México", 15 May 201 [online] https://www.xataka.com.mx/ aplicaciones/wanna-decryptor-el-ransomware-que-aterrorizo-al-mundo-tambien-llego-a-mexico [accessed in November 2020].
(3) Sindipetro, "Petrobras tambiem, alvo do ataque global de hackers", 13 May 2017 [online] https://www.sindipetroprsc.org.br/site/index.php/noticias/item/2932-petrobras-tambem-e-alvo-do-ataque-global-de-hackers [accessed in November 2020].
(4) SAPEI, "Un ciberataque global dejó dos puertos de nuestra región sin poder operar", 31 May 2017 [online] https://www.sapei.com.ar/website/category/noticias--/477-un-ciberataque-global-dejo-dos-puertos-de-nuestra-region-sin-poder-operar;jsessionid=3420A364DF08C105DD4A7946A0A845DA [accessed in November 2020].
(5) El Sol de México, "Hackean sistema de empresa portuaria en Michoacán", 29 June 2017 [online] https://www.elsoldemexico.com.mx/republica/justicia/hackean-sistema-de-empresa-portuaria-en-michoacan-147426.html [accessed in November 2020].
(6) Portal Portuario, "Maersk calcula en USD 300 millones pérdidas generadas por ciberataque", 16 August 2017 [online] https://portalportuario.cl/maersk-calcula-usd-300-millones-perdidas-generadas-ciberataque/ [accessed in November 2020].
(7) Asociación Peruana de Agentes Marítimos, "Terminales del muelle norte del Puerto del Callao sufrieron ataque cibernético", 29 June 2017 [online] https://www.apam-peru.com/web/terminales-del-muelle-norte-del-puerto-del-callao-sufrieron-ataque-cibernetico/ [accessed in November 2020].
(8) SAPEI, "Un ciberataque global dejó dos puertos de nuestra región sin poder operar", 30 June 2017 [online] https://www.sapei.com.ar/website/category/noticias--/477-un-ciberataque-global-dejo-dos-puertos-de-nuestra-region-sin-poder-operar;jsessionid=3420A364DF08C105DD4A7946A0A845DA [accessed in November 2020].
(9) Noticias de ciberseguridad, "La naviera Clarksons víctima de un ciberataque", 28 December 2017 [online] https://blog.intec2.com/2017/12/la-naviera-clarksons-victima-de-un.html [accessed in November 2020].
(10) El hacker, "Banco de Estado Chileno víctima ataque ransomware Revil: cajeros cerrados", 7 September 2020 [online] https://blog.elhacker.net/2020/09/banco-de-estado-chile-victima-de-ransomware-Revil-Sodinokibi.html [accessed in November 2020].

(11) C. Farro, "Banco de Chile, virus para distraer y luego robo por 10 millones de dólares en la red SWIFT, 24 de mayo", 10 June 2018 [online] https://cesarfarro.medium.com/banco-de-chile-robo-por-m%C3%A1s-de-10-millones-de-d%C3%B3lares-el-24-de-mayo-4a3511afc956 [accessed in November 2020].
(12) FedEx, "Fedex afectado por el ataque del ransomware Petya", 17 July 2018 [online] https://www.clasesordenador.com/fedex-afectado-por-el-ataque-ransomware-petya/ [accessed in November 2020].
(13) Portal Puertario, "Operaciones de Cosco en América vuelven a la normalidad tras ciberataque", 30 July 2018 [online] https://portalportuario.cl/operaciones-de-cosco-en-america-vuelven-a-la-normalidad-tras-ciberataque/ [accessed in November 2020].
(14) Optical Networks, "Crónica del ciberataque a entidades bancarias peruanas", 24 August 2018 [online] https://www.optical.pe/blog/cronica-del-ciberataque-a-entidades-bancarias-peruanas/ [accessed in November 2020].
(15) S. Davidovsky, "Secuestro virtual y rescate en bitcoins: la historia detrás del ciberataque a una cooperativa en Esquel", La Nación, 4 February 2019 [online] https://www.lanacion.com.ar/tecnologia/secuestro-virtual-rescate-bitcoins-historia-detras-del-nid2216640/ [accessed in November 2020].
(16, 17, 18 y 19) Bienvenidos a Portal Tecnológico, "Chile: ciberataque a Minagri y virus informático en sistemas de ultramar", 2 July 2019 [online] https://diemmatotal.over-blog.com/2019/07/chile-ciberataque-a-minagri-y-virus-informatico-en-sistemas-de-ultramar.html [accessed in November 2020].
(20) R. Riquelme, "El rescate por el hackeo a Pemex es el segundo mayor por ransomware", El Economista, 15 November 2019 [online] https://www.eleconomista.com.mx/empresas/El-rescate-por-el-hackeo-a-Pemex-es-el-segundo-mayor-por-ransomware-20191115-0035.html [accessed in November 2020].
(21) Istoé dinheiro, "Cosan: interrupção em sistemas operacionais ocorreu devido a ataque de hackers", 16 March 2020 [online] https://www.istoedinheiro.com.br/cosan-interrupcao-em-sistemas-operacionais-ocorreu-devido-a-ataque-de-hackers/ [accessed in November 2020].
(22) Centro Criptológico Nacional (CCN), *Informe anual 2019: hacktivismo y ciberyidhadismo* (CNN-CERT IA-04/20), 2020 [online] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4714-ccn-cert-ia-04-20-informe-anual-2019-hactivismo-y-ciberyihadismo-1/file.html [accessed in November 2020].
(23) Revista Marítima, "Sospecha de ciberataque contra MSC", 13 April 2020 [online] http://rm-forwarding.com/2020/04/13/sospecha-de-ciberataque-contra-msc/ [accessed in November 2020].
(24) Bnamericas, "Cyberattacks on oil & gas firms, utilities on the rise", 9 October 2020 [online] https://www.bnamericas.com/en/news/cyber-attacks-on-oil--gas-firms-utilities-on-the-rise [accessed in November 2020].
(25) Minuto da Segurança, "Ransomware Maze anuncia invasão nas redes da CPFL e outras empresas", 30 June 2020 [online] https://minutodaseguranca.blog.br/ransomware-maze-anuncia-invasao-nas-redes-da-cpfl-e-outras-empresas/ [accessed in November 2020].
(26) ABC, "Garmin admite un ciberataque por 'ransomware' que dejó inactivos a sus usuarios durante cinco días", 30 July 2020 [online] https://www.abc.es/tecnologia/redes/abci-garmin-admite-ciberataque-ransomware-dejo-inactivos-usuarios-durante-cinco-dias-202007280938_noticia.html [accessed in November 2020].
(27) R. Gómez Torres, "Banco en México sufre otro ataque ransomware, pero niega filtración de datos", Criptonoticias, 17 August 2020 [online] https://www.criptonoticias.com/seguridad-bitcoin/banco-mexico-sufre-ataque-ransomware-niega-filtracion-datos/ [accessed in November 2020].
(28) Mundo Marítimo, "CMA CGM sospecha brecha de datos como consecuencia de ataque cibernético", 1 October 2020 [online] https://www.mundomaritimo.cl/noticias/cma-cgm-sospecha-brecha-de-datos-como-consecuencia-de-ataque-cibernetico [accessed in November 2020].
(29) MasContainer, "CMA CGM vuelve a la normalidad tras dos semanas desde ciberataque", 12 October 2020 [online] https://www.mascontainer.com/cma-cgm-vuelve-a-la-normalidad-tras-dos-semanas-desde-ciberataque/ [accessed in November 2020].
(30) S. Fontes, "Braskem é alvo de hackers e declara força maior", Valor investe, 8 August 2020 [online] https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2020/10/08/braskem-e-alvo-de-hackers-e-declara-forca-maior.ghtml [accessed in November 2020].

In terms of the countries affected by the events identified, Brazil and Chile top the list, followed in descending order by Argentina, Mexico, Peru, Panama, Uruguay, Colombia, Ecuador and the Dominican Republic.

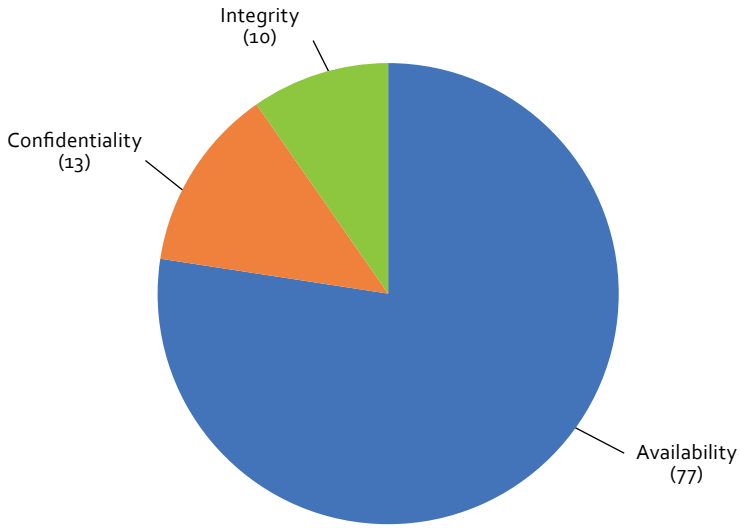
Figure 3
Countries affected, by number of incidents



Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey.

In most cases, the incidents recorded affected the cybersecurity pillar that has the greatest impact on logistics: availability. In 77.4% of cases, the organizations targeted by the attacks experienced technological disruptions that impacted on their processes. The average time during which these organizations had to do without the compromised systems was seven days. Confidentiality was the second most affected pillar, representing 12.9% of cases, while the integrity of information was compromised in 9.7% of cases (figure 4).

Figure 4
Impact on organizations
(Percentages)



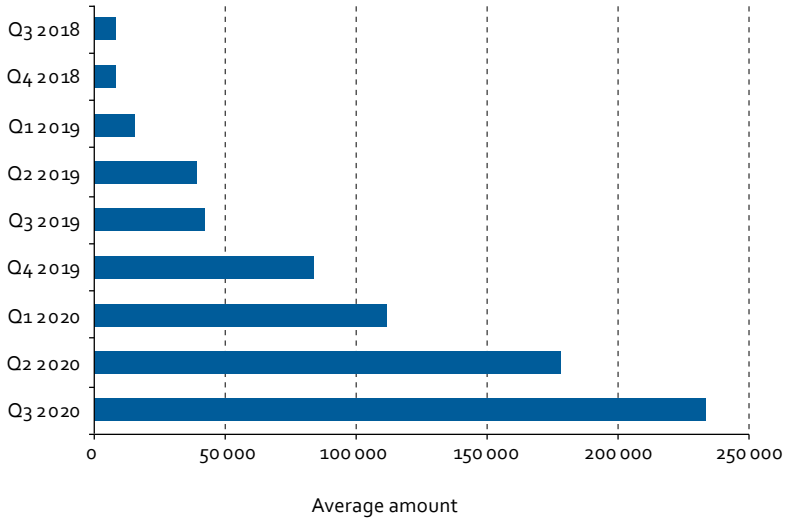
Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey.

This distribution, which is based on the main impact of the incidents occurring in the last five years, changed in 2020 with the emergence of combined ransomware attacks, in which data are exfiltrated by the attacker before being encrypted, thus compromising the confidentiality of the information captured and the availability of the systems encrypted during the attacks. In the future there will thus be a much higher risk of disclosure of the data of organizations that are attacked. In Latin American logistics, 50% of reported attacks involved ransomware, and the average ransom demand tripled in 2020, compared with 2019, with payment being demanded not only to restore operations but also to prevent public disclosure of the captured data (Sophos, 2020).

II. The evolution of ransomware

Maze ransomware, which began to circulate in late 2019, is the first type of malware to operate such that the organization behind it extorts money from its victims not only to restore operations to normal but also to stop it from disclosing the hijacked information.

Figure 5
Average ransom demands by quarter, third quarter 2018–third quarter 2020
(Dollars)



Source: Prepared by the author, on the basis of Coveware, "Q2 ransom payment amounts decline as ransomware becomes a national security priority", 23 July 2021 [online] https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority.

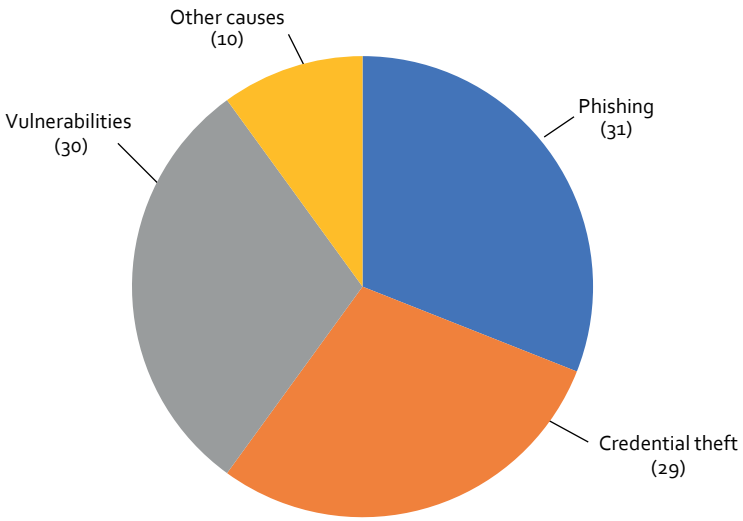
DopplePaymer, Sodinokibi, Netwalker, Conti and Egregor followed. As ransomware has evolved, the speed with which it spreads and the amounts of ransom demanded have increased. As an example

of the acceleration in the speed of ransomware spread, Maze succeeded in getting 50 victims to pay the ransom over six months of attacks, while its most recent successor, Egregor, which took Cencosud hostage in November 2020, achieved the same goal in only three weeks. Ransom demands have risen rapidly as cyberattackers have discovered that they are more successful in getting victims to pay by threatening to disclose highly valuable private information, especially in cases where the hijacked data are covered under personal data protection laws. Moreover, they have discovered that the techniques and tactics used to breach a small or medium-sized organization do not differ significantly from those required to breach larger companies that can potentially yield significantly higher payouts. As the effectiveness of ransomware collection has increased, average ransom demands have also risen, tripling from the fourth quarter of 2019 to the third quarter of 2020 (Coveware, 2020).

III. Analysis of the causes of incidents

Analysis of the root cause of cybersecurity incidents reveals that the top three attack vectors are phishing, accounting for 31% of cases, vulnerability scanning and exploitation, accounting for 30%, and theft of login credentials, accounting for 29% (Symantec, 2019). In other words, 60% of incidents are linked to weaknesses in people's savviness in using technology, be it failing to recognize a deceptive email or using weak passwords or the same passwords on multiple sites.

Figure 6
Causes of incidents
(Percentages)

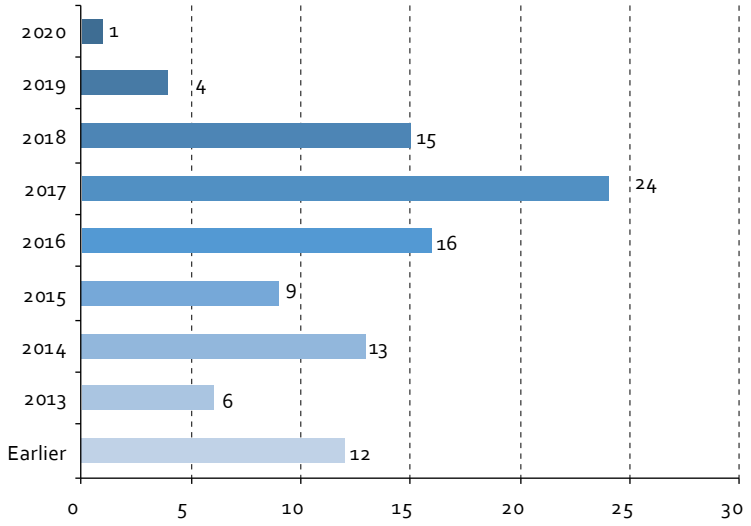


Source: Prepared by the author, on the basis of data from Symantec, *ISTR – Internet Security Threat Report*, vol. 24, February 2019 [online] https://docs.broadcom.com/doc/istr-24-2019-en.

When the cause is credential theft, the means of gaining access to the organization is generally through the native protocol that operating systems use to allow remote work. In the case of Microsoft, this protocol is the Remote Desktop Protocol (RDP), and although it has been used for the operational advantages that it offers, some organizations made greater use of RDP to enable their personnel to work during the lockdown periods that occurred during the pandemic.

Analysis of the vulnerabilities exploited as attack vectors in the first half of 2020 found that only 5% were vulnerabilities discovered in 2019 and 2020 and only 15% had been discovered in 2018. This means that 80% of the vulnerabilities exploited had been publicly known for at least two years and updates were available to fix them (Check Point Research, 2020). These figures highlight the difficulties that organizations have in keeping their computers' operating systems updated to patch known vulnerabilities, giving attackers more time to develop exploit kits and lengthening the lifespan of those kits.

Figure 7
Age of exploited vulnerabilities
(Percentages)



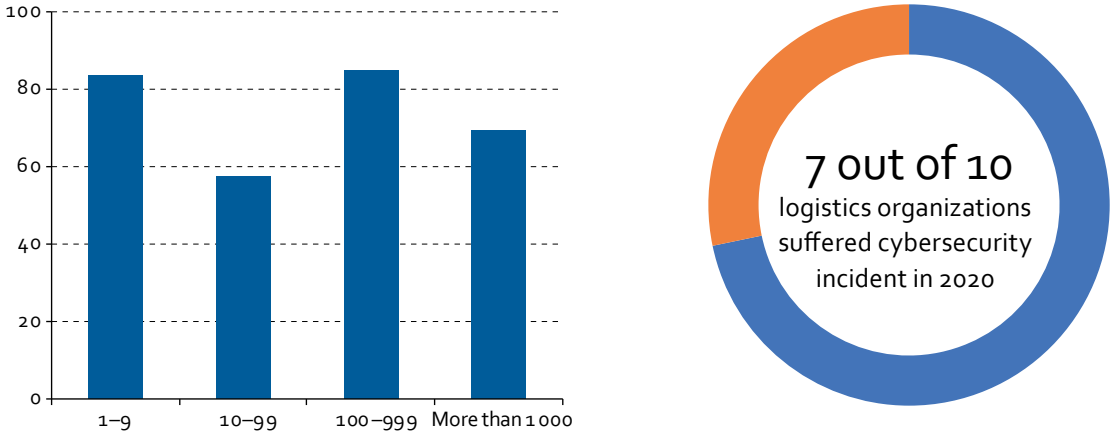
Source: Check Point Research, "Cyber attack trends: 2020 mid-year report", 22 July 2020 [online] https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/.

IV. The situation in logistics organizations

While cybersecurity levels have improved in recent years in the Latin American region, most countries are in the initial stage as measured by the Cybersecurity Capacity Maturity Model for Nations (CMM), developed by Oxford University (IDB/OAS, 2020). In this context, and in light of the scarcity of public reports or disclosures that would help logistics-related organizations to improve their individual maturity level and thus help raise the collective level, a survey was conducted among public and private organizations in this field. The main findings are described below.

Of the organizations surveyed, 72% reported at least one cybersecurity incident in the last 12 months. There is a tendency in Latin America and the Caribbean to believe that incidents increase as the size of the organization increases, but several global and regional studies have found this not to be true, and this finding was confirmed by the data from the survey, which did not show any tendency for attacks to be dependent on the size of the organization.

Figure 8
Incidents by organization size
(Percentages)

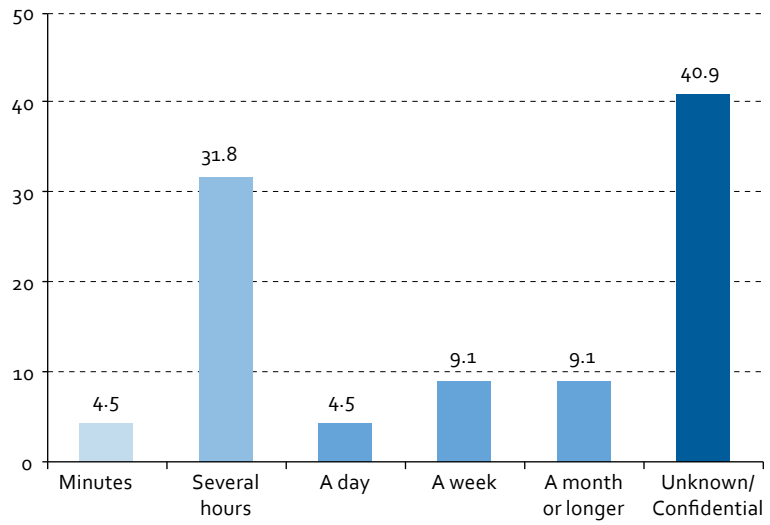


Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey.

It is striking that only 50% of organizations are concerned about incidents that may occur within the next 12 months, regardless of the size of the organization or whether they have experienced cybersecurity incidents in the recent past. This trend is a reflection of the CMM maturity level in the region and the need to share real-time data across regional public institutions. In many organizations, when a breach occurs and their staff consult with colleagues, they do not find answers that enable them to share experiences so as to address the problem in an evolutionary regional manner; rather, they find that they are able to rely only on the individual preparedness of the organization and its members. As a result, incidents can be dealt with solely on the basis of the procedure in place pre-crisis and the level of resilience that each organization has developed with regard to what needs to be done. Moreover, the current level of maturity means that smaller economies may suffer relatively greater consequences than those that have better self-defence mechanisms.

Of the organizations surveyed that had suffered a security incident in the last 12 months, 40.9% **could not specify how long it took them to normalize the situation after the incident**. Only 4.5% were able to resolve the incident within minutes, while for 54.5% it took from a few hours to more than a month to resume normal operations.

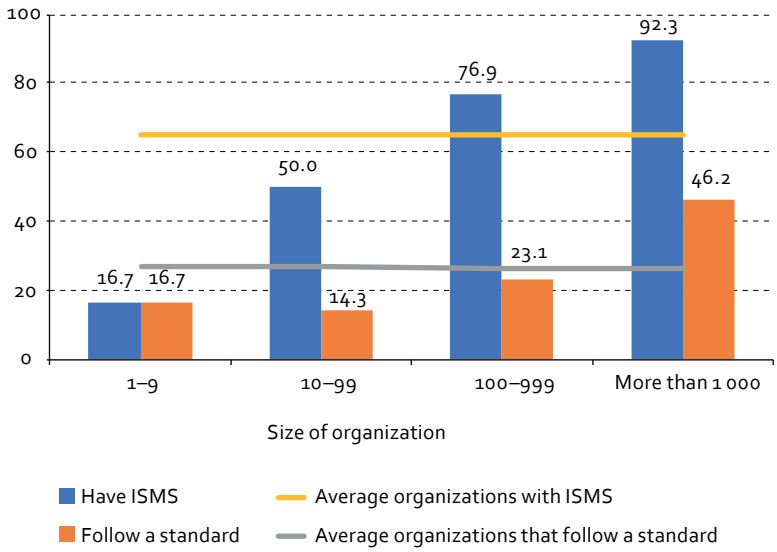
Figure 9
Incident recovery time
(Percentages)



Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey.

When asked about the extent to which security is formalized, 65.2% of the organizations indicated that they currently have a policy that is part of a cybersecurity management plan on which they rely to a moderate to high degree. However, only 26.1% base their rules and procedures on a standard as a guideline, with ISO/IEC 27001 being the guideline of choice in most cases.

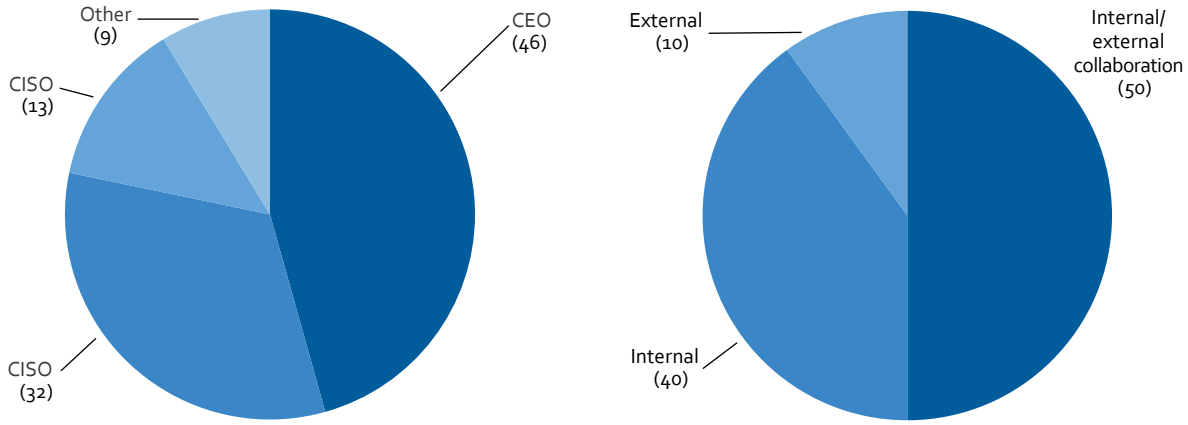
Figure 10
Formalization of cybersecurity management
(Percentages)



Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey.

With regard to organizational structure for security, 15.2% of logistics and related organizations in Latin America and the Caribbean have an independent structure to address cybersecurity needs, with security being managed by the chief executive officer (CEO) in 45.7% of the organizations and by the chief information officer (CIO) in 32.6% of cases. In 50% of cases, to deal with cybersecurity management and operational tasks, these officials have set up work teams with collaboration between their own staff and external organizations. In 40% of the organizations surveyed, security tasks are carried out by internal staff, while in 10% they are delegated entirely to third-party companies.

Figure 11
Organizational structure for security management
(Percentages)

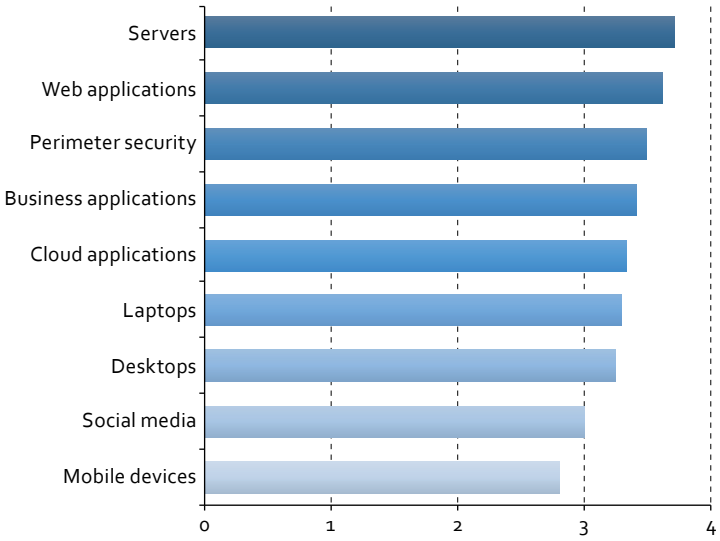


Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey.

V. A technical overview of the current situation

In terms of confidence in the security measures currently in place for various technologies, the ones that generate the highest level of confidence are those where the technical management of the information systems area has the greatest impact and where, historically, controls and measures have been implemented to reduce risk. This is the case for proprietary servers, web applications and logical perimeter security. Less trusted are technologies where end-users have the greatest influence, such as personal computers, use of social media and mobile phones.

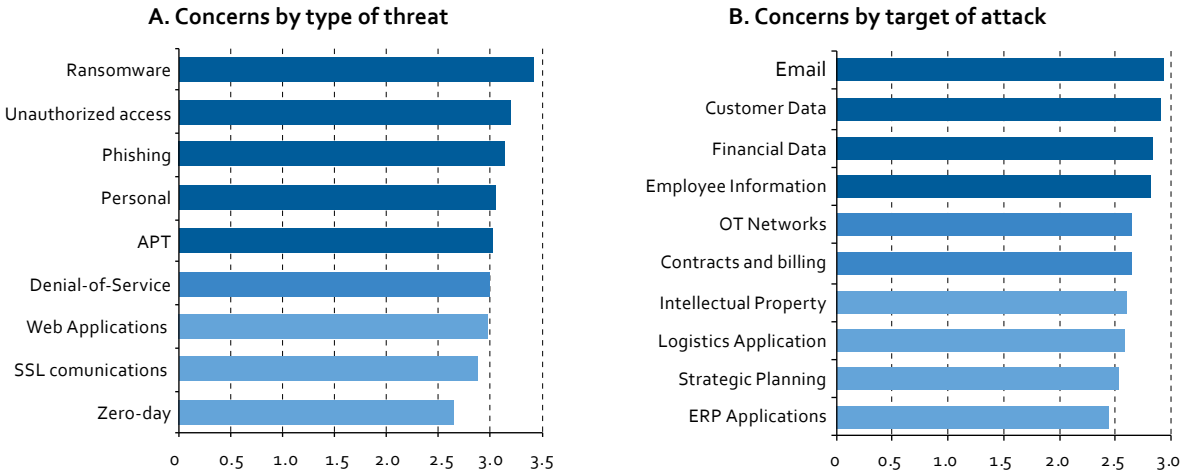
Figure 12
Level of confidence in cybersecurity controls implemented



Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey.

Analysis of existing concerns about the types of attacks and the assets to be protected showed that they are consistent with the events that have occurred to date. The threats of most concern are ransomware and unauthorized access through password theft (phishing).

Figure 13
Concerns by type of threat and target of attack
(Scale 1 to 5, with being the greatest concern)



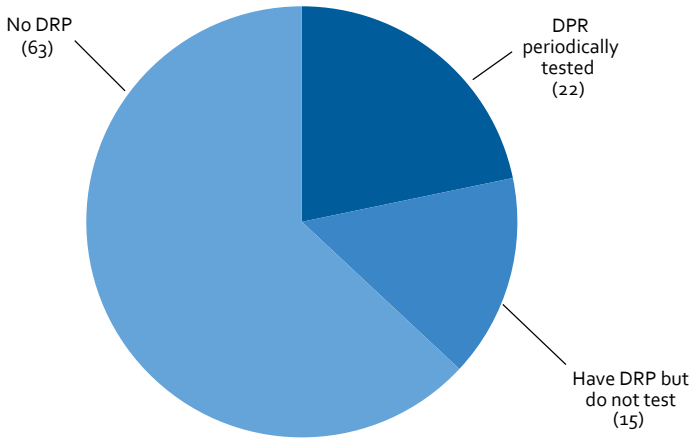
Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey.

With regard to protection of assets, the greatest concerns are email information and third-party data in the possession of the organizations surveyed.

VI. Cyberresilience practices

The concept of cyberimmunity is explored in *FAL Bulletin* No. 382 of ECLAC, entitled "Cybersecurity in the time of COVID-19 and the transition to cyberimmunity" (Díaz, 2020), where it is explained that in an environment in which the level of risk can never be reduced to zero, it is mathematically only a question of time before an attack occurs, a situation that motivates work teams to have documentation and to take services offline. When asked in the survey about this practice, only 37% of organizations reported having a disaster recovery plan (DRP) and only 22% indicated that they conduct periodic tests to enable them to deal more effectively with a real-life crisis situation.

Figure 14
Organizations with a DRP
(Percentages)



Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey.

In regions where organizations are in advanced stages of the CMM and risks are assessed more assertively, the purchase of insurance policies to cover potential cyberattack damages is growing steadily at a rate of 25% a year, with the number of claims rising from 200 in 2017 to 800 in 2019 (Allianz, 2021). The amount of coverage is related to each organization's level of dependence on technology for its core business processes, the degree to which its secondary processes may be affected and the impact that third parties, such as other organizations or individuals, may suffer.

The growth of market for insurance stems from the increase in demand for cybercrime policies and the consequent supply that has emerged to meet expectations. This results in a "feedback" phenomenon that increases trust among those at various stages in the logistics chain, not only because of the assistance that the policies provide in the event of an incident, which helps organizations to recover more quickly, but also because of the process itself that insurers require as a condition of coverage. It is worth noting that this process is the result of the needs of the actors in the logistics chain and the successful response of service providers, and it has therefore been adopted in a manner similar to compliance with a regulation or a de facto standard (Aspen, 2016).

VII. Cyberimmunity, a cybersecurity strategy for post-pandemic recovery

The data found in the research and the opinions collected from the organizations that participated in the ECLAC survey reveal results that point to the need for a cybersecurity plan or strategy to support the move towards logistics based on the new paradigms of Industry 4.0 and to facilitate the region's post-pandemic recovery of its operating capacity in a competitive manner. The organizations surveyed have indicated what they foresee for the next 12 months: an acceleration of the digitization of the economy, with an average growth of **34%** in disruptive technologies, as a result of which digital assets could be more exposed to attack, especially as the cybercrime industry is a lucrative growth area, the cost of which is expected to reach US$ 6 trillion in 2021 (Herjavec Group, 2020), in a global economy in recession.

The variables analysed suggest that plans would be much more effective if they, like information, stretched across borders. While some countries, such as Uruguay and Colombia, show indicators of an above-average level of maturity in cybersecurity as a result of local strategic plans (IDB/OAS, 2020), the nature of the technology involved requires regional collaborative action, not only in the legislative sphere, to facilitate international investigations that may be necessary following an incident, but also to promote cooperation on preventive actions that could be taken as a result of real-time analysis of cybercrime activity in the region. The accession of several countries to the Budapest Convention, which provides an international framework for cooperation in the fight against cybercrime, seems to offer an appropriate avenue for coordinating investigative and legal actions. The Dominican Republic was the first country in the region to sign the Convention, in 2013, and as a result of this strategic decision it has achieved a CMM maturity level of 4 in the legislative sphere.

In any case, it is important to analyse the experience accumulated by countries in Latin America and the Caribbean that have been in the vanguard in developing cybersecurity-related strategies and activities with a view to accelerating the adoption of measures by those that do not yet have such tools.

While actions in the public sphere tend to be more effective in the long term, organizations that are part of the logistics chain and those that are part of the critical infrastructure of nations should have an information security management system (ISMS) and implement practical actions based on international standards to increase their operational resilience.

As possible strategies for the evolution of cyberculture in the region, the following guidelines are proposed:

- States that do not yet have a national cybersecurity strategy should start by developing one in order to assign priorities and allocate resources so that subsequent efforts are aligned with this strategy.

  Human capital should be the fundamental factor for the cultural transformation required to ensure the transition to cyberimmunity. Accordingly, **the inclusion of appropriate cognitive content in educational settings at all levels** may be a first step that nations should consider.

  For example, the incorporation of content relating to personal data protection into educational curriculums would help to improve current levels of maturity in the protection of citizens' rights and provide a basis for enhancing individual understanding of the current value of data as representative not only of objects in the physical world but also, and above all, human of beings. Promoting the provision of specialized education at the tertiary or undergraduate level in cyberdefence and reviewing current curriculum content relating to information and communications technologies could be a good strategy from a national public administration standpoint, contributing to regional synergy.

- Strengthening the cyberdefence agenda of regional institutions could be a good strategy for fostering collaboration among all nations and for advancing collectively and individually in CMM maturity. Considering that continuous monitoring of cyberactivity in the region can generate early warnings to prevent cyberattacks, a regional collaboration network could be set up in this area to increase the capacity to correlate events, thus increasing early detection in order to enable organizations to take defensive action earlier and on a larger scale.

- The creation of a regulatory framework or strengthening of the framework in countries that already have one, would serve to raise the level of confidence in cybersecurity among stakeholders in the supply chain. An example of a valuable action that would increase the level of trust between stakeholders all along the logistics chain is to help organizations to put in place risk mitigation measures commensurate with their size and processes, based on ISO standard 27001, highlighting the need to have a formal DRP and to test it at least once a year and then to implement the improvements needed based on the test.[1]

- Steps should be taken to create national incident response offices or a government CSIRT, which already exist in many countries in the region, and improve the interaction between these hubs with both private and public organizations. This would help address cybersecurity events in a collaborative manner between the two spheres, similar to the service currently provided by institutions responsible for public security. To cite just one example, an organization is a victim of ransomware, the involvement of an entity trained in how to oversee recovery and deal with the ransom demand would be of great value in reducing downtime and, if necessary, in determining the course of action to take with regard to the ransom.

- Increasing public awareness of cybersecurity can help raise the overall level of immunity to cyberattacks. There is a low level of awareness of online threats in some Latin American countries. At the same time, some private organizations do not yet demonstrate a risk perception that is consistent with reality. The average percentage expressing concern about cybersecurity incidents in 2021 is 50%, which seems low, considering that 70% of organizations experienced incidents in 2020. Disclosure of incidents that have occurred

[1] In line with the recommendations made by the International Maritime Organization (IMO) in its circular MSC.1/Circ.1526 (IMO, 2016), it would be advisable to review the Ship and Port Facility Security (ISPS) Security Code in order to verify that it covers situations related to sabotage that might occur as a result of the use of current cyberattack techniques against critical infrastructure and that could have consequences with regional and international impact.

would improve the perception of risk, and organizations might therefore attach higher priority to their cyberattack prevention strategies.

- At the individual level, in addition to continuing with the traditional measures of technological perimeter protection, adequate data backups and protection and updating of end-user equipment, organizations should consider incorporating early incident detection through real-time monitoring of network data traffic and advanced tools for its analysis, ideally using artificial intelligence techniques, addressing events immediately through an incident response team or security operations centre (SOC). At the same time, the spread of possible incidents should be limited vertically through layered defence models and laterally through the use of microsegmentation of the data network.
- In technology transformation projects, cybersecurity implications should be considered from the initial stage of the project, with appropriate design, definition and implementation tasks distributed as appropriate to the technology project. Viewing cybersecurity as a separate discipline may lead to unexpected costs and risks and, as a result, delays in the implementation of such projects, with all the consequences that this may entail.

In general, continued work is needed to strengthen cybersecurity in logistics, both at the level of institutional and regulatory frameworks and from the standpoint of collective and individual awareness-raising, without losing focus on people, who continue to account for two thirds of cybersecurity incidents. At the same time, work is needed to create or strengthen the ISMS of organizations at the individual level, with a view to developing operational resilience to meet the technological challenges of Industry 4.0.

Bibliography

Allianz (2021), "Managing the impact of increasing interconnectivity: Trends in cyber risk", March [online] https://www.agcs.allianz.com/news-and-insights/reports/cyber-risk-trends-2020.html.

Aspen (2016), *Cyber Risk and the Evolution of Supply Chains*.

Barleta, E., G. Pérez and R. Sánchez (2019), "Industry 4.0 and the emergency of Logistics 4.0", *FAL Bulletin*, No. 375, Santiago, Economic Commission for Latin America and the Caribbean (ECLAC).

Check Point Research (2020), "Cyber attack trends: 2020 mid-year report", 22 July [online] https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/.

Cichonski, P. and others (2012), *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology (NIST).

Clement, J. (2021), "Year-on-year change in online traffic worldwide as of May 2021", 15 January [online] https://www.statista.com/statistics/1105495/coronavirus-traffic-impact/#statisticContainer.

Coveware (2020), "Ransomware demands continue to rise as data exfiltration becomes common, and maze subdues", 4 November [online] https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report.

Díaz, R. M. (2020), "Cybersecurity in the time of COVID-19 and the transition to cyberimmunity", *FAL Bulletin*, No. 382, Santiago, Economic Commission for Latin America and the Caribbean (ECLAC).

Herjavec Group (2020), "The 2020 Official Annual Cybercrime Report" [online] https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/.

IDB/OAS (Inter-American Development Bank/Organization of American States) (2020), *Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean*.

IDG Communications (2020), "CIO COVID-19 Impact Study", 30 April [online] https://www.idg.com/tools-for-marketers/cio-cv-19-impact-study/.

IMO (International Maritime Organization) (2016), *Interim Guidelines on Maritime Cyber Risk Management* (MSC.1/Circ.1526), London.

ITU (International Telecommunication Union) (2018), *Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity*.

Johnson, J. (2021), "Number of internet users worldwide from 2009 to 2020, by region", 27 January [online] https://www.statista.com/statistics/265147/number-of-worldwide-internet-users-by-region/.

SonicWall (2020), "Capture labs threat metrics", SonicWall Security Center [online] https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics.

Sophos (2020), *Sophos 2021 Threat Report*, November.

Symantec (2019), ISTR – *Internet Security Threat Report*, vol. 24, February [online] https://docs.broadcom.com/doc/istr-24-2019-en.

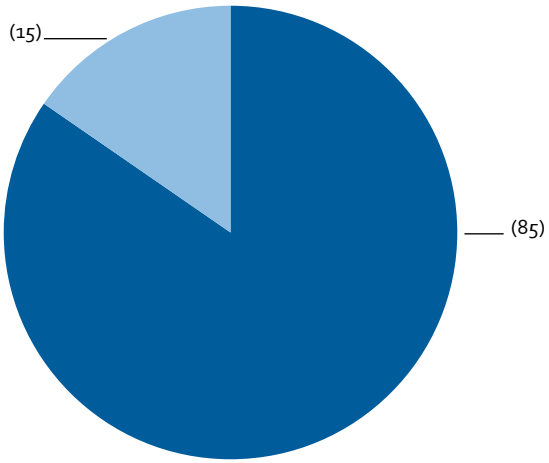
Annexes

Annex 1
Situation by country: Argentina

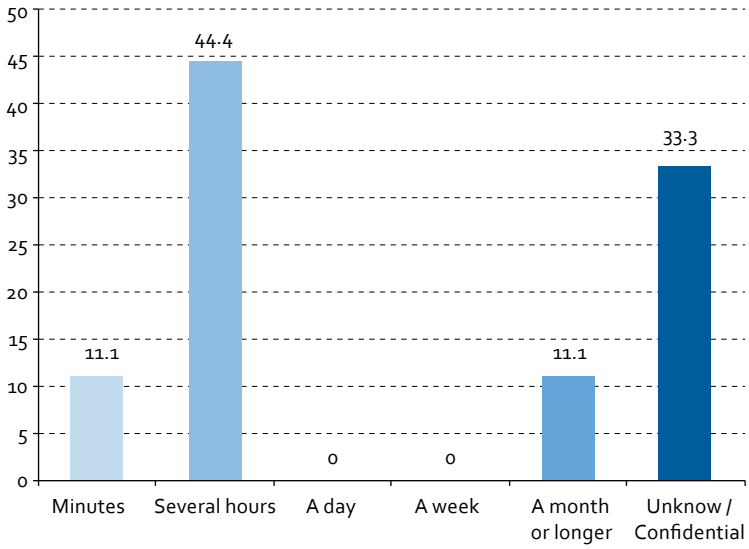
The general trend of Argentina's indicators, according to the Cybersecurity Report covering the period 2016–2020, has been positive, but it should be noted that the average indicators for 2020 are below the expected average (2.09). Argentina has made progress in creating an institutional superstructure, but it does not yet ensure the necessary level of effectiveness.

Figure A1
Situation in Argentina
(Percentages)

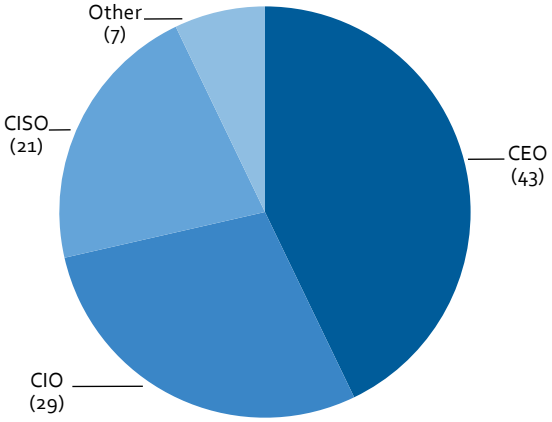
CMM maturity level: 2, formative
A. Percentage of organizations reporting incidents in 2020



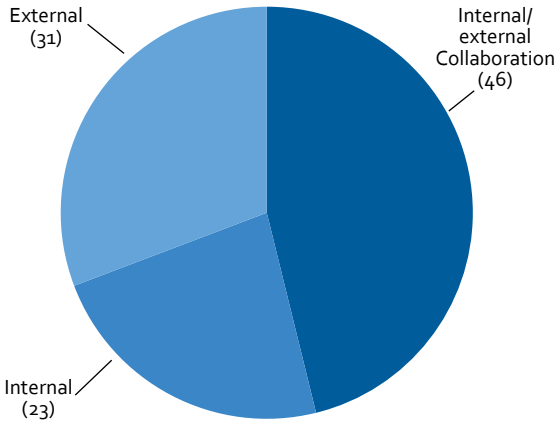
B. Incident recovery time



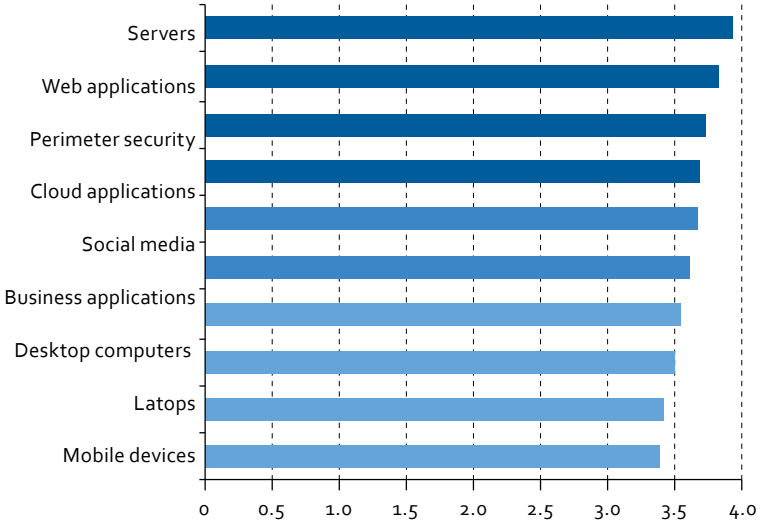
C. Security manager



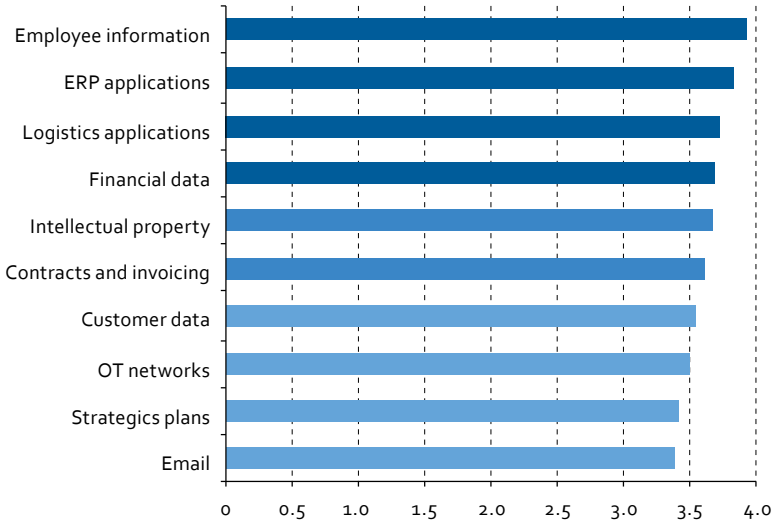
D. Work team



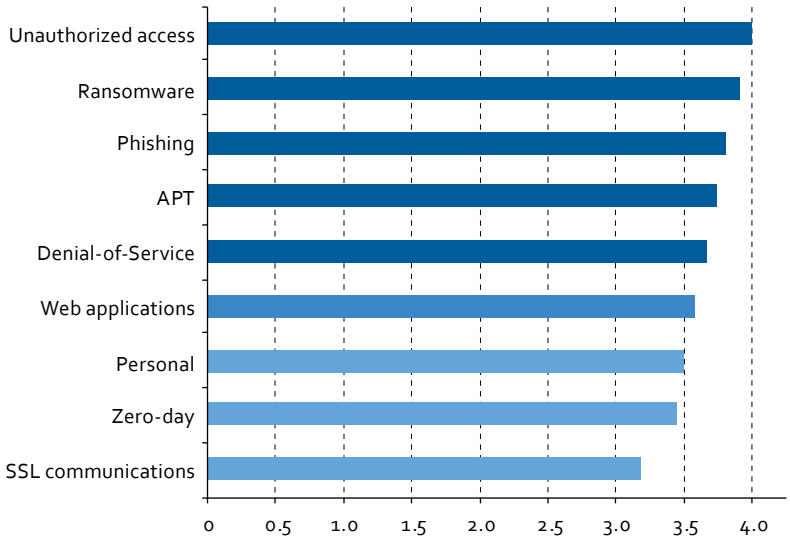
E. Level of confidence in cybersecurity controls implemented



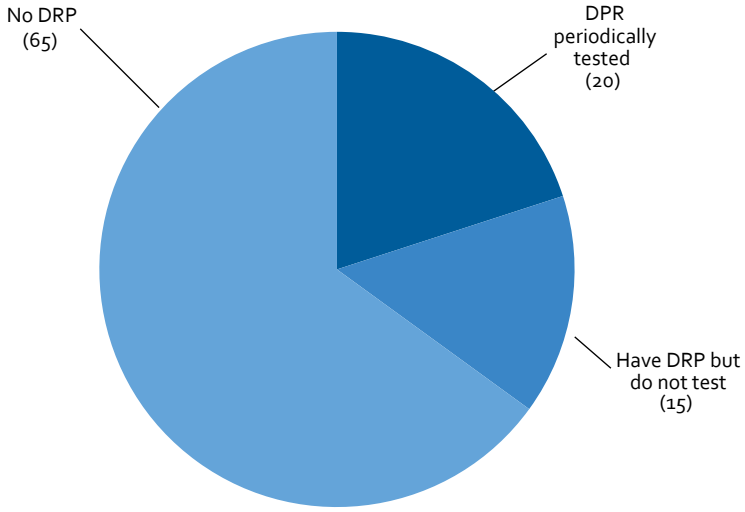
F. Concerns by target of attack



G. Concerns by type of threat



H. Organizations with a DRP



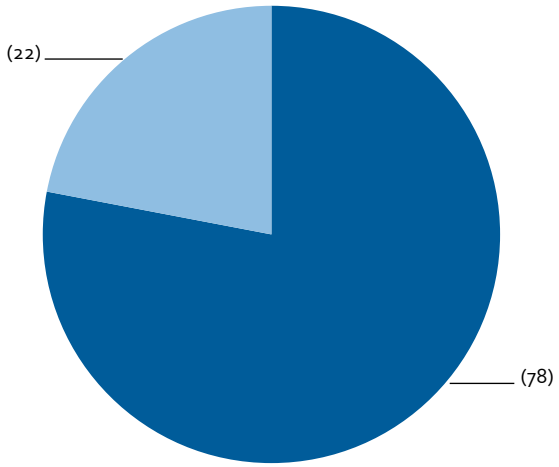
Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey and Inter-American Development Bank/Organization of American States (IDB/OAS), *Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean*, 2020.

Annex 2
Situation by country: Brazil

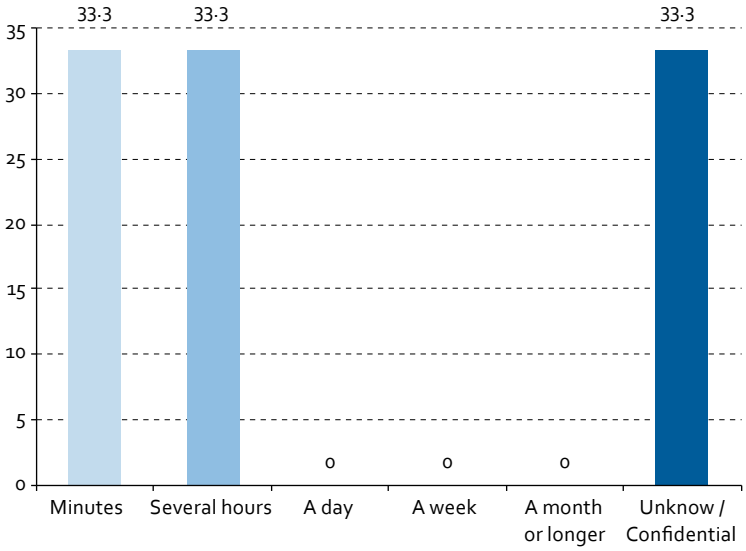
Brazil's greatest strength is its cybersecurity policy and strategy. It has also developed infrastructure to enhance its response capacity to address and resolve cyberincidents, coupled with a good level of maturity with regard to cybersecurity culture.

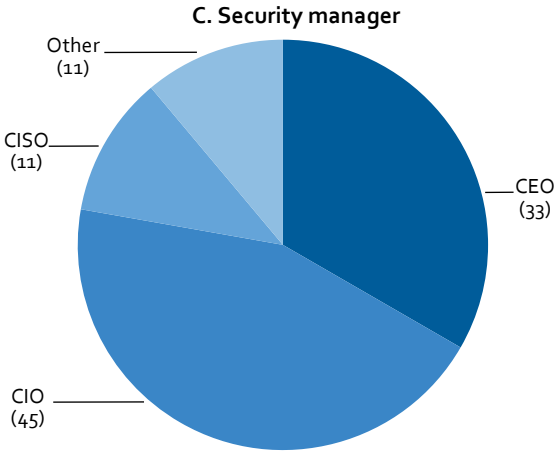
Figure A2
Situation in Brazil
(Percentages)

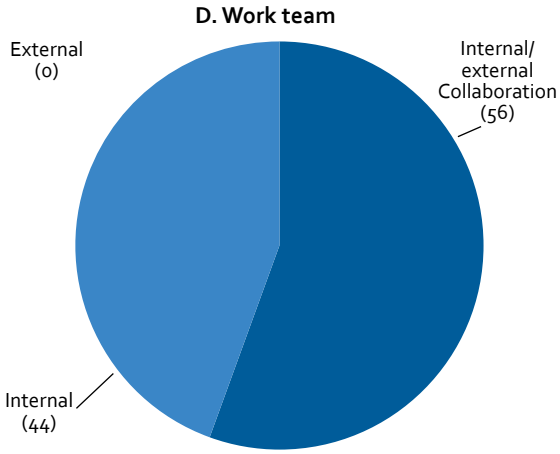
CMM maturity level: 2, formative
A. Percentage of organizations reporting incidents in 2020

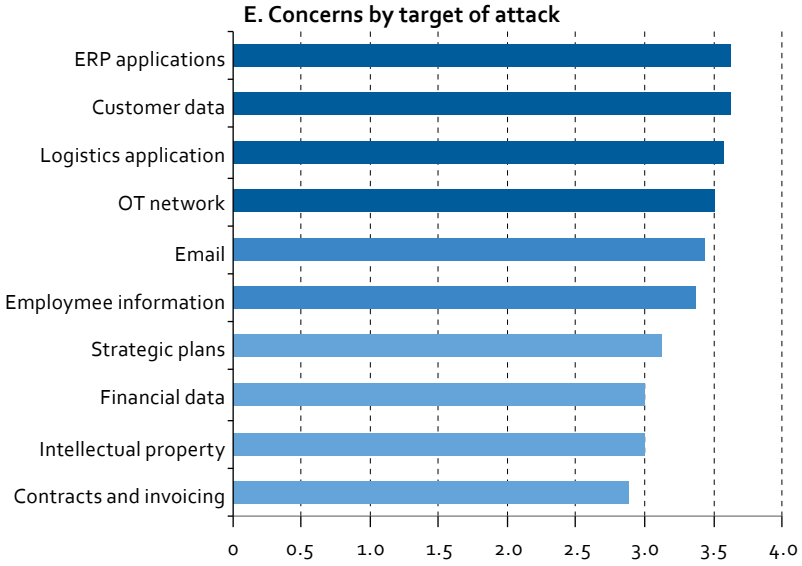


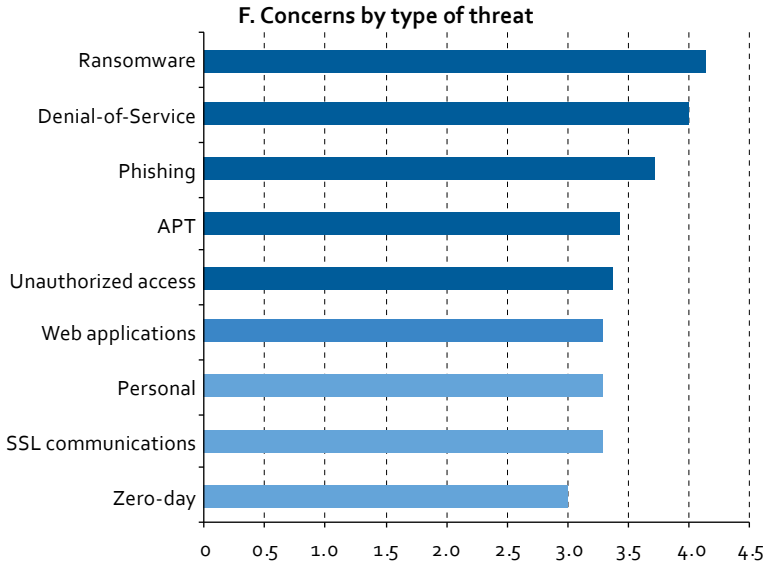
B. Incident recovery time



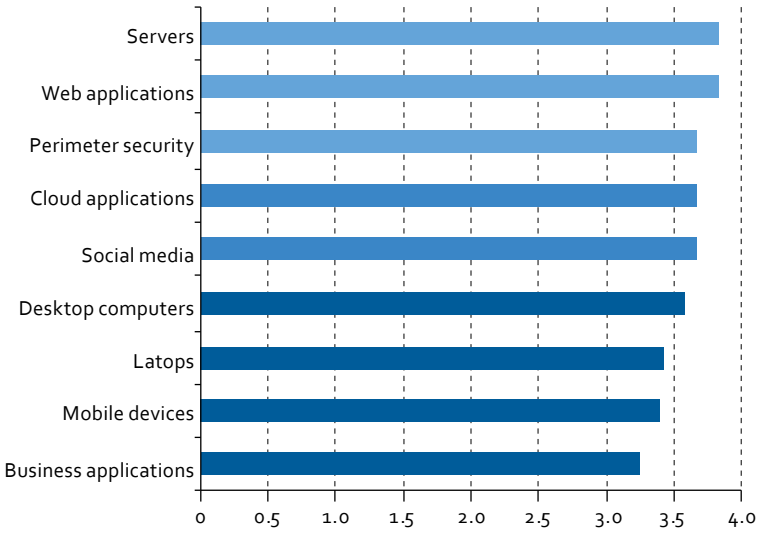

C. Security manager
Other (11)
CISO (11)
CEO (33)
CIO (45)


D. Work team
External (0)
Internal/ external Collaboration (56)
Internal (44)

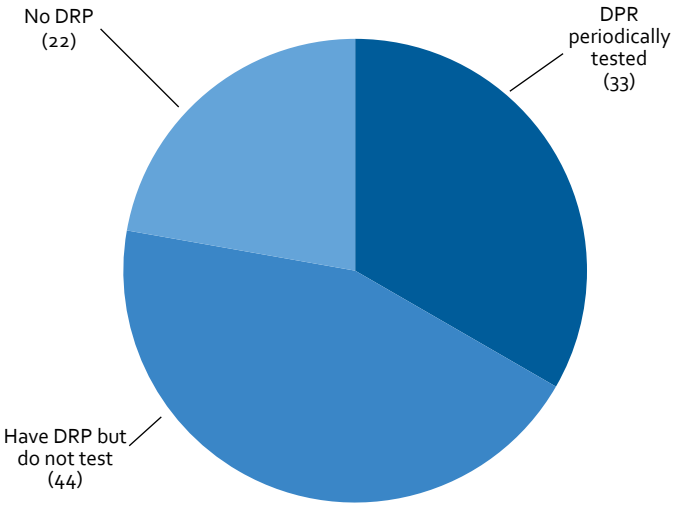

E. Concerns by target of attack
ERP applications
Customer data
Logistics application
OT network
Email
Employmee information
Strategic plans
Financial data
Intellectual property
Contracts and invoicing
0
0.5
1.0
1.5
2.0
2.5
3.0
3.5
4.0


F. Concerns by type of threat
Ransomware
Denial-of-Service
Phishing
APT
Unauthorized access
Web applications
Personal
SSL communications
Zero-day
0
0.5
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5

G. Level of confidence in cybersecurity controls implemented



H. Organizations with a DRP



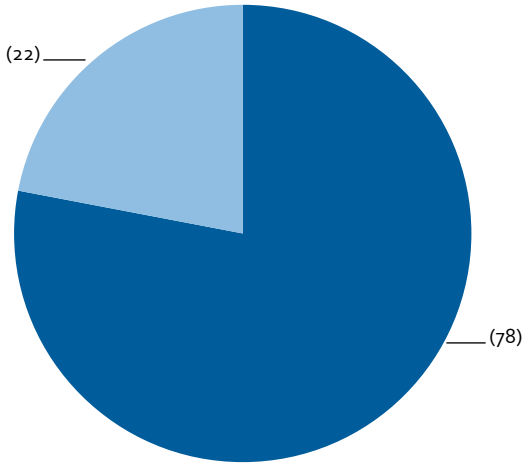
Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey and Inter-American Development Bank/Organization of American States (IDB/OAS), *Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean*, 2020.

Annex 3
Situation by country: Chile

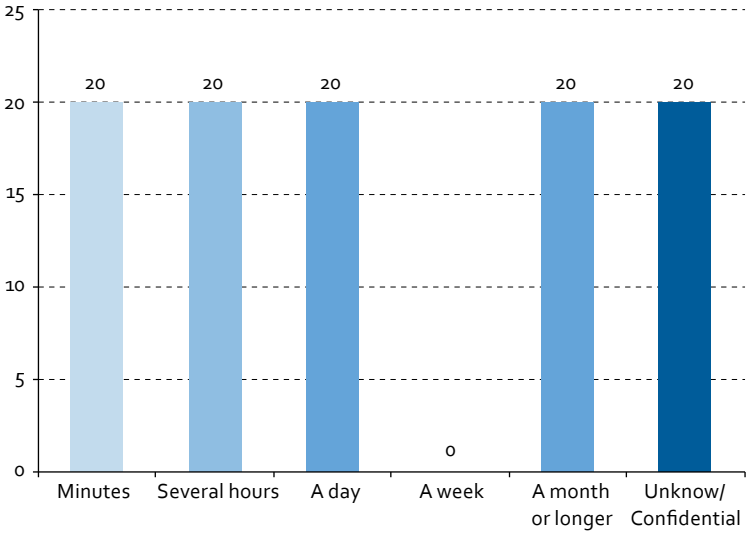
Chile has made substantial progress in all its indicators, notably with regard to strategy and incident response and also the development of cyberculture.

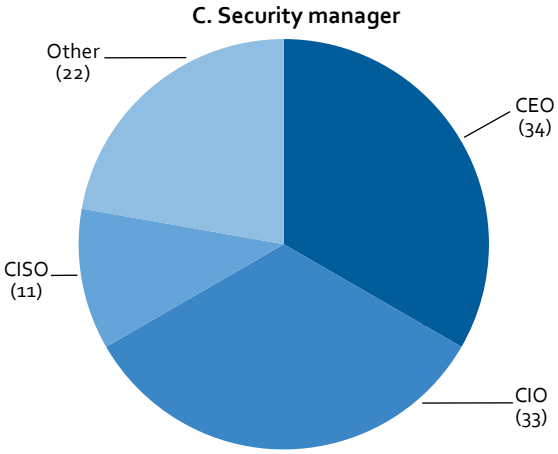
Figure A3
Situation in Chile
(Percentages)

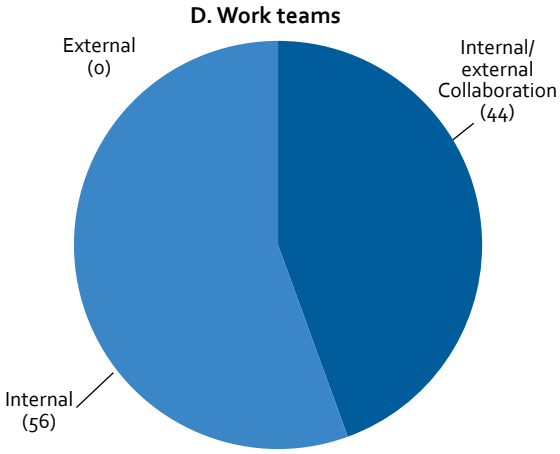
CMM maturity level: 2, formative
A. Percentage of organizations reporting incidents in 2020

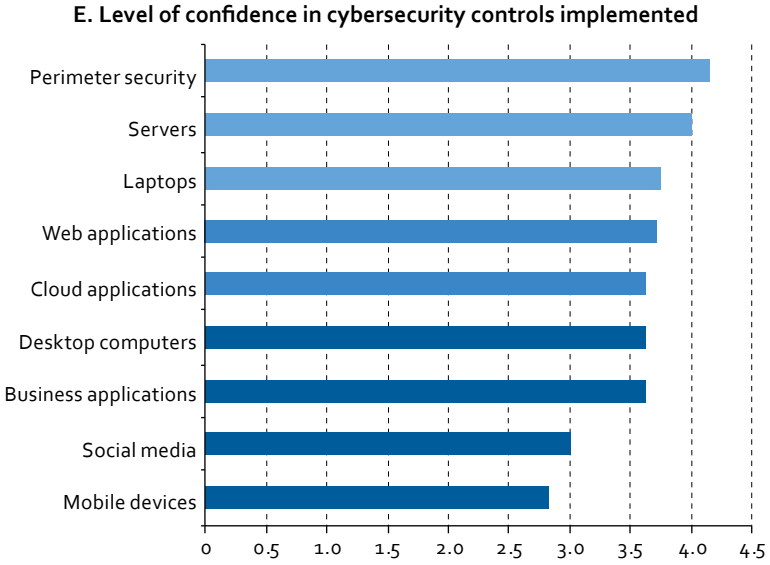


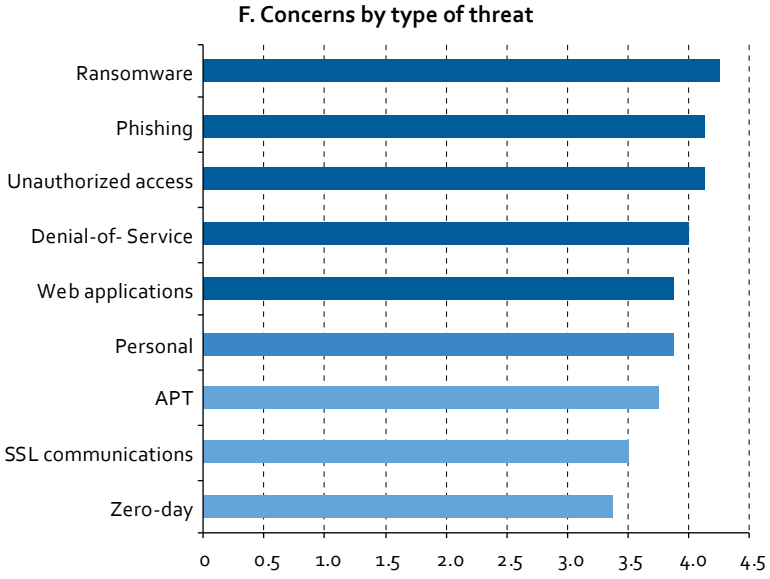
B. Incident recovery time

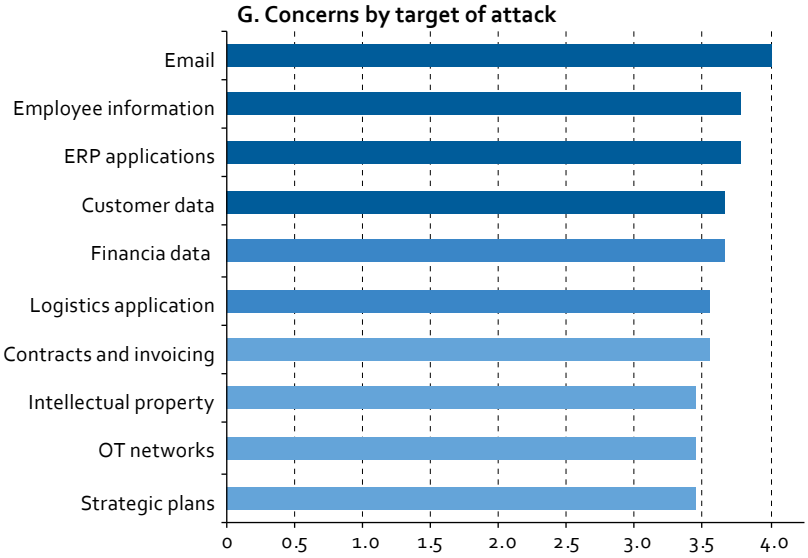


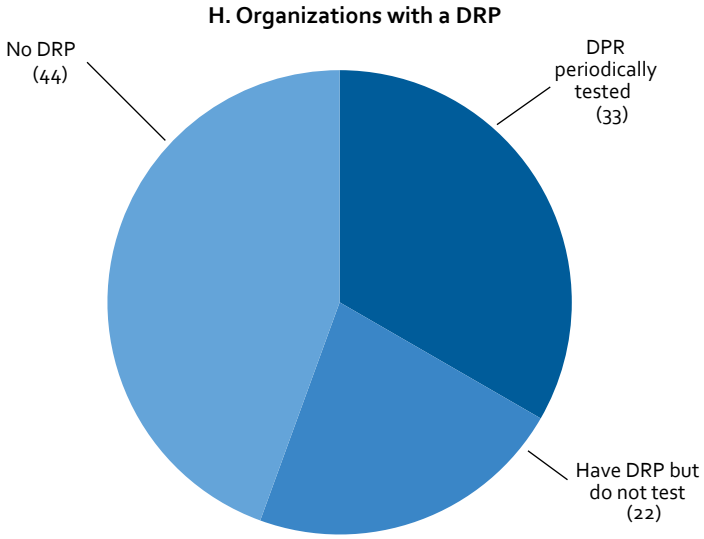

C. Security manager
Other (22)
CEO (34)
CISO (11)
CIO (33)


D. Work teams
External (0)
Internal/ external Collaboration (44)
Internal (56)


E. Level of confidence in cybersecurity controls implemented
Perimeter security
Servers
Laptops
Web applications
Cloud applications
Desktop computers
Business applications
Social media
Mobile devices
0
0.5
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5


F. Concerns by type of threat
Ransomware
Phishing
Unauthorized access
Denial-of- Service
Web applications
Personal
APT
SSL communications
Zero-day
0
0.5
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5





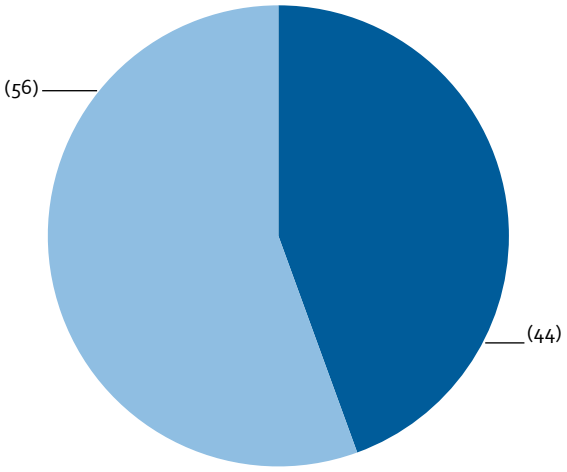
Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey and Inter-American Development Bank/Organization of American States (IDB/OAS), *Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean*, 2020.

Annex 4
Situation by country: Colombia

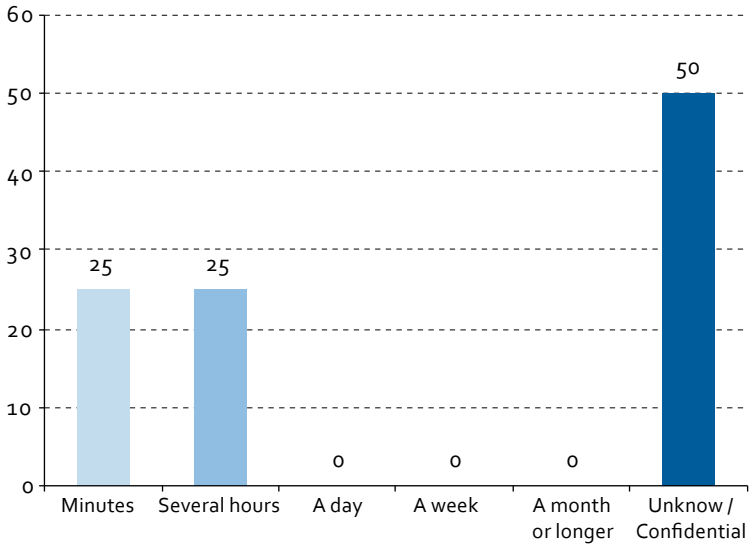
Colombia has seen much progress in its indicators in recent years, reaching a stage of maturity as a result of a strong national strategic policy, which has had a positive impact on organizations in the country. The challenge for Colombia is to continue efforts to raise individual awareness among the population outside the sphere of organizations.

Figure A4
Situation in Colombia
(Percentages)

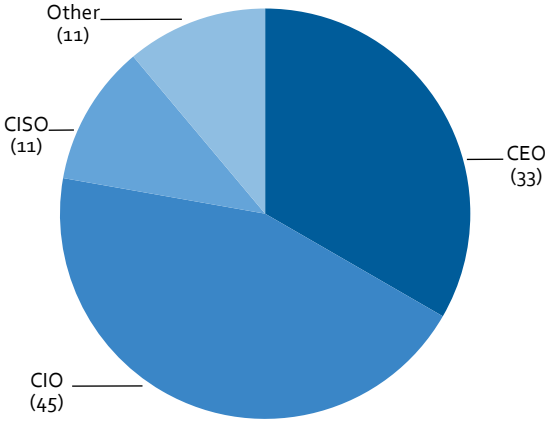
CMM maturity level: 3
A. Percentage of organizations reporting incidents in 2020



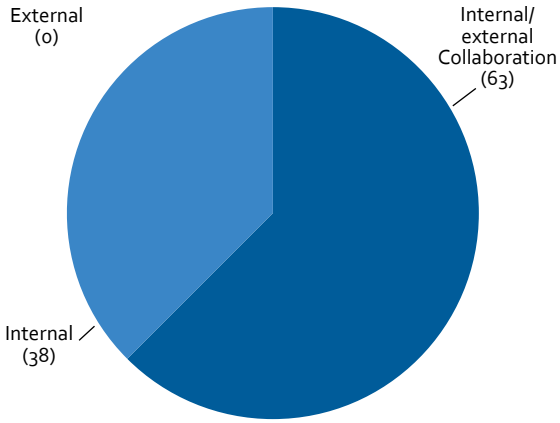
B. Incident recovery time



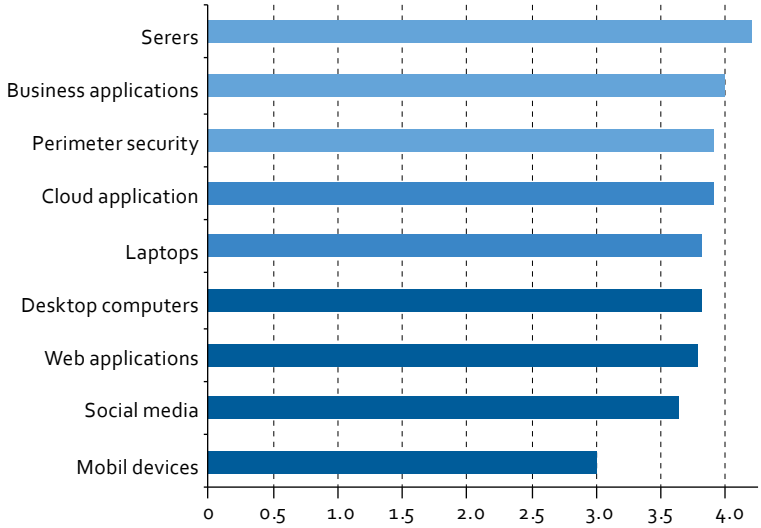
C. Security manager



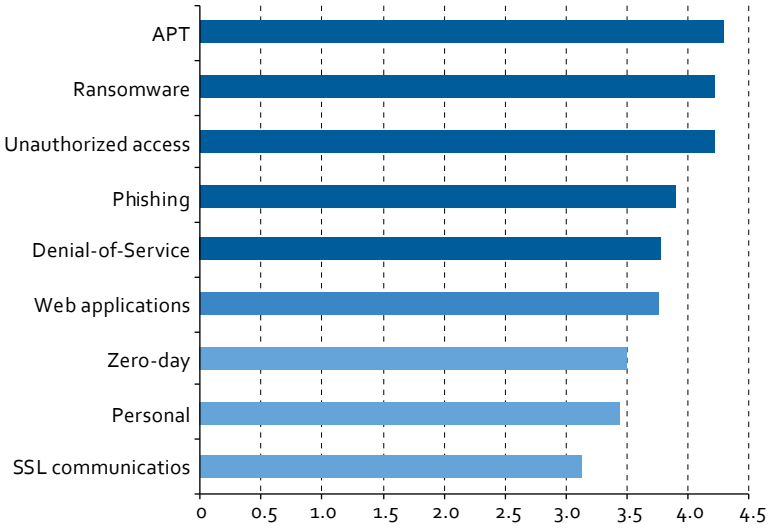
D. Work teams

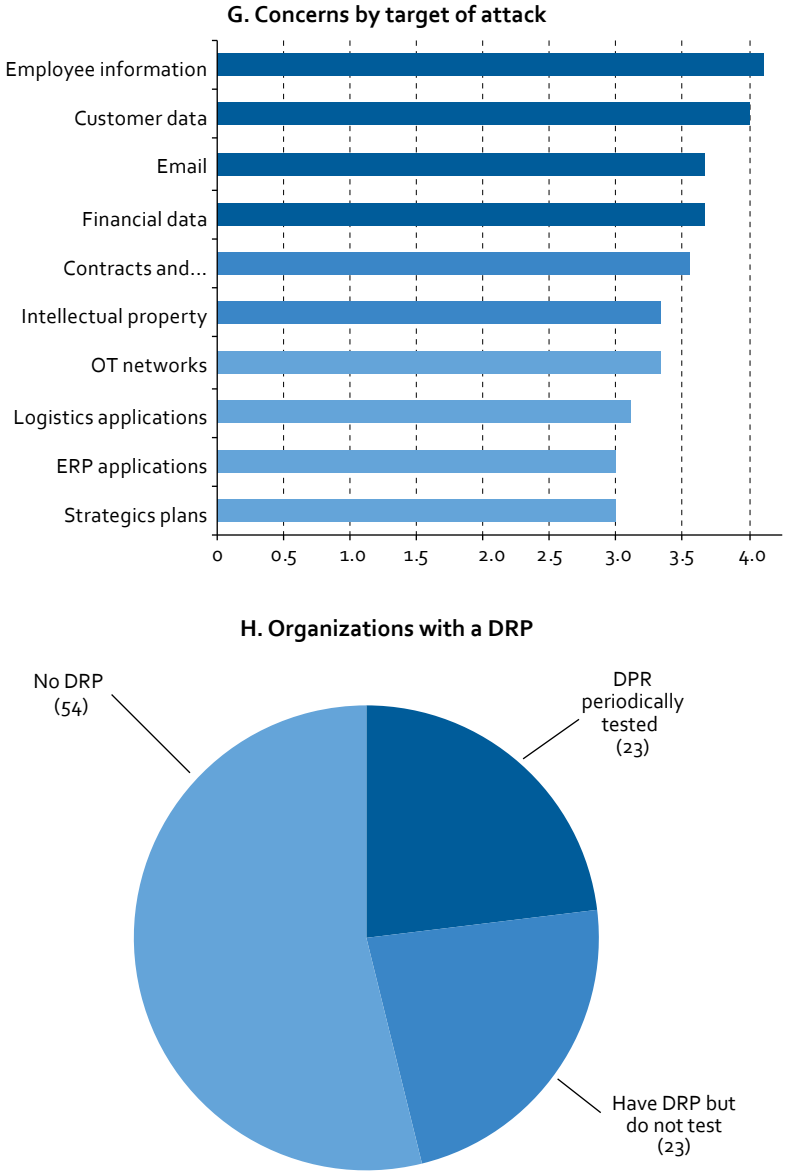


E. Level of confidence in cybersecurity controls implemented



F. Concerns by type of threat





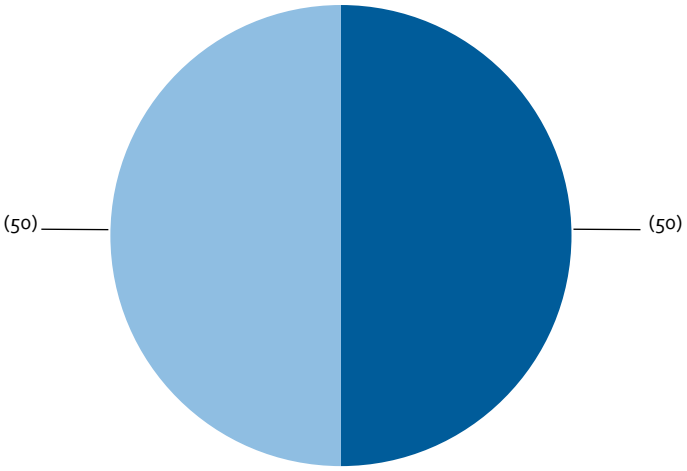
Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey and Inter-American Development Bank/Organization of American States (IDB/OAS), *Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean*, 2020.

Annex 5
Situation by country: Ecuador

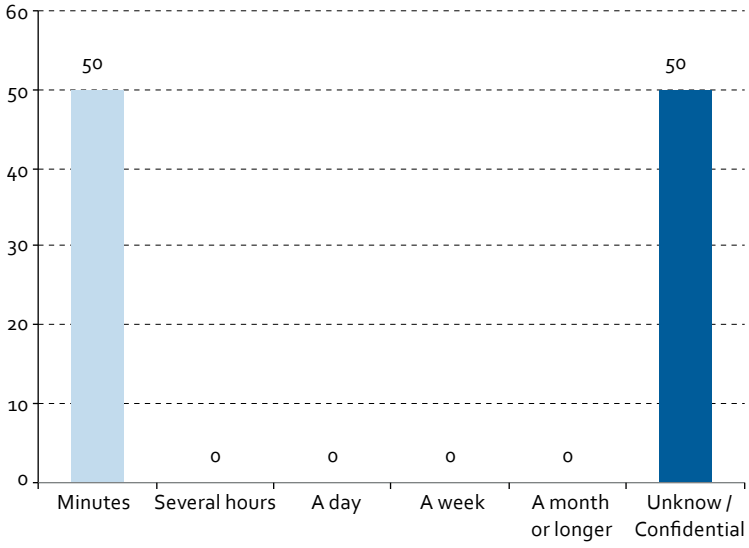
Although Ecuador's overall average places it in stage 2 (formative), as a result of the establishment of a legal framework and standards, mostly in the last four years, together with recent, incipient advances in cyberculture. However, it is still at the start-up stage with regard to operational aspects. Ecuador could find that the development of operational cybersecurity strategies at the national level will catalyse the efforts already made in relation to the legal framework and standards, which could help it to advance in the consolidation of these efforts.

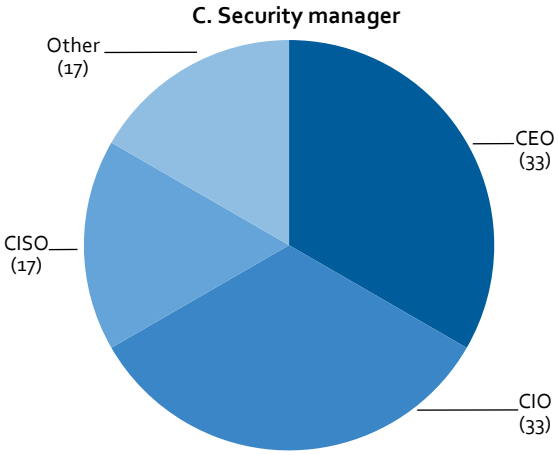
Figure A5
Situation in Ecuador
(Percentages)

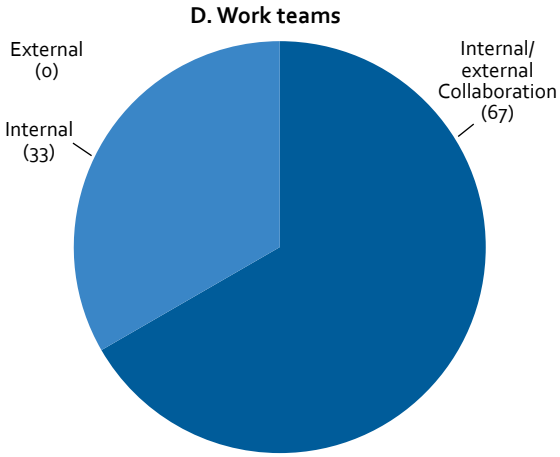
CMM maturity level: 2
A. Precentage of organizations reporting incidents in 2020

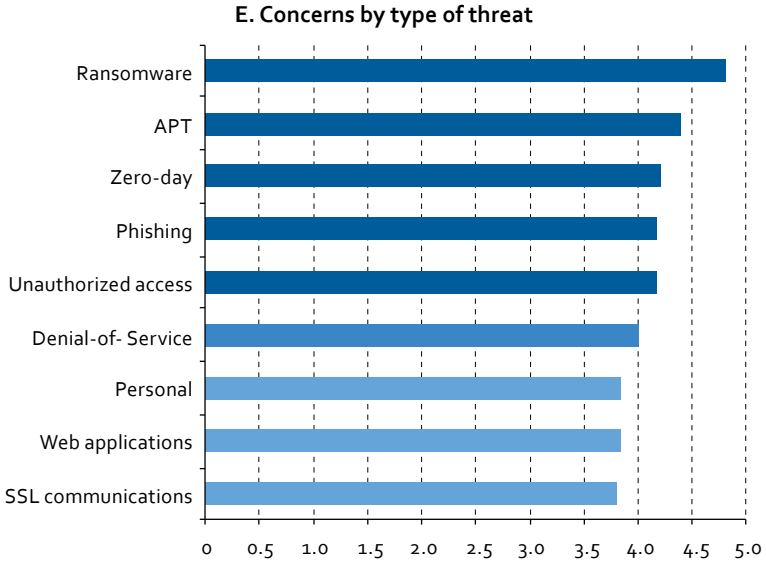


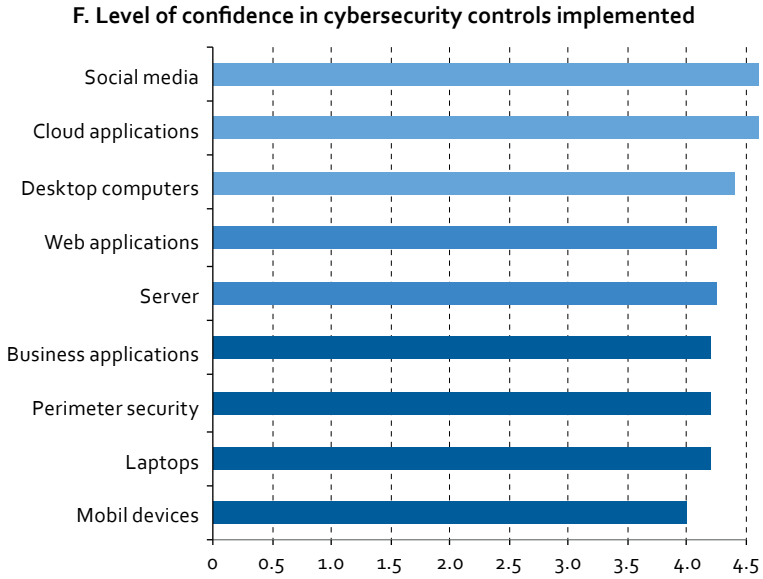
B. Incident recovery time



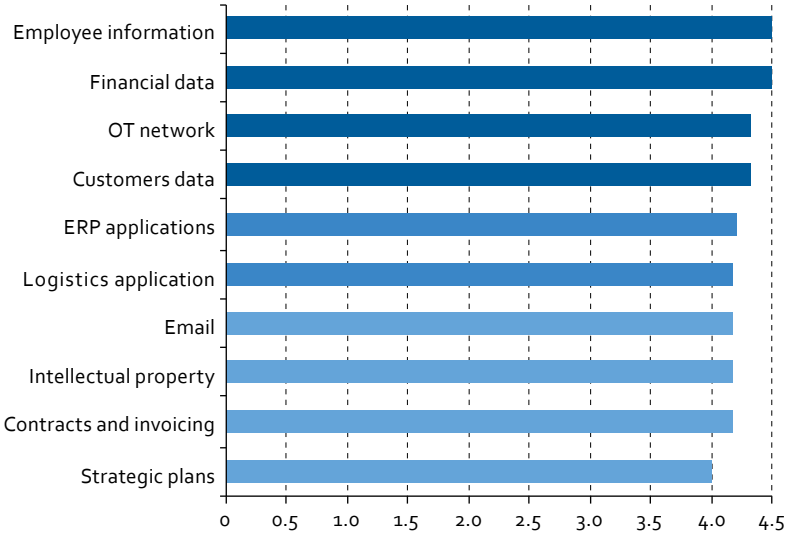

C. Security manager
Other (17)
CEO (33)
CISO (17)
CIO (33)


D. Work teams
External (0)
Internal/ external Collaboration (67)
Internal (33)

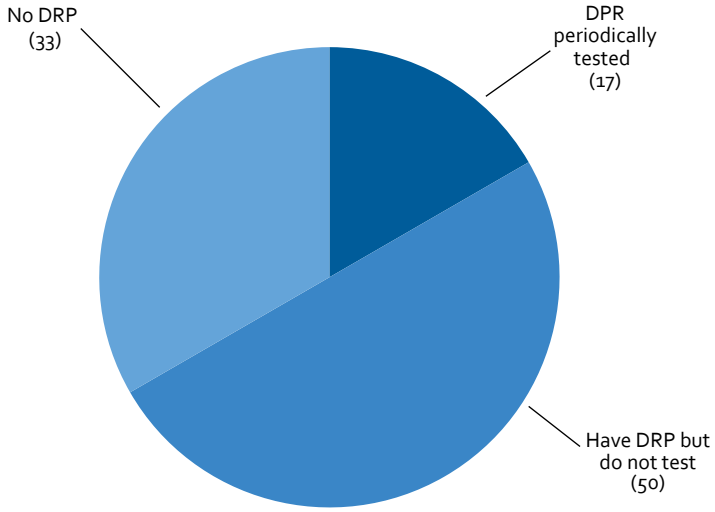

E. Concerns by type of threat
Ransomware
APT
Zero-day
Phishing
Unauthorized access
Denial-of- Service
Personal
Web applications
SSL communications
0 0.5 1.0 1.5 2.0 2.5 3.0 3.5 4.0 4.5 5.0


F. Level of confidence in cybersecurity controls implemented
Social media
Cloud applications
Desktop computers
Web applications
Server
Business applications
Perimeter security
Laptops
Mobil devices
0 0.5 1.0 1.5 2.0 2.5 3.0 3.5 4.0 4.5

G. Concerns by target of attack



H. Organizations with a DRP



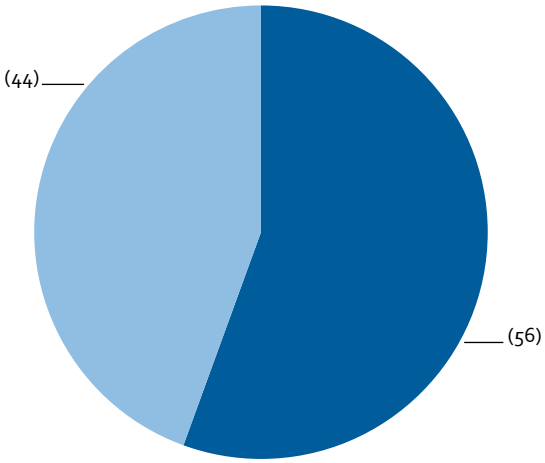
Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey and Inter-American Development Bank/Organization of American States (IDB/OAS), *Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean*, 2020.

Annex 6
Situation by country: Mexico

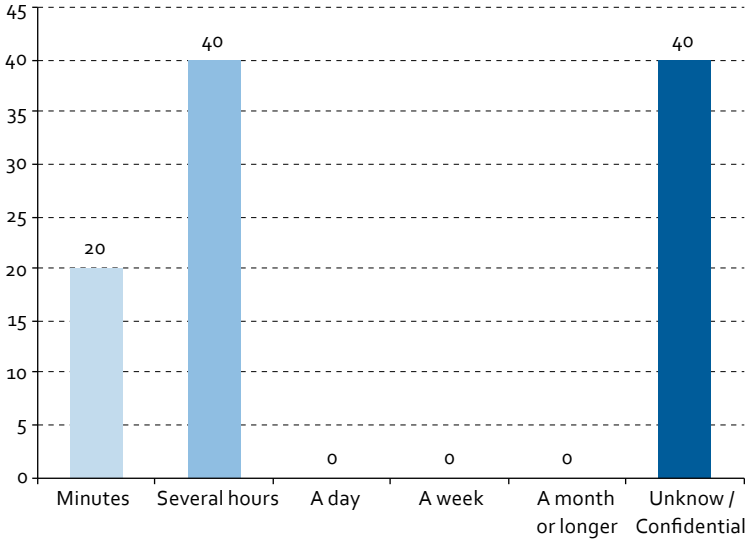
Mexico's situation is similar to that of Colombia in that there has been significant progress in its indicators in recent years, driven by a strong national strategic policy that has had a positive impact on organizations. It would be natural to expect that indicators of maturity with regard to individual awareness among the population outside the sphere of organizations would continue to evolve.

Figure A6
Situation in Mexico
(Percentages)

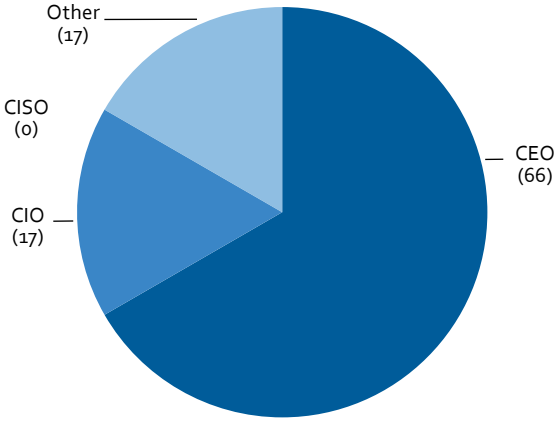
CMM maturity level: 3
A. Percentage of organizations reporting incidents in 2020



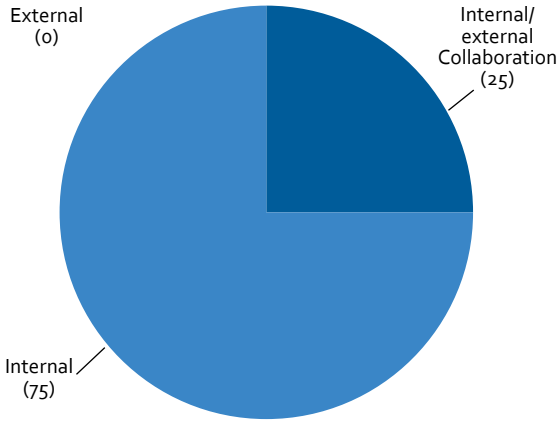
B. Incident recovery time



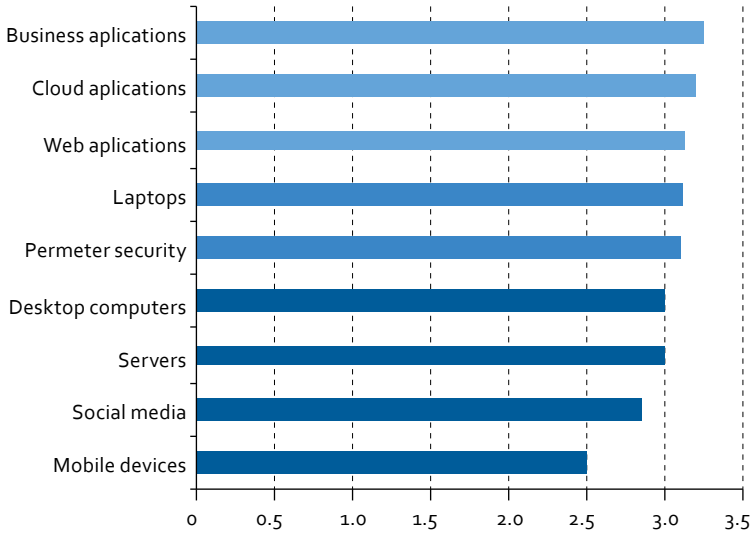
C. Security manager



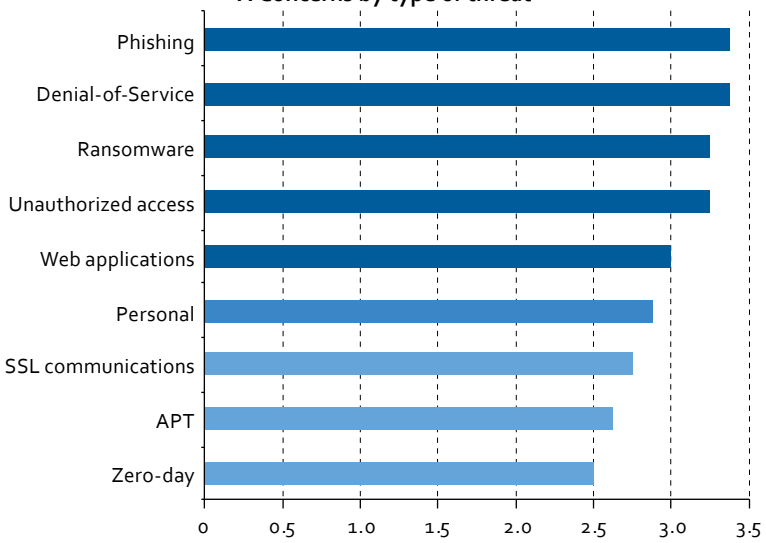
D. Work team

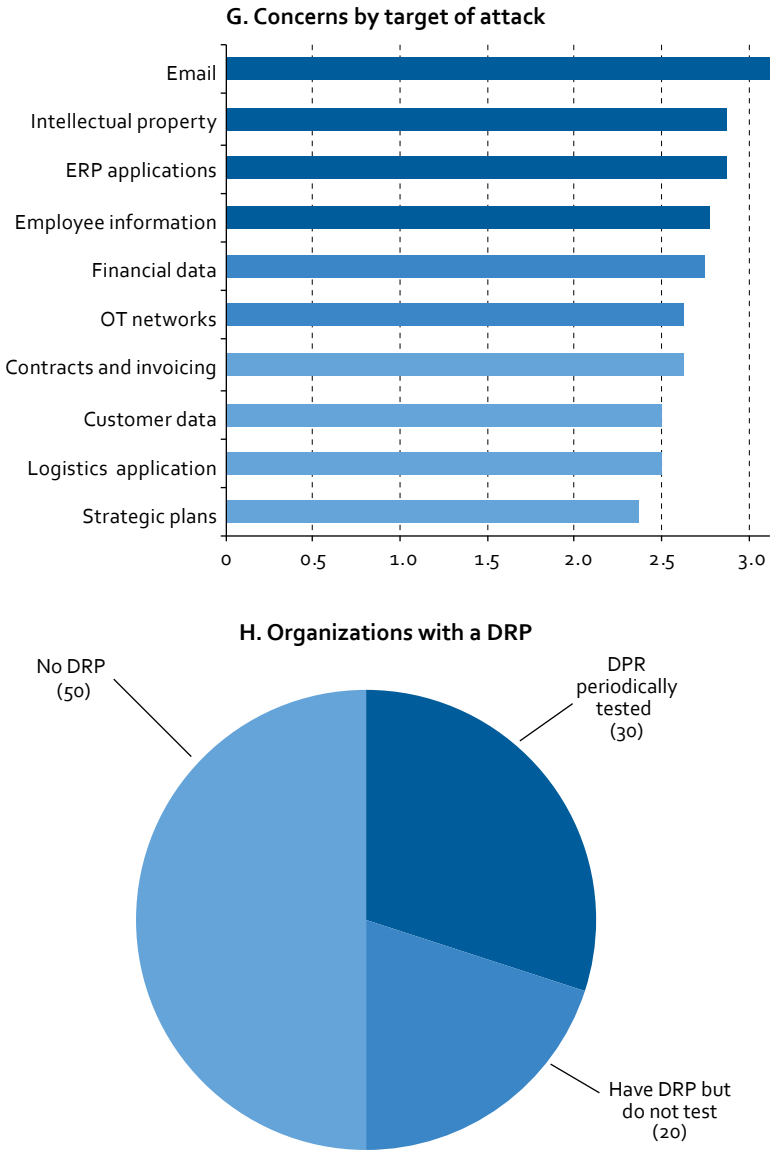


E. Level of confidence in cybersecurity controls implemented



F. Concerns by type of threat





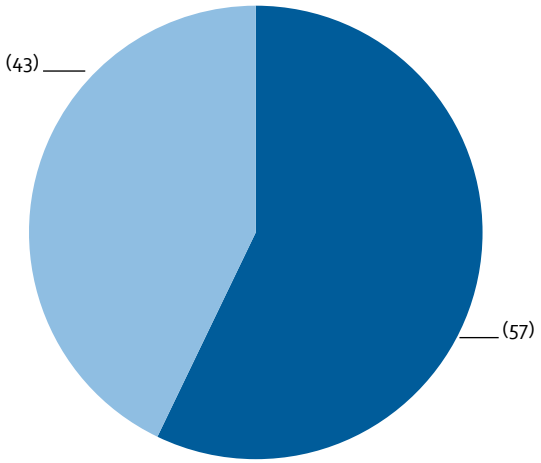
Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey and Inter-American Development Bank/Organization of American States (IDB/OAS), *Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean*, 2020.

Annex 7
Situation by country: Panama

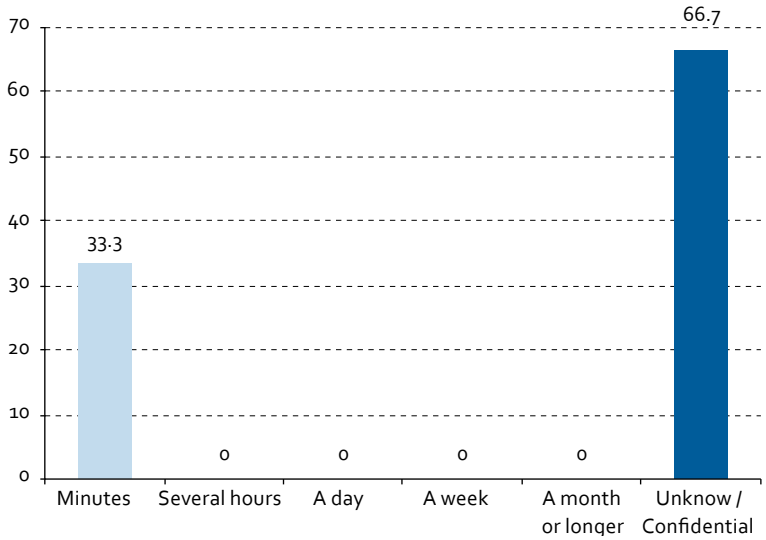
Panama shows continuity in its CMM indicators from 2016 to 2020 (IDB/OAS, 2020), a situation which, combined with the appeal that its financial structure holds for cybercriminals, could indicate the need for improvement, both in terms of infrastructure and cybersecurity culture.

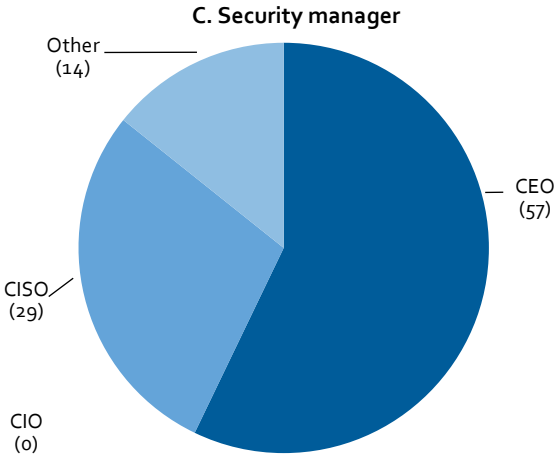
Figure A7
Situation in Panama
(Percentages)

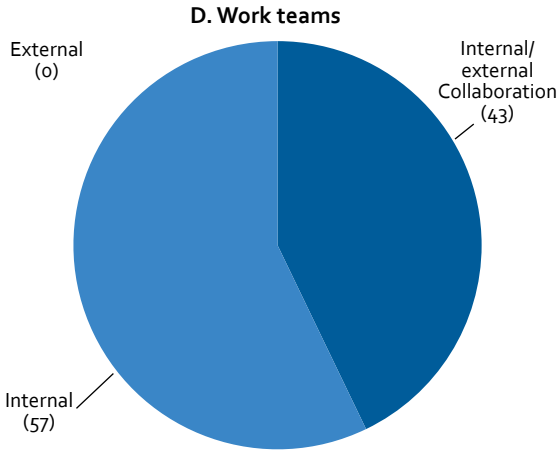
CMM maturity level: 2
A. Percentage of organizations reporting incidents in 2020

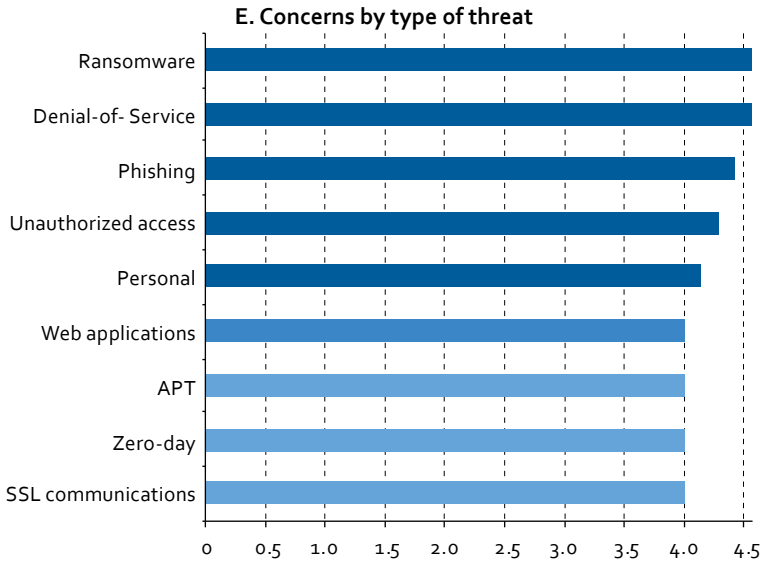


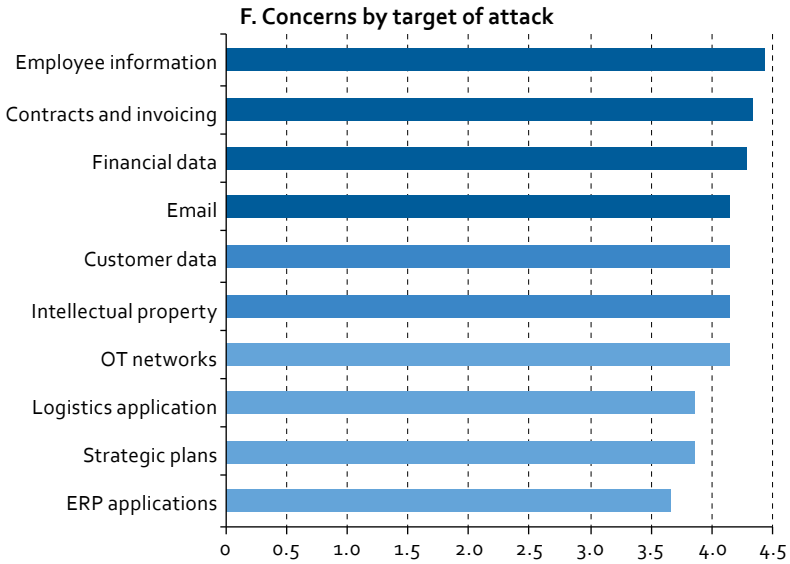
B. Incident recovery time



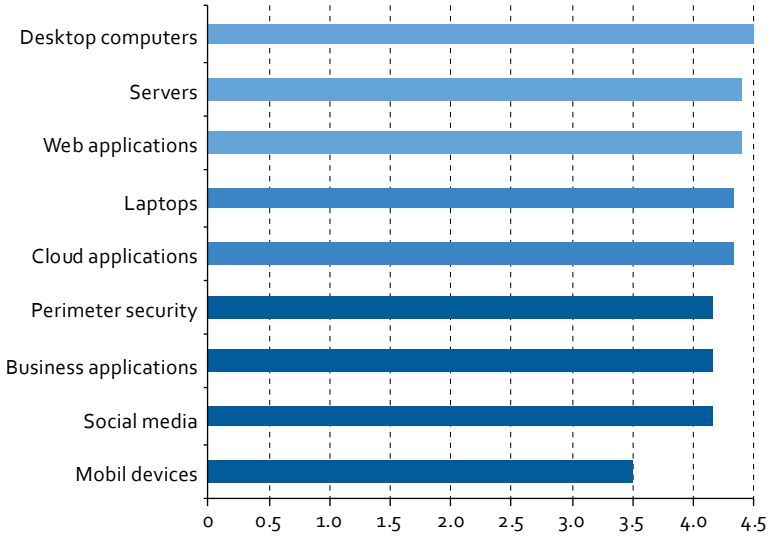

C. Security manager
Other (14)
CEO (57)
CISO (29)
CIO (0)


D. Work teams
External (0)
Internal/ external Collaboration (43)
Internal (57)

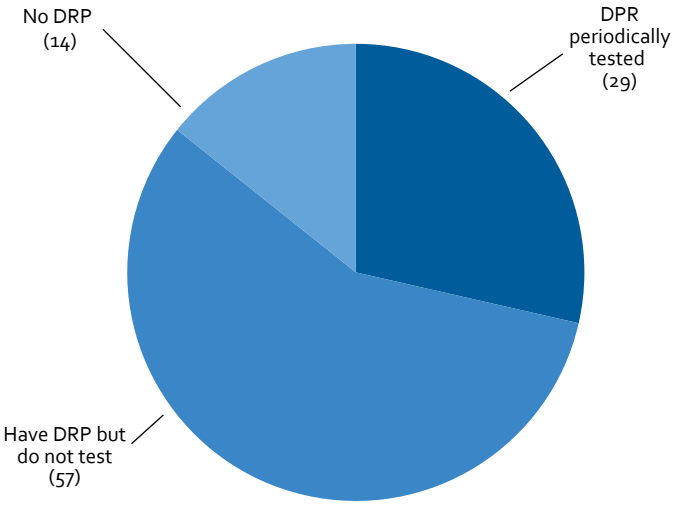

E. Concerns by type of threat
Ransomware
Denial-of- Service
Phishing
Unauthorized access
Personal
Web applications
APT
Zero-day
SSL communications
0 0.5 1.0 1.5 2.0 2.5 3.0 3.5 4.0 4.5


F. Concerns by target of attack
Employee information
Contracts and invoicing
Financial data
Email
Customer data
Intellectual property
OT networks
Logistics application
Strategic plans
ERP applications
0 0.5 1.0 1.5 2.0 2.5 3.0 3.5 4.0 4.5

G. Level of confidence in cybersecurity controls implemented



H. Organizations with a DRP



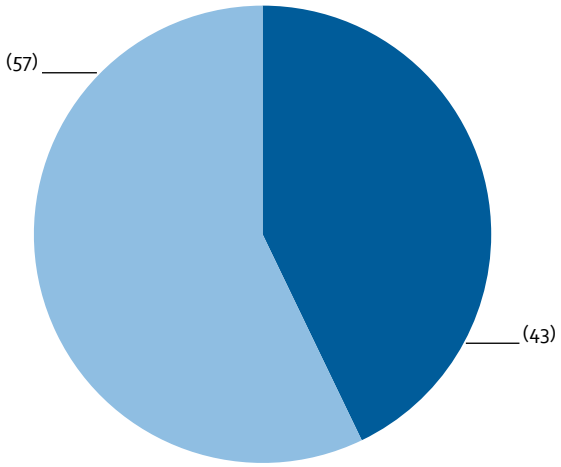
Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey and Inter-American Development Bank/Organization of American States (IDB/OAS), *Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean*, 2020.

Annex 8
Situation by country: Peru

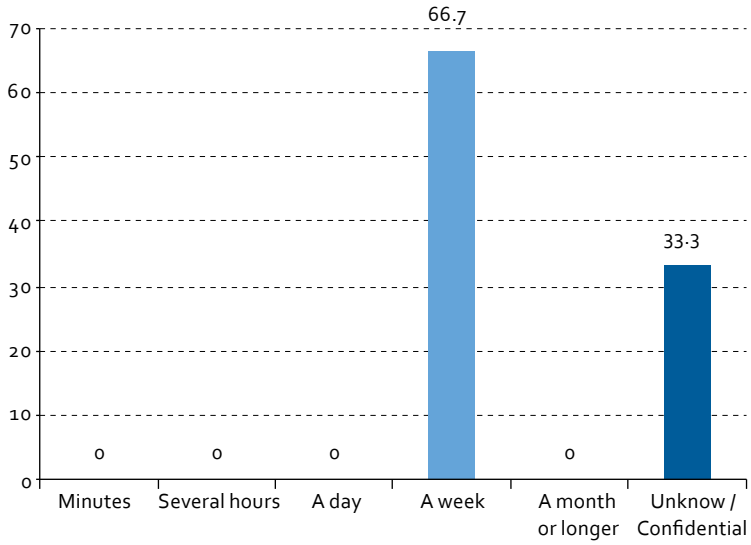
Peru has shown great progress in its indicators in recent years, reaching stage 2 of maturity as a result of a strong national strategic policy, which has had a positive impact on organizations. As in the case of Colombia and Mexico, there should be continued effort to raise individual awareness among the population outside the sphere of organizations.

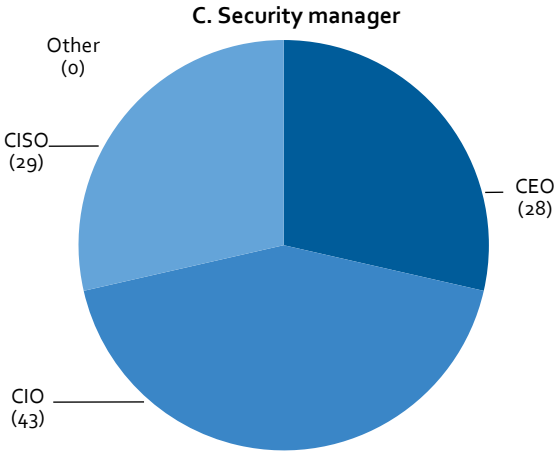
Figure A8
Situation in Peru
(Percentages)

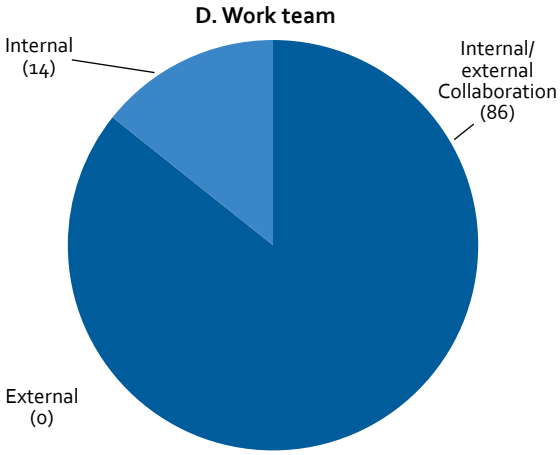
CMM maturity level: 2
A. Percentage of organizations reporting incidents in 2020

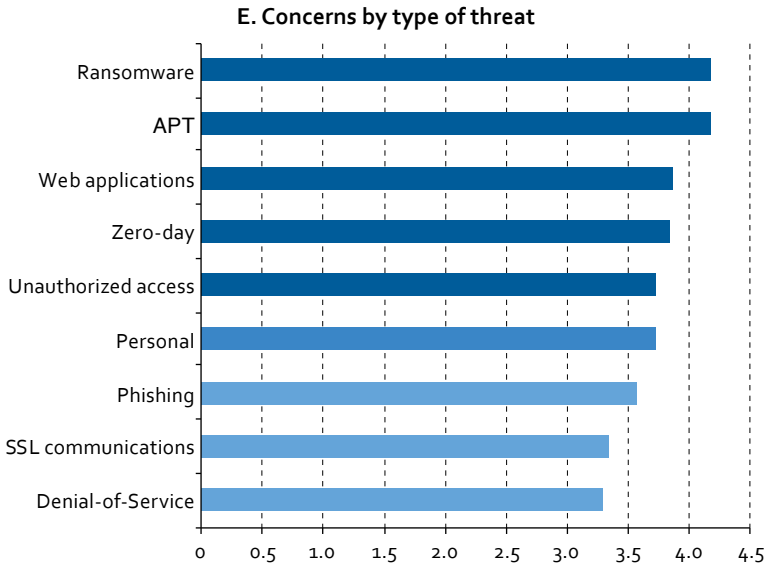


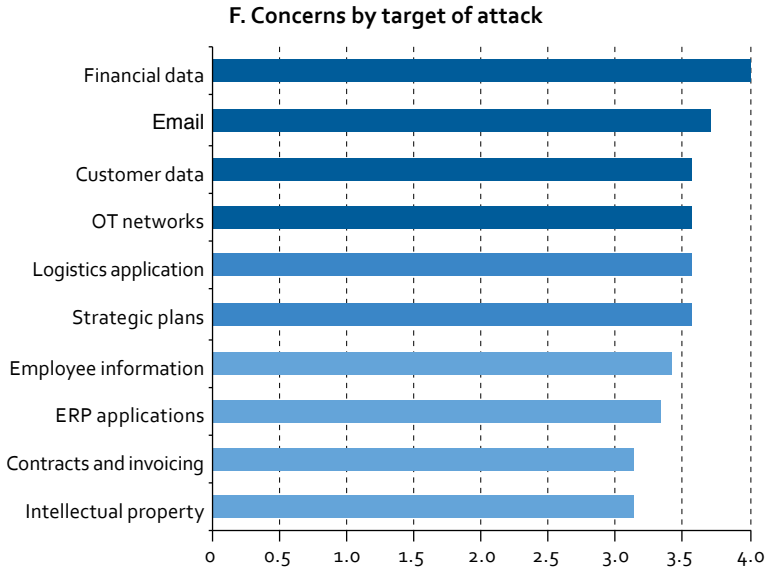
B. Incident recovery time

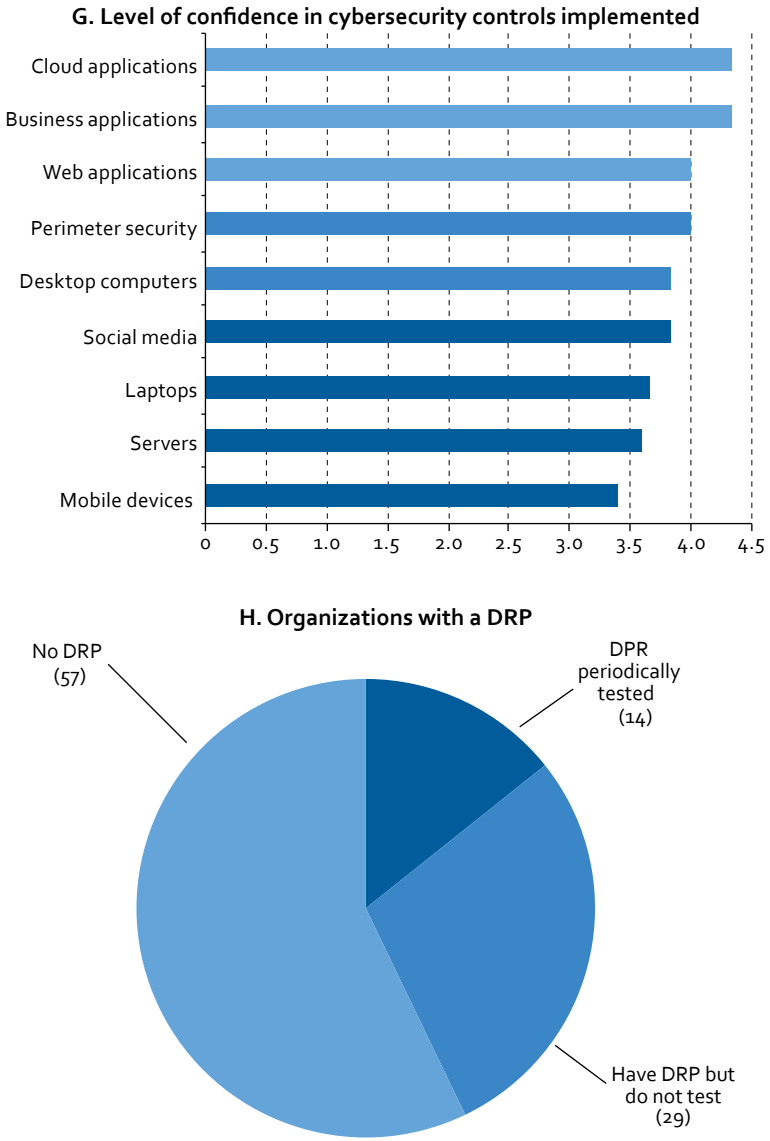



C. Security manager
Other (0)
CISO (29)
CEO (28)
CIO (43)


D. Work team
Internal (14)
Internal/ external Collaboration (86)
External (0)


E. Concerns by type of threat
Ransomware
APT
Web applications
Zero-day
Unauthorized access
Personal
Phishing
SSL communications
Denial-of-Service
0 0.5 1.0 1.5 2.0 2.5 3.0 3.5 4.0 4.5


F. Concerns by target of attack
Financial data
Email
Customer data
OT networks
Logistics application
Strategic plans
Employee information
ERP applications
Contracts and invoicing
Intellectual property
0 0.5 1.0 1.5 2.0 2.5 3.0 3.5 4.0



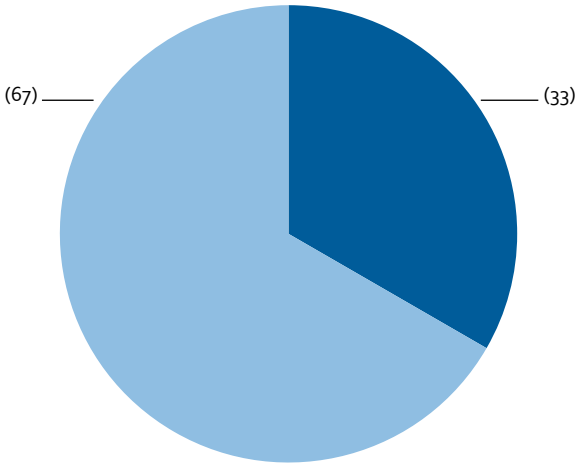
Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey and Inter-American Development Bank/Organization of American States (IDB/OAS), *Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean*, 2020.

Annex 9
Situation by country: Uruguay

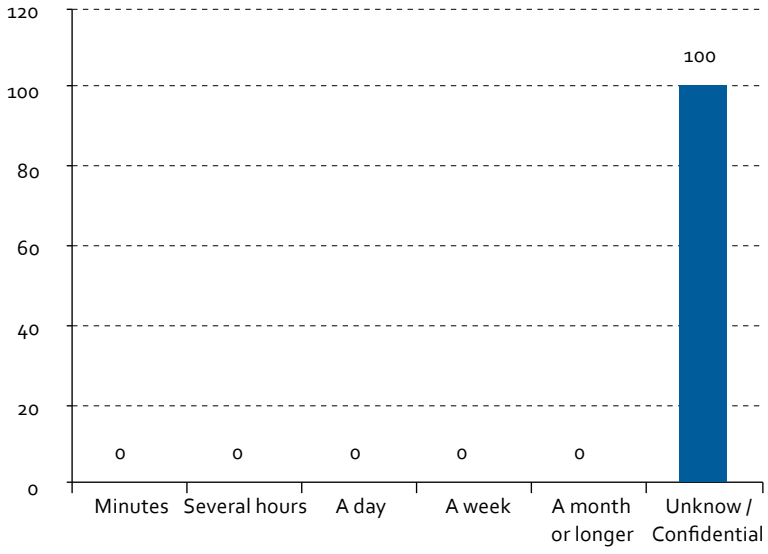
A clear national cybersecurity strategy has been in place in Uruguay since 2016, and the country showed consistent progress in 2020 (IDB/OAS, 2020), reaching the strategic stage of the CMM model in that year. Its capacity for incident response management is at the dynamic stage, as is its level of maturity in personal data protection. Both of these achievements are related to a high level of cybersecurity awareness-raising at the national level.

Figure A9
Situation in Uruguay
(Percentages)

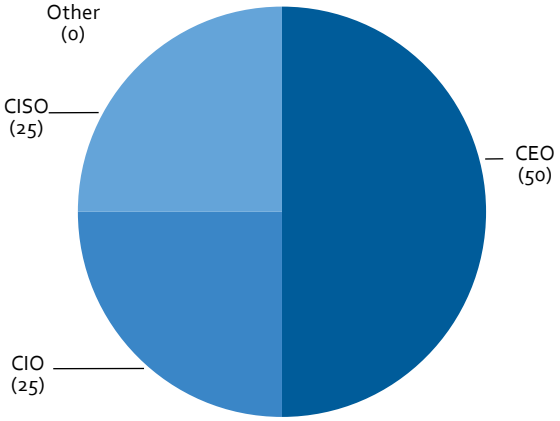
CMM maturity level: 4
A. Percentage of organizations reporting incidents in 2020



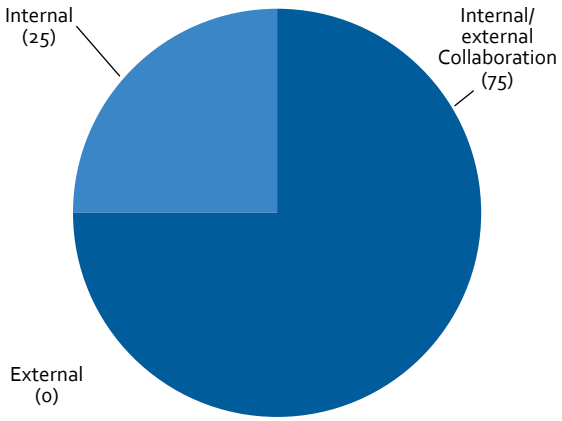
B. Incident recovery time



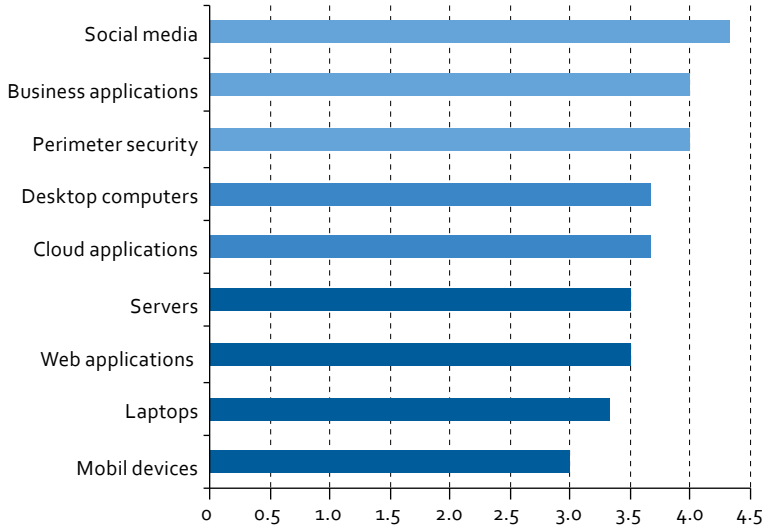
C. Security manager



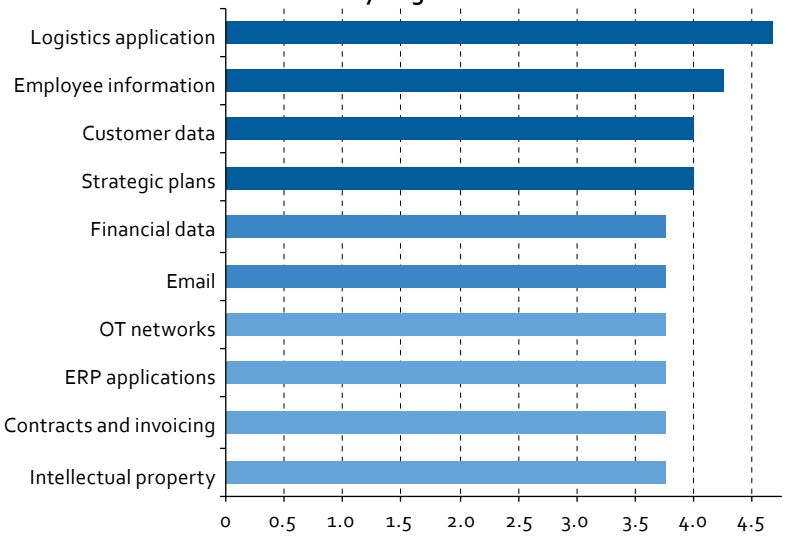
D. Work team

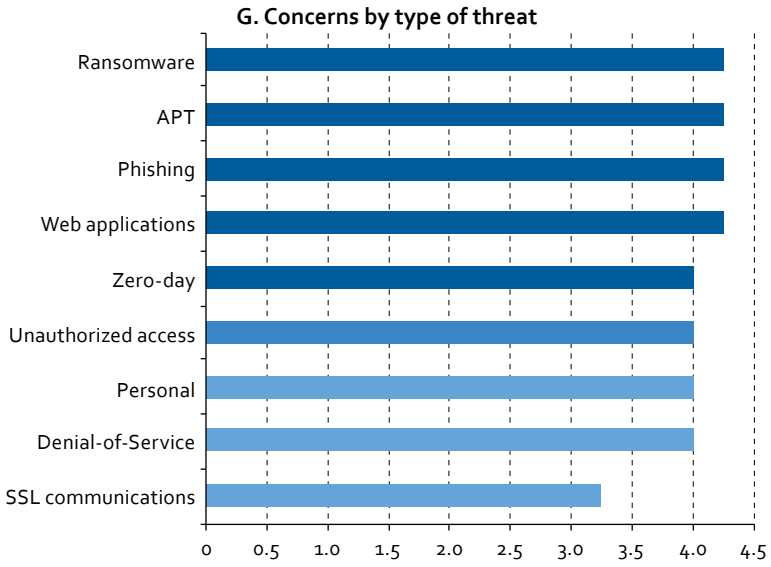


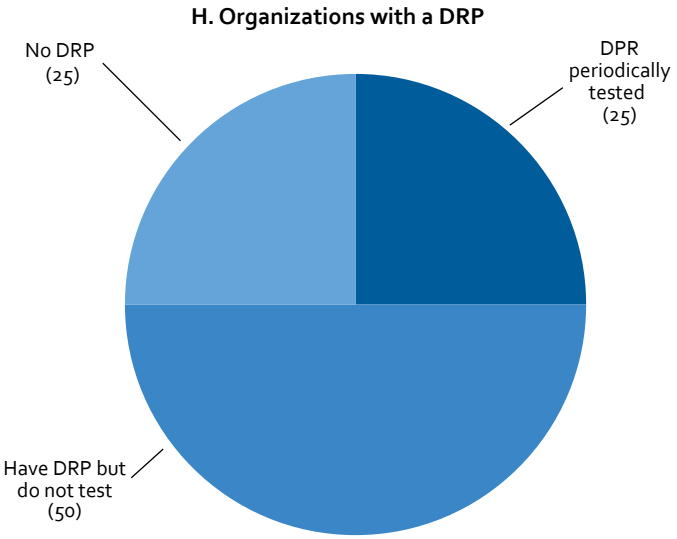
E. Level of confidence in cybersecurity controls implemented



F. Concerns by target of attack







Source: Prepared by the author, on the basis of information obtained through the Economic Commission for Latin America and the Caribbean (ECLAC) survey and Inter-American Development Bank/Organization of American States (IDB/OAS), *Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean*, 2020.

UNITED NATIONS

E C L A C

Series Production Development

Issues published

A complete list as well as pdf files are available at www.eclac.org/publicaciones

228. State of cybersecurity in logistics in Latin America and the Caribbean, Rodrigo Díaz (LC/TS.2021/108), 2021.
227. Mesoamérica digital 2025: propuesta para una agenda digital mesoamericana, Juan Jung (LC/TS.2021/77), 2021.
226. Infraestructura de Internet en América Latina: puntos de intercambio de tráfico, redes de distribución de contenido, cables submarinos y centros de datos, Raúl Echeberría (LC/TS.2020/120), 2020.
225. Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean, Héctor J. Lehuedé, (LC/TS.2020/103), 2020.
224. Institutional change and political conflict in a structuralist model, Gabriel Porcile y Diego Sanchez-Ancochea (LC/TS.2020/55), 2020.
223. Corporate governance and data protection in Latin America and the Caribbean, Héctor J. Lehuedé (LC/TS.2019/38), 2019.
222. El financiamiento de la bioeconomía en países seleccionados de Europa, Asia y África: experiencias relevantes para América Latina y el Caribe. Adrián G. Rodríguez, Rafael H. Aramendis y Andrés O. Mondaini (LC/TS.2018/101), 2018.
221. The long-run effects of portfolio capital inflow booms in developing countries: permanent structural hangovers after short-term financial euphoria, Alberto Botta (LC/TS.2018/96) 2018.
220. Agencias regulatorias del Estado, aprendizaje y desarrollo de capacidades tecnológicas internas: los casos del Servicio Nacional de Pesca y Acuicultura y el Servicio Nacional de Geología y Minería de Chile, Rodrigo Cáceres, Marco Dini y Jorge Katz (LC/TS.2018/40), 2018.

PRODUCTION DEVELOPMENT

Issues published:

228. State of cybersecurity in logistics in Latin America and the Caribbean
Rodrigo Díaz

227. Mesoamérica digital 2025
Propuesta para una agenda digital mesoamericana
Juan Jung

226. Infraestructura de Internet en América Latina
Puntos de intercambio de tráfico, redes de distribución de contenido, cables submarinos y centros de datos
Raúl Echeberría

225. Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean
Héctor J. Lehuedé

ECLAC
Economic Commission for Latin America and the Caribbean (ECLAC)
Comisión Económica para América Latina y el Caribe (CEPAL)
www.eclac.org

LC/TS.2021/108