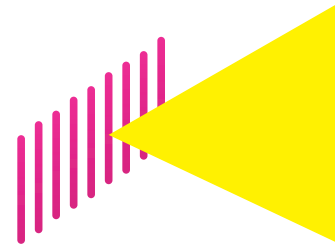




IMPACT OF DIGITAL SECURITY INCIDENTS IN

COLOMBIA 2017



OAS Cataloging-in-Publication Data

Impact of digital security incidents in Colombia 2017 / [Prepared by the Organization of American States, the Inter-American Development Bank and the Ministry of Information and Communication Technologies of Colombia].

p.; cm. (OAS / Official Documents, OEA / Ser.D / XXV.11)

ISBN 978-0-8270-6675-5

1. Computer security - Colombia. 2. Cyberspace - Security measures - Colombia. 3. Computer networks - Security measures - Colombia. 4. Computer crimes - Colombia.

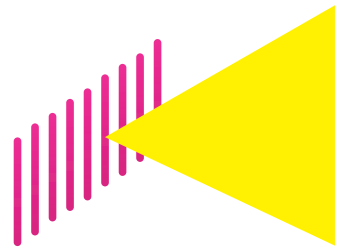
I. Organization of American States. Secretariat for Multidimensional Security. II. Inter-American Development Bank. III. Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones. IV. Series. V. OAS / CICTE Cyber Security Program. VI. Inter-American Committee against Terrorism.

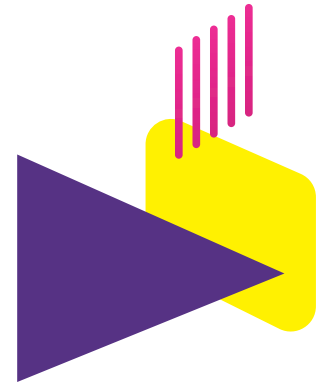
OEA / Ser.D / XXV.11 2017

Original Published in Spanish

IMPACT OF DIGITAL SECURITY INCIDENTS IN

COLOMBIA 2017





Copyright © 2017 Organization of American States.

This work is subject to a Creative Commons Attribution-Noncommercial-NoDerivs 3.0 IGO license (CC BY-NC-ND 3.0 IGO) (<http://creativecommons.org/licenses/by-ncnd/3.0/igo/legalcode>) and may be reproduced for any non-commercial use by granting recognition to the OAS and MINTIC. Derivative works are not allowed. Any dispute relating to the use of the work which cannot be amicably resolved shall be submitted to arbitration in accordance with UNCITRAL rules. The use of the OAS and/or MINTIC name for any purpose other than the respective recognition and use of the OAS and/or MINTIC logo are not authorized by this CC-IGO license and require an additional license agreement of the relevant organization. Note that the URL link includes additional terms and conditions of this license. The views expressed in this publication are those of the authors and do not necessarily reflect the views of the Organization of American States or its member countries.

This study has the financial support of the government of Canada



CREDITS

DAVID LUNA

Minister of Information and
Communication Technologies of
Colombia (MINTIC)

LUIS ALMAGRO

Secretary General of the Organization
of American States (OAS)

MINTIC TECHNICAL TEAM

Juanita Rodríguez
Orlando Garcés
Antonio Carrillo

OAS TECHNICAL TEAM

Claudia Paz y Paz
Alison August Treppel
Belisario Contreras
Bárbara Marchiori de Assis
Kerry-Ann Barrett
Jorge Bejarano
Harold Coronado

IDB TECHNICAL TEAM

Ana María Rodríguez-Ortiz
Carlos Santiso
Javier León
Miguel Porrúa
Florencia Cabral

ASSOCIATES

Danil Kerimi
Lara Pace
Andres Galindo
Gonzalo Romero

ASSOCIATES

Asociación Bancaria y de Entidades Financieras de Colombia

-ASOBANCARIA-

Asociación Colombiana de las Micro, Pequeñas y Medianas Empresas

-ACOPI-

Asociación Nacional de Empresarios de Colombia -ANDI-

Asociación Nacional de Empresas de Servicios Públicos y Comunicaciones

-ANDESCO-

Cámara Colombiana de Comercio Electrónico -CCCE-

Cámara Colombiana de Informática y Telecomunicaciones -CCIT-

Centro Cibernético Policial de la Policía Nacional -CCP-

Comando Conjunto Cibernético del Comando General de las Fuerzas

Militares -CCOC-

Comisión de Regulación de Comunicaciones -CRC-

Confederación Colombiana de Cámaras de Comercio -CONFECAMARAS-

Consejo Nacional Gremial -CNG-

CSIRT de la Policía Nacional -CSIRT PONAL-

Departamento Administrativo Dirección Nacional de Inteligencia -DNI-

Departamento Nacional de Planeación

Federación Colombiana de la Industria de Software y Tecnologías de la

Información -FEDESOFIT-

Federación Nacional de Comerciantes -FENALCO-

Grupo de Respuesta a Emergencias Cibernéticas -colCERT-

Ministerio de Defensa Nacional

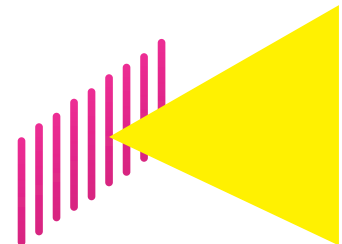
Ministerio de Justicia y del Derecho

Ministerio de Relaciones Exteriores

Ministerio de Tecnologías de la Información

y las Comunicaciones

Presidencia de la República





A decorative graphic on the left side of the page, consisting of a series of vertical bars of varying heights in shades of pink and purple, followed by a large yellow triangle pointing to the right.

TABLE OF CONTENTS

MAIN CONCLUSIONS AND OBSERVATIONS	13
READER'S GUIDE	19
FOREWORD	23
PART 1 PRIVATE SECTOR ANALYSIS	31
COMPANY PROFILES	32
DIGITAL SECURITY PRACTICES IN COMPANIES	36
DIGITAL INCIDENTS IN COMPANIES	46
DIGITAL SECURITY BUDGET IN COMPANIES	56
COST OF DIGITAL INCIDENTS FOR COMPANIES	61
PART 2 – ANALYSIS OF PUBLIC SECTOR ENTITIES	69
PROFILE OF THE ENTITIES	70
DIGITAL SECURITY PRACTICES IN ENTITIES	74
DIGITAL INCIDENTS IN ENTITIES	80
DIGITAL SECURITY BUDGET IN ENTITIES	85
COST OF DIGITAL INCIDENTS FOR ENTITIES	89
APPENDIX 1 – SITUATIONAL ANALYSIS	97
APPENDIX 2 – METHODOLOGY	115
APPENDIX 3 – COMPLEMENTARY STATISTICAL ANALYSIS	119



TABLE OF TABLES

TABLE 1: Median of the Annual Digital Security Budget by Enterprise that Assigns Resources for IT (2016)	58
TABLE 2: Budget Allocation for Digital Security Issues (2016)	59
TABLE 3: Total Median Cost per Company that estimated the Impact of Digital Incidents (2016)	67
TABLE 4: Total Cost per Company Sales (2016)	67
TABLE 5: Median of the Digital Security Budget by Entity that Assigned IT Resources (2016)	87
TABLE 6: Allocation of the Digital Security Budget by Entity that Allocated Resources to IT (2016)	88
TABLE 7: Estimation of the likelihood that a Company will identify Digital Incidents (2016)	120
TABLE 8: Regression Results - Number of Incidents (2016)	121
TABLE 9: Regression Results - Budget assigned by Company for Digital security (2016)	122
TABLE 10: Regression Results - Cost With Digital Incidents (2016)	123
TABLE 11: Estimation of the likelihood that a Public Entity will identify Digital Incidents (2016)	124
TABLE 12: Regression Results - Budget Allocated by the Public Entity for Digital security (2016)	125

TABLE OF GRAPHS



GRAPH 1: Size of the Companies _____	32
GRAPH 2: Economic Sector of Interviewees _____	33
GRAPH 3: Number of Employees in the Companies _____	34
GRAPH 4: Approximate Percentage of your Company Personnel with Internet Access _____	35
GRAPH 5: Level of Readiness to Deal with a Digital Incident (Economic Sector) _____	37
GRAPH 6: Level of Readiness to Deal with a Digital Incident (Company Size) _____	38
GRAPH 7: Digital Security Practices (Economic Sector) _____	39
GRAPH 8: Digital security Practices (Company Size) _____	40
GRAPH 9: Position (s) or Role (s) Dedicated to Digital security (Companies' Size and Economic Sector) _____	41
GRAPH 10: Cyber Risk Assessment (Size of Enterprises) _____	42
GRAPH 11: Cyber Risk Assessment (Economic Sector) _____	43
GRAPH 12: Data and Assets Prioritized by the Company (2016) _____	44
GRAPH 13: Percentage of Companies that Identified Digital Incidents, According to Company Size (2016) _____	46
GRAPH 14: Percentage of Companies that Identified Digital Incidents, by Economic Sector (2016) _____	47
GRAPH 15: Change in the Severity of Digital Incidents (2016) _____	49
GRAPH 16: Gravity of Digital Incidents (2016) _____	51
GRAPH 17: Notice of Digital Incident (2016) _____	54
GRAPH 18: Number of Digital Incidents Identified by Companies (2016) _____	55
GRAPH 19: Annual Digital Security Budget of Companies that Allocate Resources for IT (2016) _____	57
GRAPH 20: Companies That Estimated the Negative Consequences of Digital Incidents (2016) _____	61
GRAPH 21: Costs of Operation Disruption Incurred by Companies That Estimated the Impact of Digital Incidents (2016) _____	62
GRAPH 22: Costs of Damage to Assets and Infrastructure Incurred by Companies That Estimated the Impact of Digital Incidents (2016) _____	63
GRAPH 23: Costs of Penalties, Fines and Legal Expenses Incurred by Companies That Estimated the Impact of Digital Incidents (2016) _____	64
GRAPH 24: Costs of Reputational Damage Incurred by Companies That Estimated the Impact of Digital Incidents (2016) _____	67



TABLE OF GRAPHS

GRAPH 25: Costs of Intellectual Property Losses Incurred by Companies That Estimated the Impact of Digital Incidents (2016)	66
GRAPH 26: Investment in R&D&I	68
GRAPH 27: Public Power Branch of Which the Entity is Part	70
GRAPH 28: Government Tier of the Entity	71
GRAPH 29: Region Where the Entity is Located	72
GRAPH 30: Number of People Working in the Entities	73
GRAPH 31: Percentage of Staff of Your Institution with Access to the Internet (2016)	74
GRAPH 32: Level of Readiness of the Entity to Deal with a Digital Incident	75
GRAPH 33: Digital Security Practices Implemented by Entities	76
GRAPH 34: Entities with an Area, Position (s) or Role (s) Dedicated to Digital security	77
GRAPH 35: Data and Assets Prioritized by Entities	79
GRAPH 36: Percentage of State Entities That Identified Digital Incidents (2016)	81
GRAPH 37: Change in the Severity of Digital Incidents	83
GRAPH 38: Severity of Digital Incidents	84
GRAPH 39: Digital Security Budget (2016)	86
GRAPH 40: Entities that Estimated the Negative Consequences of Digital Incidents (2016)	89
GRAPH 41: Information Disruption Costs Incurred by State Entities That Estimated the Impact of Digital Incidents (2016)	90
GRAPH 42: Costs of Damage to Assets and Infrastructure Incurred by State Entities That Estimated the Impact of Digital Incidents (2016)	91
GRAPH 43: Costs of Penalties, Fines and Legal Expenses Incurred by State Entities That Estimated the Impact of Digital Incidents (2016)	91
GRAPH 44: Reputational Damage Incurred by State Entities That Estimated the Impact of Digital Incidents (2016)	92
GRAPH 45: Costs of Loss of Intellectual Property and Sensitive Information Incurred by State Entities That Estimated the Impact of Digital Incidents (2016)	93
GRAPH 46: Investment in R&D&I of Entities Estimating the Impact of Digital Incidents (2016)	95
GRAPH 47: Comparison of CMM results (2016 and 2017)	105



MAIN CONCLUSIONS AND OBSERVATIONS



MAIN CONCLUSIONS AND OBSERVATIONS ✦

This collaborative study between MINTIC, the OAS and the IDB represents a pioneering initiative in the region, which is rare on a global scale, since it highlights information, which is difficult to collect, about threats to a country's digital security and its ability to defend itself against them. The Colombian government is thus at the forefront of the generation of knowledge in the area of digital security to facilitate the design and implementation of policies that address the weaker aspects of the scenario as revealed in this study.

The information gathered provides a complete picture of the attacks on both the public and private sectors, as well as their level of preparedness to defend against such attacks. The study aims to present the information according to the

different profiles of both public and private institutions, and numerous statistical tools have been used to make it easier for the readers to draw their own conclusions.

Colombian organizations participating in this study have a high level of connectivity, for the most part. Of the companies interviewed, 65% reported that between 81% and 100% of their workforce had access to the Internet. In the public sector, 69% of the participating entities reported that between 81% and 100% of their employees had access to the Internet at work.

When Colombian organizations are asked if they believe they are prepared to deal with a digital incident, a simple average of 37% of the companies that participated in the study (companies in the Service, Industry and Commerce sectors) believe that they are prepared to handle a digital incident. As for the size of these companies, 70% of large enterprises feel very prepared or prepared to handle a digital incident, compared to 45% of micro-enterprises. When public entities are asked the same question, one of the results found is that most entities at the national level "feel prepared". Study participants at the national level reported that 13% and 48% felt very prepared or prepared, respectively. However, when compared to municipal and province authorities, data show that only 28% at the




municipal level and 38% at the province level felt very prepared or prepared to handle an incident. A higher level of confidence in preparation is observed at the national level, so it would be interesting to develop public policy initiatives focused at the province and municipal levels.

The study also included specific questions about digital security measures adopted by the organization, in order to be able to compare them with their level of security perception. **It was noted that, in general, Colombian organizations that replied that they feel prepared, in fact, adopt more security measures than other organizations.** For example, **large enterprises tend to adopt more security measures than microenterprises, and national public entities have a greater concern with digital security than territorial entities.** However, organizations that feel more prepared still need to increase their digital security measures, which should include a larger budget allocation for digital security issues.

Among the most important measures that could be identified to ensure a Colombian organization against digital incidents is the identification of a full-time position for the management of digital incidents. This position is important because it will help organizations quickly detect, isolate and resolve incidents as they occur.

Among all those who answered the question: "Does your entity/company have an area, position (s) or role (s) dedicated to digital security (digital security and/or information security)?," 70% of large enterprises responded "yes" compared to merely over 20% of micro-enterprises. Among economic sectors, most companies in the industry sector said they have a dedicated team, with a little more than 54% responding positively to the question, compared to only 45% and 42% of companies in the Service and Commerce sectors, respectively. Among public entities, only 33% at the national level and 10% and 17% at the municipal and province level, respectively, have an area dedicated to digital security within their organization. It was noted that there is a general tendency to transfer responsibility for incident response and digital security under the general functions of IT departments.

When asked, on a scale of 1-5, what respondents believe to be the main factors that would affect their ability to address digital security, they respond that the **lack of dedicated staff and lack of budget were rated as the main factors, with the lack of awareness of employees immediately following.** In fact, analyses of the budget allocation to digital security issues confirmed this concern of respondents, as noted below.



Having the ability to identify incidents is important for entities, given it is the first step to contain a malicious attack and to be able to respond. When asked whether digital incidents against their organization were identified in 2016, **more than 70% of micro-enterprises replied that they had not identified digital incidents.** Among small enterprises, approximately 60% also did not identify digital incidents. However, among medium and large enterprises, most replied that they did identify digital incidents: 51% and 63%, respectively. When analyzing the different economic sectors, only in the industry sector was where most of the companies identified digital incidents, with 52% of the companies. With respect to state entities, 59% of national entities identified digital incidents, while 56% of territorial-province entities responded alike. On the other hand, 42% of municipal entities responded that they have identified digital incidents.

A statistically significant positive relationship was shown between the implementation of technical measures—such as vulnerability testing and maintenance of the Information Technology infrastructure—and the identification of digital incidents by public and private organizations. This is also seen with the explanatory variable related to the practice of cybernetic risk assessment. That is, organizations that implement more digital security measures tend to identify a greater number of digital incidents. This

means that many organizations that do not implement these measures are unaware that they are targets of cyber-attacks. Likewise, a statistically positive relationship was observed in the National Digital Security Policy (CONPES Document 3854, 2016), approved on April 11, 2016, and the identification of digital incidents by state entities.

Regarding the types of incidents occurring, in the question: What types of digital incidents, cyber threats or cyber-attacks has your entity/company identified in 2016?, the study participants responded that malware and phishing were among the most common types of incidents. It was noted that within the Service sector, 50% of respondents noticed an increase in malware attacks, 47% phishing, 39% web-based attacks, and 18% denial of service attacks. In the Commerce sector, similar observations were made with 53% reporting an increase in malware, 41% reported an increase in phishing and 21% noticed an increase in both web-based attacks and denial-of-service attacks. Interestingly, however, there were some variations within the industry sector in this observation, since 67% reported an increase in the severity of web-based attacks and malware and 59% reported an increase in phishing attacks. In terms of entities that actually identify not only the increase in severity but the type of attacks, study participants reported that they have seen a major increase in phishing and malware attacks.

When analyzing the values of companies that allocated a budget to digital security, **it was observed that the median digital security budget in relation to company sales was approximately 0.3% of sales in 2016.** Micro-enterprises have smaller digital security budgets in absolute terms. On the other hand, companies in the service sector (mainly in the financial sector) tend to allocate a larger budget to digital security.

In public entities, the estimate of the median budget allocated to digital security in relation to the investment budget was approximately 0.05% of total investments in 2016.

That is, when the digital security budget was allocated, this budget did not reach 1% of organizations' sales or investments in 2016. In addition, it was verified that, on simple average, most of the budget was allocated for platforms and technological means, while the capacity generation received the least amount of resources in both public and private organizations. It should be stressed that capacity building includes issues such as training and awareness of employees and officials. As mentioned, the lack of dedicated staff to the area and lack of budget were classified as the main factors that affected digital security in organizations, with the lack of awareness of employees immediately following.

It is important to note that many of the organizations do not estimate the cost of digital incidents: 79% of companies said they had no estimated costs, while 85% of public entities said they did not make any estimates. In this context, estimates were made based on the organizations that did estimate the cost of digital incidents.

It can be observed that the relative cost of digital incidents decreased as companies increased in size. Although large enterprises had an absolute cost with digital incidents much higher than the costs incurred by a microenterprise, the relative cost of digital incidents of a large company was significantly smaller. **It is very important to note that there is a greater number of companies with costs related to the loss of intellectual property in excess of \$325 million Colombian pesos about 10% of the companies, where 3% had intellectual property losses of more than COP 4,000,000,000.** In the latter group, the majority consisted of large enterprises, including enterprises in the commerce sector, and the financial sector.

The results indicate that there is a significant and positive relationship between cost and number of incidents. **According to the model, it is estimated that the increase of one unit in the number of incidents increases the cost incurred by companies in Colombia by approximately \$ 500,000 Colombian pesos because of digital**



incidents. It is important to keep in mind that this value is an estimate based on the reported information and that some incidents may have lower values, while others higher.

In relation to the national state entities, the cost represented approximately 0.5% of the investment of the public entities.

However, these data refer to national state entities of the executive branch or to autonomous national entities. There was not a significant number of territorial entities that responded to information regarding cost.

In summary, it can be concluded that implementation of digital security measures is essential not only for protection, but also to gain a better understanding of the impact of digital incidents on Colombian organizations. **Although many organizations claim to be prepared for digital incidents, many do not have dedicated digital security personnel**, with the general tendency to shift responsibility for incident response and digital security to the overall functions of IT departments.

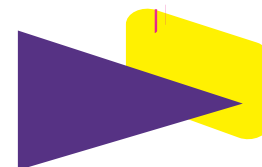
Budget allocation to digital security is less than 1% of organizations' sales/investments and about 10% of this 1% is allocated to training and awareness issues. This is worrying, especially when considering that most organizations involved in the study have about 81% to 100% of their employees and officials

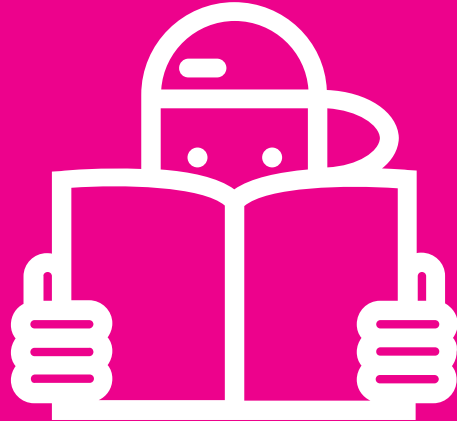
connected to the Internet, and particularly with the increase in the severity of phishing and malware attacks, which can target any person within the organization.

The data collected show that cyber-attacks increase in sophistication and impact, but investment in human and technological resources for defense and budget allocations focused on digital security is still small and growing slowly. The seriousness of the threats and the harm they cause require urgent action where the public and private sectors can collaborate closely.

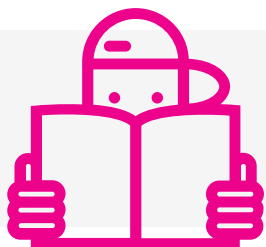
From the analysis of the different Colombian organizations, it was observed that large enterprises are more prepared and, although absolute costs of digital incidents are higher, their relative costs are smaller than the costs of microenterprises.

That is, it is estimated that the costs of digital incidents have a greater impact on microenterprises. With respect to state entities, there is statistically positive relationship in knowing the National Digital Security Policy (CONPES Document 3854 of 2016) and identifying digital incidents, mainly among the national entities. It would be interesting to develop digital security policy actions with a particular focus on territorial entities.





READER'S GUIDE



READER'S GUIDE

The purpose of this instrument, prepared by the Government of Colombia through the Ministry of Information and Communication Technologies (MINTIC), the Organization of American States (OAS) and the Inter-American Development Bank (IDB), is to obtain information on digital security threats (cybersecurity and/or information security) and their impact on the country.

The National Digital Security Policy, approved on April 11, 2016 by the National Digital Security Council, through the issuance of Document CONPES 3854 of 2016, reported on the need to ***“Create both the conditions for multiple stakeholders to manage the digital security risk in their socio-economic activities and the confidence in the use of the digital environment”***. In this context, this study will serve as input for the national government to generate relevant instruments in relation to compliance with the defined policy and prioritization of the development

of future plans in the field. More specifically, this study will identify the main incidents, threats and attacks against digital security (cybersecurity and/or information security) that are affecting the country, recognize the main targets or objectives and know the economic costs that they represent for the different sectors

of the economy of the country and the Government, among others. Therefore, this study aims to identify how digital security incidents are affecting Colombian organizations in both the private sector and the public sector, using the figures for 2016.

The study is divided into two parts as follows:

PART 1) Private Sector Analysis: This analysis is divided into five sections. The first section provides information on the profile of Colombian companies, such as the size, number of employees, economic sector and the approximate percentage of company personnel with Internet access to carry out their professional activities. This data aided in the analysis of companies' digital security taking into account their different profiles. The second section of the analysis presents information on digital security measures taken by companies, such as digital security technical measures, organizational policies and risk management. The third section describes the digital incidents to the company during

the time period analyzed. The fourth section estimates the budget allocated to digital security issues by the company, and finally, the last section seeks to identify the costs of the consequences of digital incidents.

PART 2) Analysis of public sector entities: Similar to the analysis of the private sector, this analysis is divided into five sections. The first provides a summary of the profile of the Colombian public entities interviewed, also including information about the government tier to which the entity belongs, number of personnel, and percentage of the entity staff with access to the Internet. The second section describes the digital security measures taken by the various entities, while the third section describes the types of incidents occurring during the period of time analyzed by the entities interviewed. The fourth section describes the budget allocation, and the last part analyzes the costs related to the digital incidents.

APPENDIX 1) Situational Analysis: It provides an overview of Colombia's digital security landscape and it includes an situational analysis of digital security capacity in Colombia, based on the results of the Report prepared by the OAS, IDB and the Global Cybersecurity Capacity Centre, University of Oxford, entitled "*Cybersecurity: Are We Ready in Latin America and the Caribbean?*" The levels

of maturity described in this report cover five dimensions: (1) Policy and Strategy; (2) Culture and Society; (3) Education; (4) Legal Frameworks; and (5) Technologies. The situational analysis also provides information on the progress in digital security and other activities related to the field of digital security.

APPENDIX 2) Methodology: It describes the methodology adopted for this study. It includes the rationale for the development of the questions raised in the information collection instrument used, as well as the distribution methodology adopted.

APPENDIX 3) Supplementary statistical analysis: It presents the results of the linear regressions conducted in this study, as well as the estimates of the LOGIT models adopted.







FOREWORD



**DAVID
LUNA**

MINISTER OF INFORMATION TECHNOLOGIES AND COMMUNICATION OF COLOMBIA (MINTIC)

IMPACT OF CYBER INCIDENTS, THREATS AND ATTACKS IN COLOMBIA

The development of solid digital economies that contribute to the generation of economic and social prosperity in Latin America and the Caribbean requires the construction of an open, as well as safe and reliable digital environment, in line with the increase and dynamism of their

citizens' activities. To this end, the countries of our region must have a strategic vision regarding digital security and the management of the risks associated with incidents and threats that may affect the integrity of the members of society, the Social Rule of Law, the exercise of fundamental rights, national security, national defense and sovereignty.

In the case of Colombia, the growing use of Information and Communication Technologies (ICT), increased Internet connections, the massification of telecommunications networks as the basis for any socio-economic activity, and the increase in the number of services available online show a significant increase in the participation of Colombians using electronic channels.

However, the exponential use of the digital environment entails uncertainties and inherent digital security risks that, if not properly and timely managed, can lead to cyber incidents, threats and attacks, with serious economic or social consequences for the country.

Given the above, and by identifying a clear problem to be resolved, Colombia issued the National Digital Security Policy (CONPES Document 3854 of 2016), championed by the Ministries of National Defense and Information and Communications Technologies of Colombia and with the participation of all interested parties. This is one of the first national policies in the world and the first in the region to accept the September 2015 recommendations on management of digital security risks issued by the Organization for Economic Co-operation and Development (OECD). The document also incorporated the recommendations of

other international organizations such as the Organization of American States (OAS), the International Telecommunication Union (ITU) and the North Atlantic Treaty Organization (NATO).

The Policy articulates a strategic vision that seeks to make responsible use of the digital environment by the national and territorial governments, public and private organizations, the Public Force, owners and operators of critical national cybernetic infrastructures, academia and civil society, as well as strengthen their capacities to identify, manage, address and mitigate digital security risks in their socio-economic activities in the digital environment, within a framework of cooperation, collaboration and assistance.

In order to have basic input to formulate strategic documents and prioritize actions by the national government, the Ministry of ICT of Colombia, the OAS and the IDB, together with national and international experts in the field, have conducted this study, entitled Impact of cyber incidents, threats and attacks in Colombia, which presents a current overview of digital security (cybersecurity and/or information security) in Colombia; it identifies the main types of incidents, threats and attacks against it affecting public sector entities and companies; it identifies the main targets or objectives and it estimates, generally, some of the economic costs they represent for different sectors of the country's economy.

The Colombian national government is convinced that the management of digital security risks is a fundamental requirement for the processes of sector digitalization and

digital transformation of the country, and it constitutes a valuable tool for consolidating peace, strengthening confidence, massification of the Internet, poverty reduction and firming the digital economy.

For this reason, and based on the results presented in this study, it is necessary for the leaders of the public and private organizations of Colombia and the region to make a detailed review of the digital security measures implemented until today and their level of investment, in order to adapt their management and business models to maximize opportunities in the development of socio-economic activities in the digital environment.

¹ In Colombia, the number of Internet connections increased by 11 times, from 2.6 million in 2010 to 28.7 million in 2017. With 15.6 million millions of broadband Internet connections in 2017, the country increased by 609% compared to 2010, approaching similar levels of access to OECD countries, such as Portugal, Turkey and Israel, and well above the average countries of Latin America and the Caribbean.

² The country has a national fiber optic network and advances in the connection of remote areas of the national territory, through the high speed network. At present, more than 160 thousand with Internet at social rates and have installed more than 1,300 new Live Digital Kiosks in rural areas, 37 laboratories for the development of video games, applications and digital content and more 750 free WiFi zones.

³ It is estimated that 26% of micro, medium and small Colombian companies (MSMEs) buy online and 8% sell by Internet.



**CLAUDIA
PAZY PAZ**

**SECRETARY FOR MULTIDIMENSIONAL
SECURITY OF THE ORGANIZATION OF
AMERICAN STATES (OAS)**

Cybersecurity threats are now a part of our everyday reality. Sovereign nations must consider their development and economic investments in the framework of a digital world.

According to industry estimates, global spending on cybersecurity products and services will reach USD 86.4 billion by 2017,

an increase of 7 percent since 2016, with an expected expenditure of USD 93 billion in 2018. More alarming is the fact that global spending on cybersecurity products and services is projected to exceed USD 1 trillion over the next five years, 2017-2021.

With more than a decade of experience in the field of cybersecurity, the Organization of American States (OAS) provides Member States with comprehensive research and studies on cybersecurity in Latin America and the Caribbean.

It is in this line that we present this report on the practices of digital security and the impact of cyber incidents in Colombian organizations.

Since 2016, the OAS and the Ministry of Information and Communications Technologies of Colombia (MINTIC) have been cooperating with the purpose of providing technical assistance in conducting a study like this.

The OAS, through the Inter-American Committee against Terrorism (CICTE), worked closely with the Colombian Government to obtain input from national actors throughout the process of developing the report.

The results of the report show that the vast majority of companies and state entities do not carry out a cybersecurity risk assessment, and when asked which

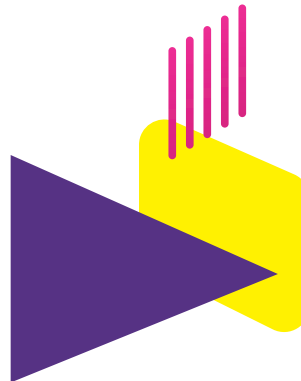
department handled cybersecurity, the vast majority responded that it was managed by the technology department: not a specific security department.

This indicates the need for enterprises to allocate greater resources for the management of cybersecurity at all levels.

The study also shows a significant relationship between cost and number of incidents, since even though organizations claim to be prepared to deal with digital incidents, many do not have dedicated cybersecurity personnel, and less than 1% of the organization's sales/investment budget is allocated to cybersecurity, with about 10% of it allocated to training and awareness-raising issues.

Colombia has demonstrated its commitment to make cybersecurity both a priority and a strong component of its socio-economic development. We are confident that this study will not only be of benefit to the Government of Colombia, but it will also provide insight into the importance of good cybersecurity practices and to the reality of the cost of cyber incidents in our region.

We look forward to continuing to support the Government of Colombia in its efforts and to continue working with the Inter-American Development Bank (IDB) to extend cybersecurity cooperation initiatives, such as this, to other countries in the region.





ANA MARÍA RODRÍGUEZ

MANAGER OF INSTITUTIONS FOR DEVELOPMENT OF THE INTER- AMERICAN DEVELOPMENT BANK (IDB)

Last year, the 2016 Cybersecurity Report “Are we ready in Latin America and the Caribbean?” showed that the region is still not ready to face the challenges of this new digital society. The region continues its efforts to keep up with the fourth digital revolution: more than half of the countries have a digital government strategy, Latin America and the Caribbean is the most active region in the world in social networks, and more than half of its population

regularly connects to the Internet. However, we are not pursuing digital security policies that ensure that our citizens and our businesses can operate in the cyberspace without risking their identity being stolen, their property damaged or their physical integrity threatened.

Like the Internet, digital security is global by nature and urges local ownership. Effective cybersecurity policies need mechanisms for the exchange of information, collaboration and coordination that bring together different countries’ efforts both in the public and private sectors. The chain that defends citizens of the digital era from cyber-attacks is as strong as its weakest link and, therefore, it must be everyone’s concern that no country is left behind in the implementation of cybersecurity policies.

Based on the data shared by companies and public institutions, this report, “Impact of Digital Security Incidents in Colombia”, reveals the main areas of digital weakness in Colombia and their effects, leaving us with messages that demand the attention of all actors in the country’s digital ecosystem. Most Colombian organizations are not adequately prepared and are being attacked; such attacks are increasingly severe and have significant economic impact. The common citizen and microenterprises are also weak links, for which it is necessary to carry out awareness and training actions to reduce their risk of

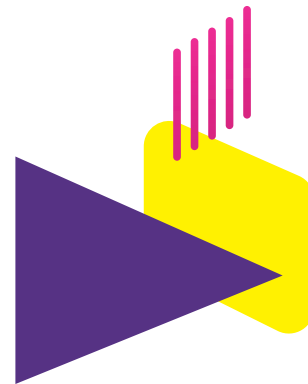
becoming victims of cyber-attacks.

The depth of this study and the information surveyed mark Colombia as a benchmark in the collection of complete data about a topic on which it is difficult for institutions to share information. This has been possible thanks to the collaboration between MINTIC, the OAS and the IDB, and the technical contributions of the World Economic Forum and the University of Oxford.

I am sure that this publication will be a useful tool to guide the implementation of the National Digital Security Policy recently launched in Colombia, and I am confident that other countries will follow its

example by studying in depth the impact of cybersecurity incidents and design the necessary policies to decrease it.

The IDB is and will continue to be an active partner in the digital transformation in Latin America and the Caribbean to maximize its benefits and control its risks. The data show that the investment in preventing cyber-attacks is less than is required to recover from them.







PART 1

PRIVATE SECTOR ANALYSIS

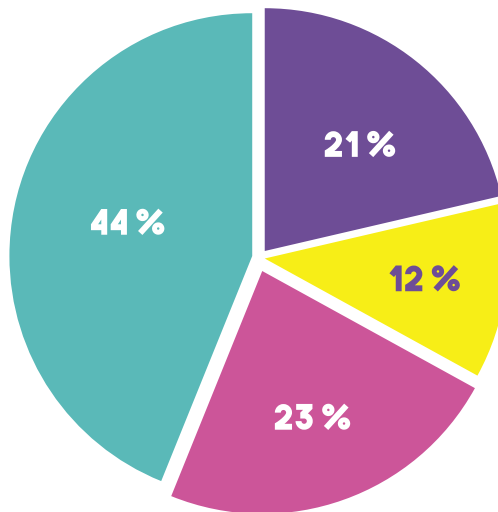


COMPANY PROFILES

For the purposes of this study, an **enterprise** is a Colombian enterprise: i) from the private sector or ii) from a mixed economy with a State share of less than 50%. To

answer the question: **What is the size of your company?** 44% of the respondents said that they were microenterprises, 23% were small enterprises and 12% and 21% reported medium and large enterprises, respectively, as shown in the following diagram:

GRAPH 1: SIZE OF THE COMPANIES



WHAT IS THE SIZE OF YOUR COMPANY?

- Large Enterprise (assets totaling over 15,000 CMMLW)
- Medium Enterprise (total assets 5,001 - 15,000 CMMLW)
- Small Enterprise (total assets 501 - 5,000 CMMLW)
- Micro Enterprise (total assets less than 501 CMMLW)

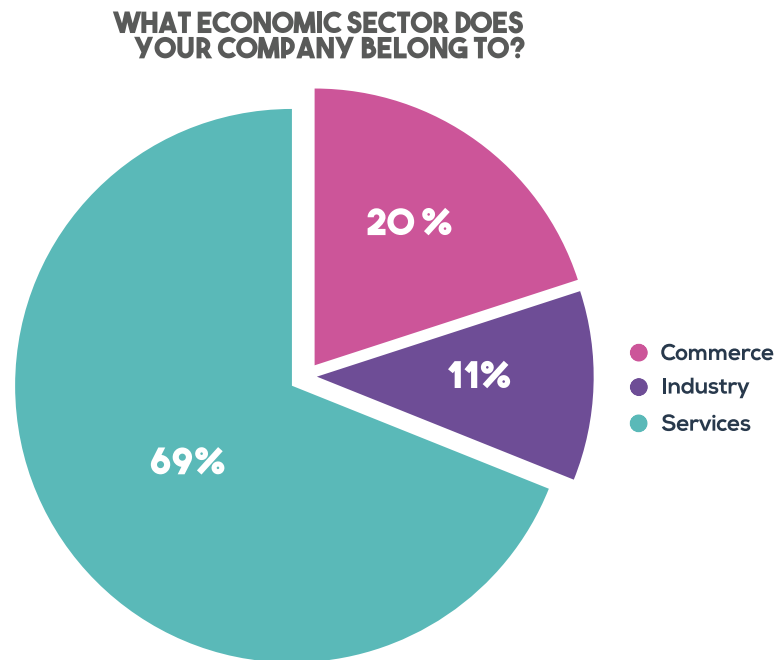
Number of Observations: 515

Note: CMMLW is the Current Minimum Monthly Legal Wage in force in Colombia

Among the companies, 84% reported that 100% were privately owned, while 16% were either i) publicly owned or ii) publicly and privately owned (mixed). Of the

enterprises interviewed, 69% belong to the service sector, which includes, for example, the financial sector, 20% to the commerce sector and 11% to the industry sector.

GRAPH 2: ECONOMIC SECTOR OF INTERVIEWEES



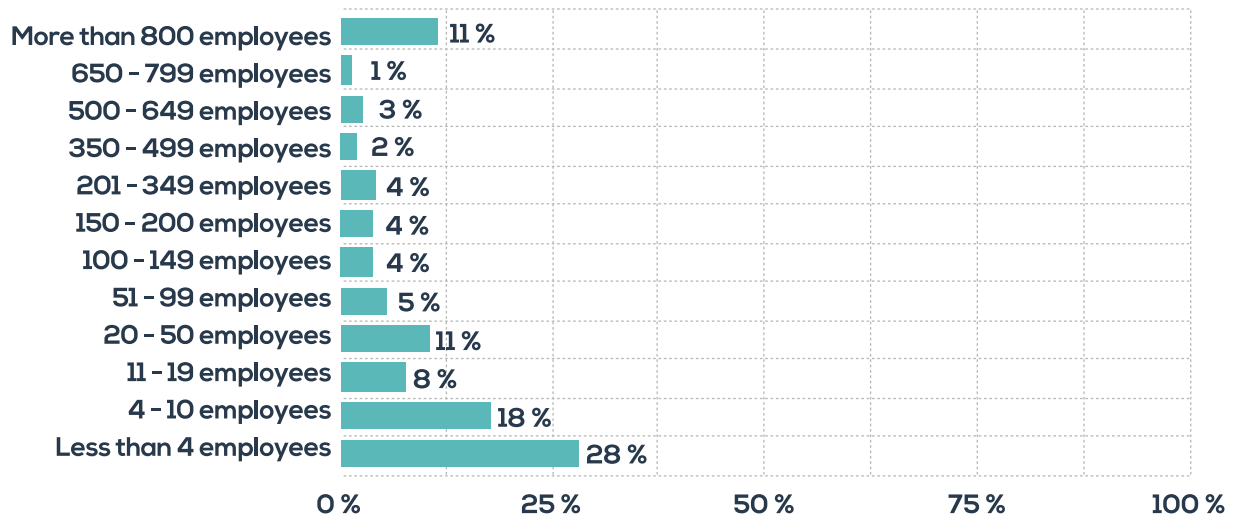
Number of Observations: 515

As for the number of companies according to size, 28% had less than 4 employees, 60% between 4 and 799 employees, and

11% of companies have more than 800 employees.

GRAPH 3: NUMBER OF EMPLOYEES IN THE COMPANIES

WHAT IS THE NUMBER OF EMPLOYEES IN YOUR COMPANY?



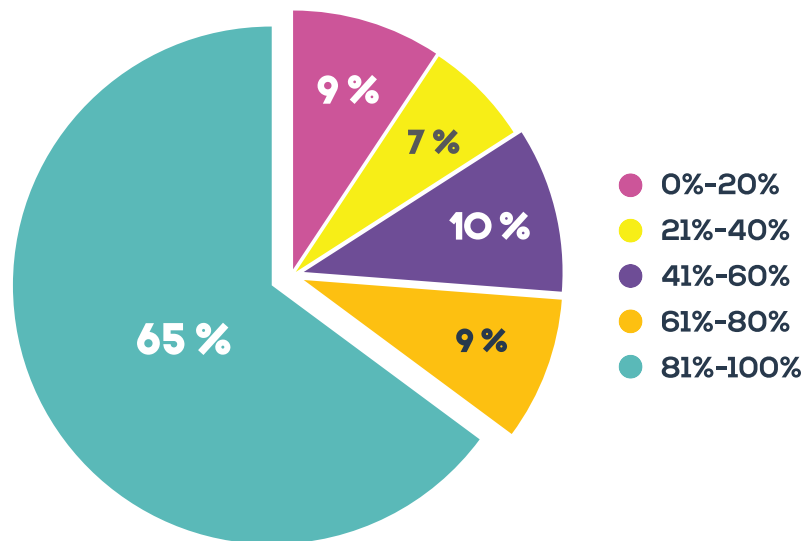
Number of Observations: 515

Regarding the companies that participated in this study, 65% reported that between 81% and 100% of their workforce had access to the Internet, 9% responded that

they gave access to 61% -80% of their employees and 26% provided between 0 and 60% of its employees.

GRAPH 4: APPROXIMATE PERCENTAGE OF YOUR COMPANY PERSONNEL WITH INTERNET ACCESS

WHAT APPROXIMATE PERCENTAGE OF YOUR COMPANY PERSONNEL HAS ACCESS TO THE INTERNET TO CONDUCT COMPANY ACTIVITIES?



Number of Observations: 515

When asking the question: Does the Company apply a “Bring Your Own Device” Policy? 40% of those interviewed reported that they had a BYOD policy compared to 60% which indicated that they did not.

In general, it can be concluded that the general profile of those participating in

this study are Microenterprises, with the majority of the service sector. However, it is important to note that 21% of respondents belong to large enterprises and 34% of those interviewed had a minimum of 99 employees or more.



DIGITAL SECURITY PRACTICES IN COMPANIES

As part of the study, a number of questions were asked regarding digital safety practices. These questions were asked to assess how their practices impacted the level of attacks experienced and the ultimate impact these practices may have on actual costs incurred as a result of an attack.

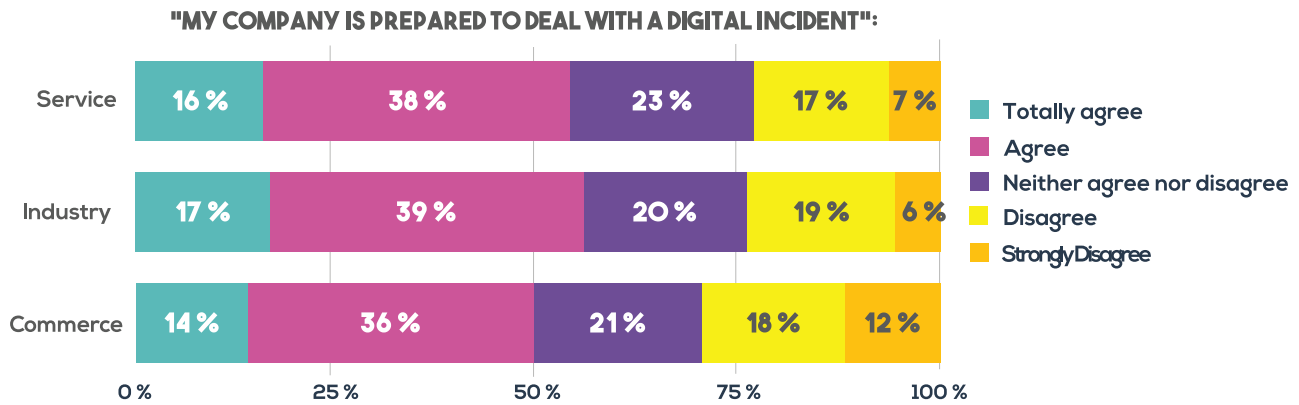
In response to the question: “My entity/ company is prepared to deal with a digital incident”, the data were analyzed taking into account both their sector and size. Among the sectors of service, industry and commerce, a simple average of 37% of respondents in all three sectors believe

they are prepared to handle a cyber incident.

Approximately 30% of respondents in the commerce sector considered that they were not prepared or were not fully prepared for a cyber incident.



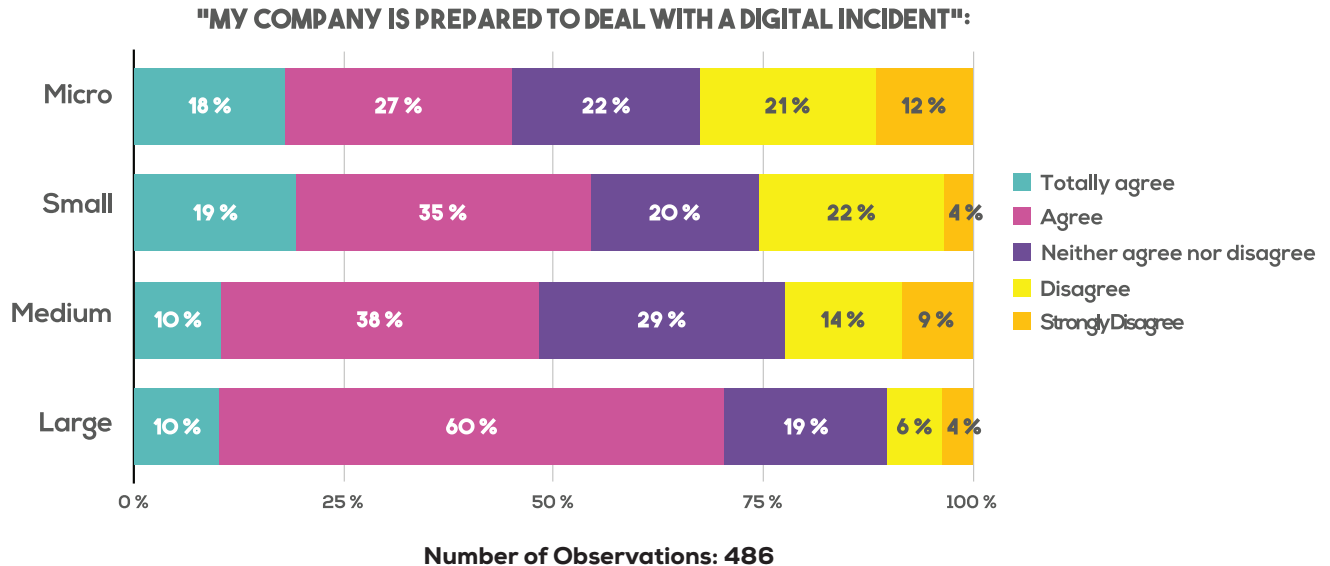
GRAPH 5: LEVEL OF READINESS TO DEAL WITH A DIGITAL INCIDENT (ECONOMIC SECTOR)



Number of Observations: 486

As for the size of these companies, 70% of large enterprises feel very prepared or prepared for a digital incident, compared to 45% of micro-enterprises. The results show that a simple average of about 22% of companies of all sizes replied that they "Neither agree nor disagree" with the statement "My company is prepared to deal with a digital incident".

GRAPH 6: LEVEL OF READINESS TO DEAL WITH A DIGITAL INCIDENT (COMPANY SIZE)

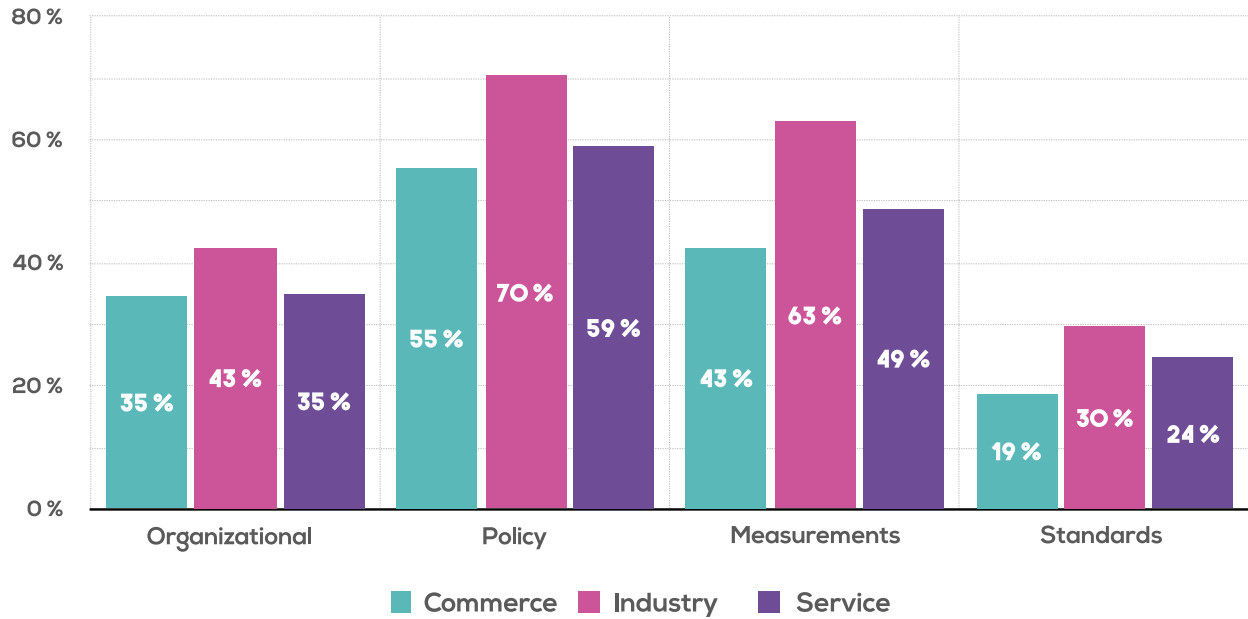


An important aspect of cybernetic readiness is the measures implemented, whether they are policies, technical measures or standards. In order to understand these examples, the following are listed below:

1. Organizational (e.g. area, department dedicated to digital security, head of information security, roles associated with information security, functions around information security)
2. Policy (e.g. system access policy, password update policy, awareness)
3. Technical measures (e.g. vulnerability testing, maintenance of IT infrastructure)
4. Standards (e.g. ISO 27001, other international standards)

In relation to this, respondents were asked: Which of the following practices in digital security (cybersecurity and/or information security) are implemented by your entity/ company? Among respondents from the three economic sectors, a majority responded that they had implemented policy measures (55% of the commerce sector, 70% of the industry sector and 59% of the service sector), with the implementation of technical standards (e.g. ISO 27001, other international standards), it being the next highest measure implemented (commerce 43%, industry 63% and service 49%).

GRAPH 7: DIGITAL SECURITY PRACTICES (ECONOMIC SECTOR)

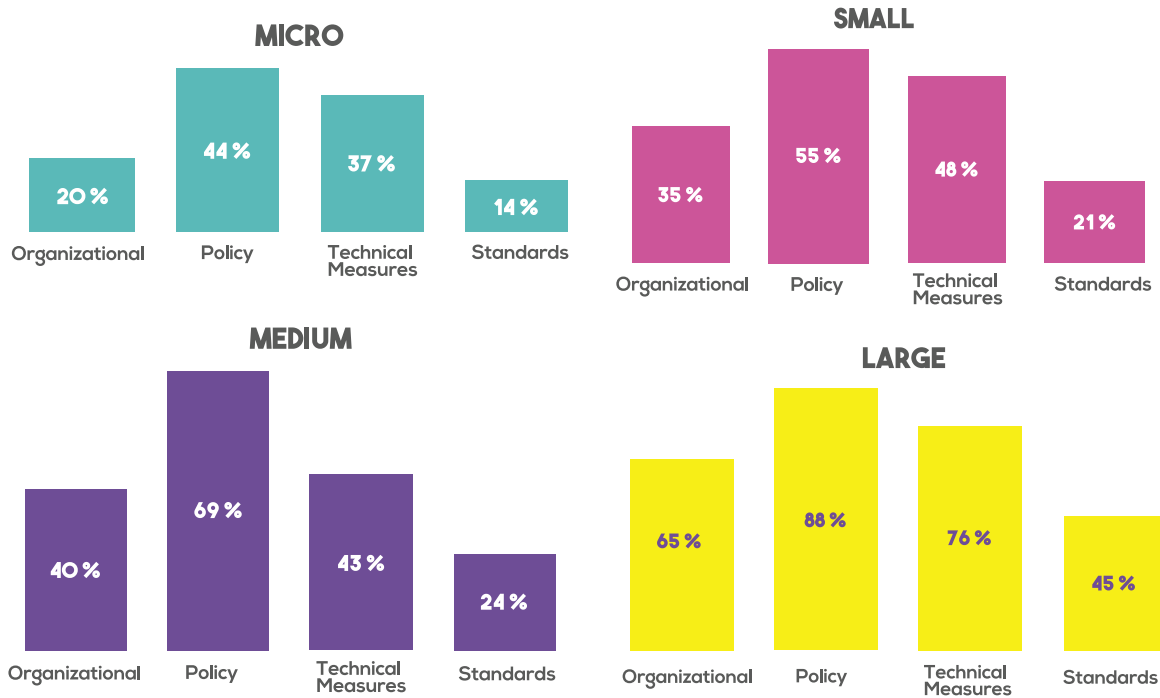


Number of Observations: 554

Compared by size, it is clear that the majority of respondents also placed greater weight on the implementation of policies as a digital security measure. Among micro-enterprises, 44% of them have implemented policies, 37% technical measures and 34% standards and organizational measures. Among the larger companies, an interesting observation was that 88% implemented policy measures, but only 45% of the companies participating

in this study mention that they adopted standards. Among all the interviewees, the implementation of organizational measures and standards was identified as the lowest priority practice. See the graphs below.

GRAPH 8: DIGITAL SECURITY PRACTICES (COMPANY SIZE)

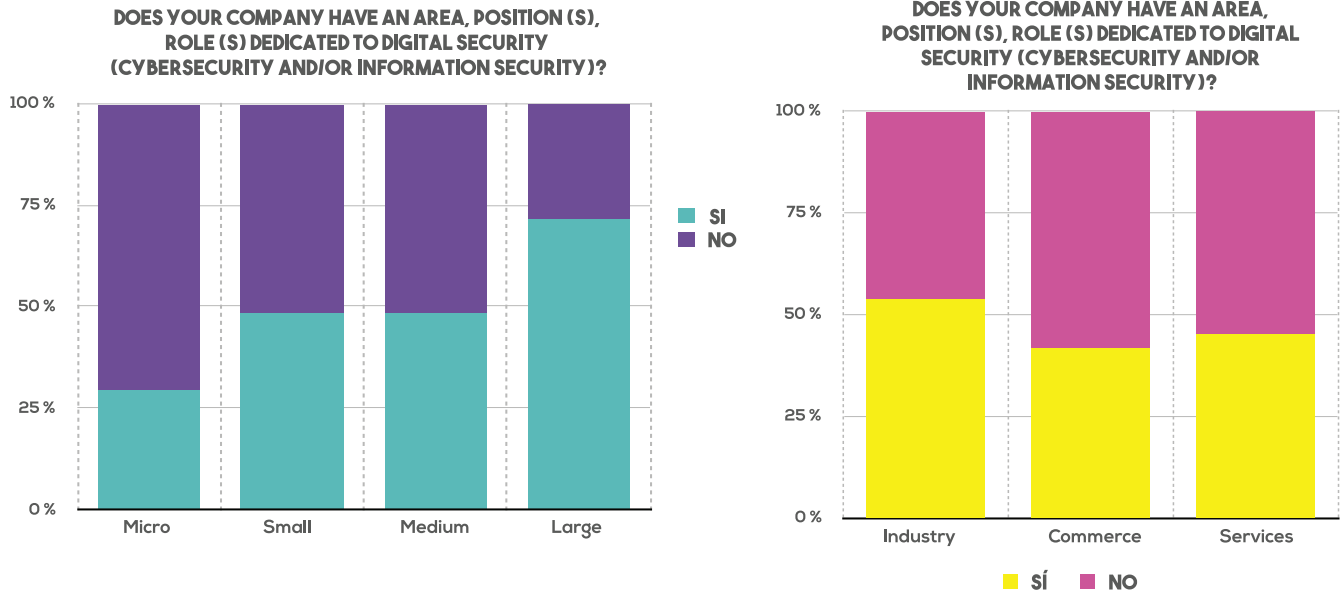


Number of Observations: 486

One of the most important steps to safeguard an organization against digital incidents is to identify a full-time position for the management of digital incidents. This position is important because it will help companies quickly detect, isolate and resolve incidents when and if they occur. If this position does not exist, attackers could remain in the organizations' system longer than necessary, making detection a longer process as well. Among all who answered the question: ***Does your entity/company have***

an area, position (s) or role (s) dedicated to digital security (cybersecurity and/or information security)? 70% of large enterprises replied 'yes' compared to a little over 20% of micro-enterprises. Among the economic sectors, most of the industry sector had a dedicated team, with a little over 54% responding positively to the question, compared to only 45% and 42% of the service and commerce sectors, respectively. See graphs by size and sector below:

GRAPH 9: POSITION (S) OR ROLE (S) DEDICATED TO DIGITAL SECURITY (COMPANIES' SIZE AND ECONOMIC SECTOR)



Number of Observations: 486

The above question can be compared to the following question: ***Under which of the following schemes does your entity/company manage security?*** Among respondents, 37% of micro, 58% of small, 64% of medium and 58% of large enterprises responded that digital security was managed under the IT department. Only 22% of micro, 18% of small, 7% of medium and 21% of large enterprises reported that it was managed under a digital security area.

In terms of sectors, approximately 83% of the Commerce sector reported that it was under the IT department, compared to 55% in the Industry sector and 47% in the Service sector, which responded in a similar way. What the answers might indicate is that most respondents see the need to address digital security issues and have placed them under the department most closely associated with digital security (i.e. Information Technology). However, this trend of reorienting information technology

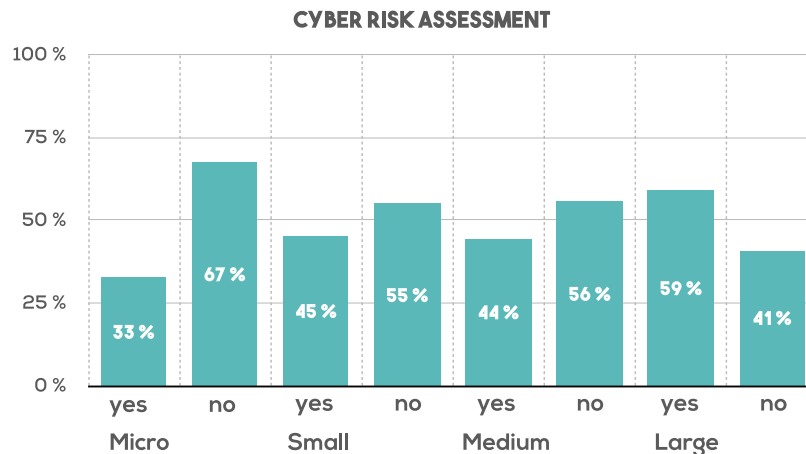
departments to handle digital security and incident response can, in the long run, lead to having a team of people without the skills to respond to more sophisticated incidents¹.

When the interviewees were asked, **How many people make up the team or area responsible for digital security (cybersecurity and/or information security) in their company?** 55% said they had 1-2 people dedicated, 27% answered 3-5 people and only 18% reported more than 5 people.

This further demonstrates that while companies have recognized the importance of addressing cyber incidents, they have not invested in the organizational areas of their companies to address this.

Finally, in relation to organizational practices, when asked whether their organization conducted digital security risk assessment, most respondents reported that they did not. This, in terms of business size, is broken down as follows:

GRAPH 10: CYBER RISK ASSESSMENT (SIZE OF ENTERPRISES)

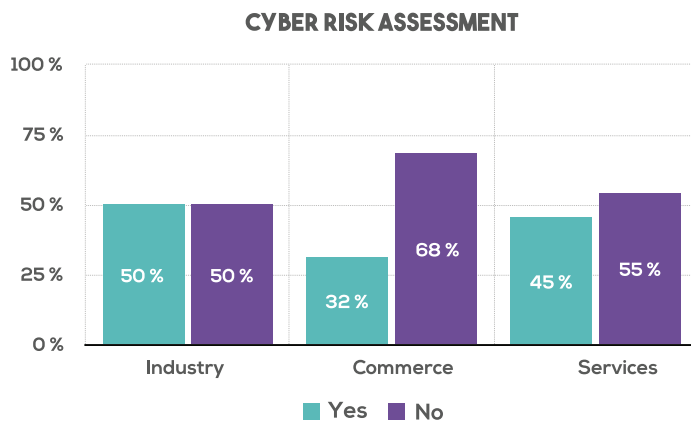


Number of Observations: 439

¹ Similar observations were made in the Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey, p. 5 Accessed at: <https://www.sans.org/reading-room/whitepapers/incident/incident-response-capabilities-2016-2016-incident-response-survey-37047> Last consulted on August 28, 2017

Regarding the economic sectors, 50% of respondents in the industry sector reported that they did not, compared to only 32% and 45% of the commerce and service sectors that did undertake a digital security risk assessment.

GRAPH 11: CYBER RISK ASSESSMENT (ECONOMIC SECTOR)



Number of Observations: 439

This result leads to significant observations since the purpose for conducting a risk assessment for any organization is to help it develop enforceable recommendations to improve safety and implement industry best practices. One of the best industry practices is the digital security framework

of the National Institute of Standards and Technology (NIST)², which emphasizes that the purpose of a risk assessment is for an organization to understand “the risk of digital security for organizational operations (including mission, functions, image or reputation), assets of the organization and individuals”. As established by NIST, conducting a risk assessment typically includes the following six steps:

1. Identify and document asset vulnerabilities.
2. Identify and document internal and external threats.
3. Acquire information about threats from and vulnerabilities to external sources.
4. Identify potential trade impacts and probabilities.
5. Determine business risk by reviewing threats, vulnerabilities, probabilities and impacts.
6. Identify and prioritize risk responses.

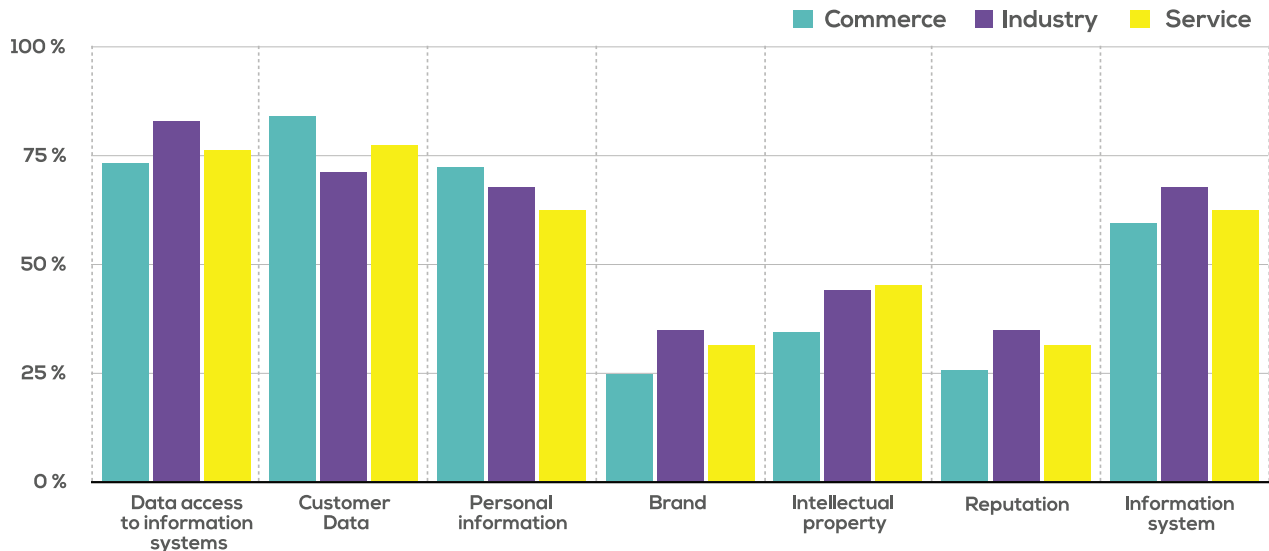
In this sense, it can be inferred that many of the respondents do not fully appreciate the value that best practices could award their commercial operations. For example, when asked: ***When protecting yourself from digital incidents, cyber threats and/or cyber-attacks, which of these data and/or information assets are prioritized by***

² NIST Cybersecurity Framework, Accessed at: <https://www.nist.gov/cyberframework>; Last access: August 29, 2017

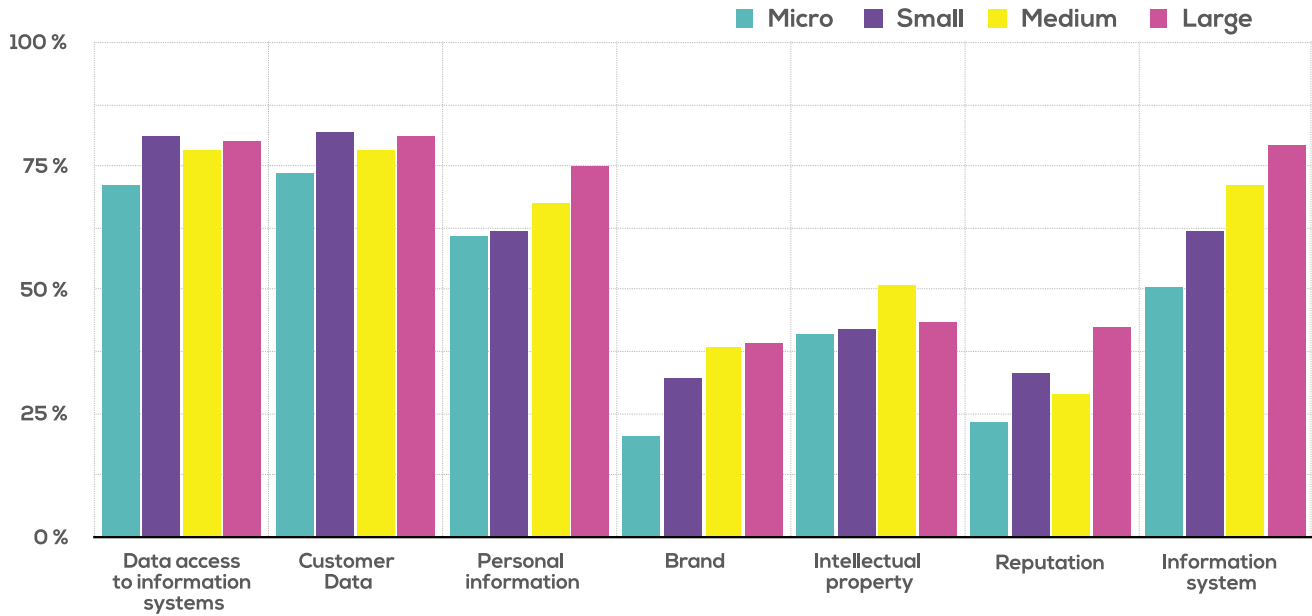
your entity/company? Please check the options that apply, almost all respondents across sectors and sizes reported that they would give priority to **Data access to information systems (e.g. passwords, tokens, credentials) and Customer data**. As for the economic sectors, companies of the three sectors (Commerce, Industry and Service) placed the lowest priority on **Brand, Intellectual Property/Industrial Secrets and Reputation**.

Interestingly, when data were compared by size of organizations, the results were almost exactly the same in terms of priority levels. This is significant since one of the best practices for digital risk management is for entities to be proactive rather than reactive and as such it is important to review threats, identify vulnerabilities and consequences and it is clear that most organizations see the data as a significant asset to protect. The following graphs show the summary of results by sector

GRAPH 12: DATA AND ASSETS PRIORITIZED BY THE COMPANY (2016)



In terms of analysis by size:



Number of Observations: 450

Therefore, when asked, on a scale of 1-5, what respondents believe to be the main factors that would affect their ability to address digital security, lack of dedicated staff and lack of budget were classified as the highest, with the lack of employee awareness immediately following. In this respect, it can be inferred that, while most

companies see the need to address digital security, dedicated human and financial resources are still not being prioritized.

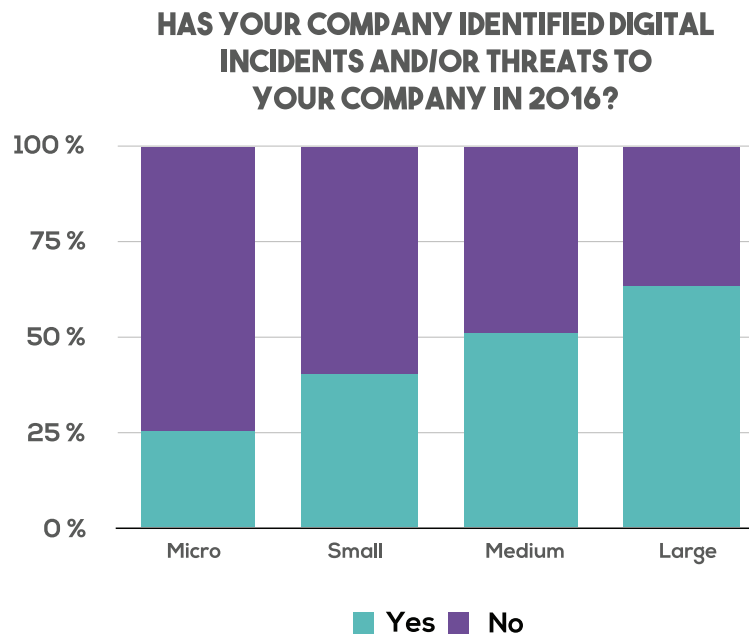




DIGITAL INCIDENTS IN COMPANIES

When asked whether digital incidents against their organization had been identified, more than 70% of micro-enterprises replied that they had not identified digital incidents. Among the small enterprises, approximately 60% also did not identify digital incidents. However, among medium and large enterprises, most companies replied that they did identify digital incidents: 51% and 63%, respectively.

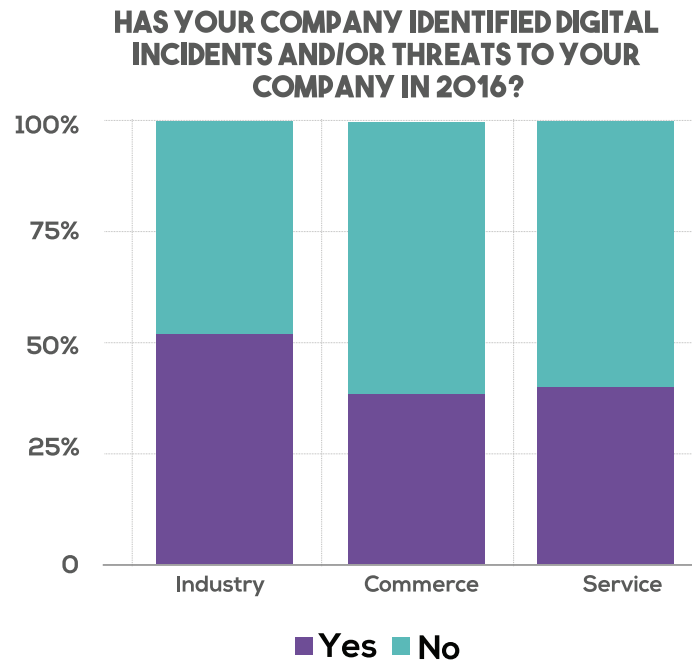
GRAPH 13: PERCENTAGE OF COMPANIES THAT IDENTIFIED DIGITAL INCIDENTS, ACCORDING TO COMPANY SIZE (2016)



Number of Observations: 451

When analyzing the different economic sectors, most of the companies—only in the industry sector—identified digital incidents: 52% of the enterprises. It is important to note that the majority of companies in the Industry sector, analyzed in this study, are large enterprises.

GRAPH 14: PERCENTAGE OF COMPANIES THAT IDENTIFIED DIGITAL INCIDENTS, BY ECONOMIC SECTOR (2016)



Number of Observations: 451

In order to understand why some companies identified digital incidents while others did not, an equation was estimated of determinants of the probability of a private sector company identifying digital incidents against its company, where the

dependent variable³ is "1" if the company identifies digital incidents and "0" if it does not identify them.

³ The dependent variable is 'dependent' on the values assumed by the independent variable

Within the explanatory variables⁴, a set of dichotomous variables⁵ was included, capturing specific factors of the companies, such as company size and the economic sector. That is, large, medium, small or micro, as well as whether the company belongs to the industry, commerce or service sector. Other dichotomous variables included: (i) whether the company implements digital security policies (e.g., system access policy, password update policy, awareness); (ii) whether the enterprise implements technical measures (e.g., vulnerability testing, maintenance of IT infrastructure); (iii) whether the company implements standards (e.g., ISO 27001, other international standards); (iv) if the company has an area, position (s) or role (s) dedicated to digital security; (v) if the company is aware of any regulations and/or national or territorial legislation requiring companies in its sector to implement digital security management practices; and (vi) if the company conducts any cyber risk assessment.

Other explanatory variables were also included, such as the number of employees in the company, the approximate percentage of company personnel with access to the Internet to carry out their

⁴ The explanatory variable, or independent, is that which explains the changes in the dependent variable.

⁵ The dichotomous or binary variable is that which has only two forms of presentation. It is a variable that can assume only two possible values, such as “yes” or “no”.

professional activities, the percentage of the company’s share capital that is foreign, the approximate value (in Colombian pesos) of the company sales during 2016, as well as the approximate budget value designated by the company for digital security matters.

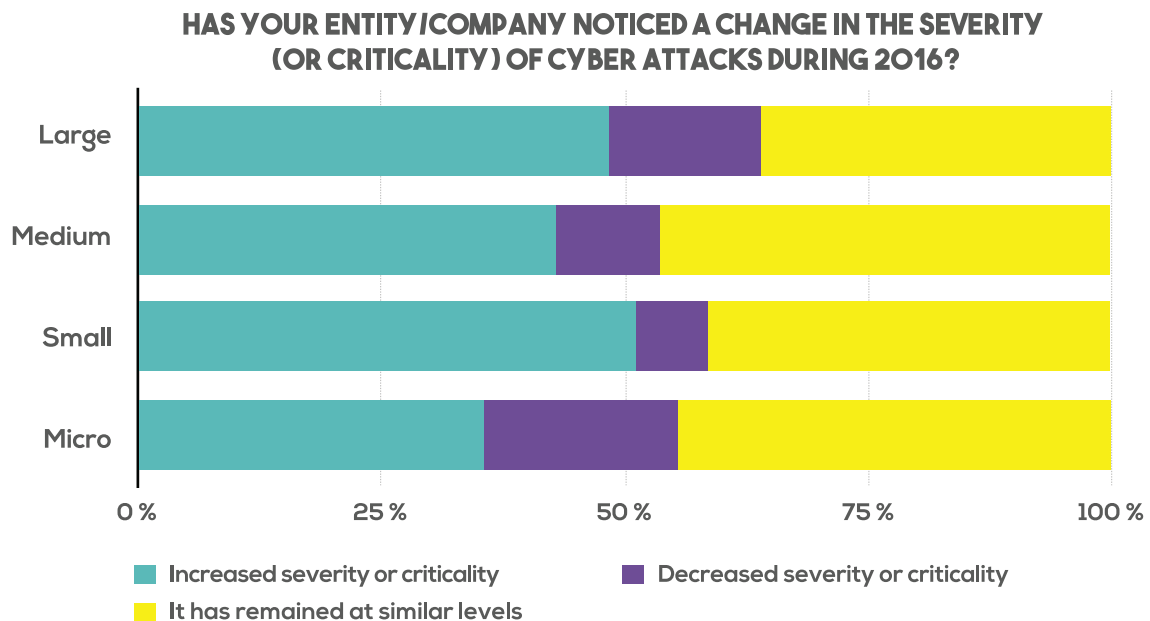
Given the binary nature of the dependent variable, a **logit**⁶ estimation model is used (Appendix 3). The results indicate that there is a statistically significant positive relationship between the implementation of technical measures—such as vulnerability testing and maintenance of the IT infrastructure—and the identification of digital incidents. This is also seen with the explanatory variable related to the practice of cybernetic risk assessment. More specifically, the results indicate that the probability that a company in Colombia identifies digital incidents increases for companies that implement technical security measures and that perform risk assessment. There is also a statistically significant positive relationship between incident identification and the number of employees in a company. On the other hand, the results indicate a statistically significant negative relationship between incident identification and microenterprises.

⁶ This model assumes that individual effects have been averaged, facilitating the calculation and interpretation of marginal effects, which in turn measure the effect of a change in one of the regressors on the dependent variable.

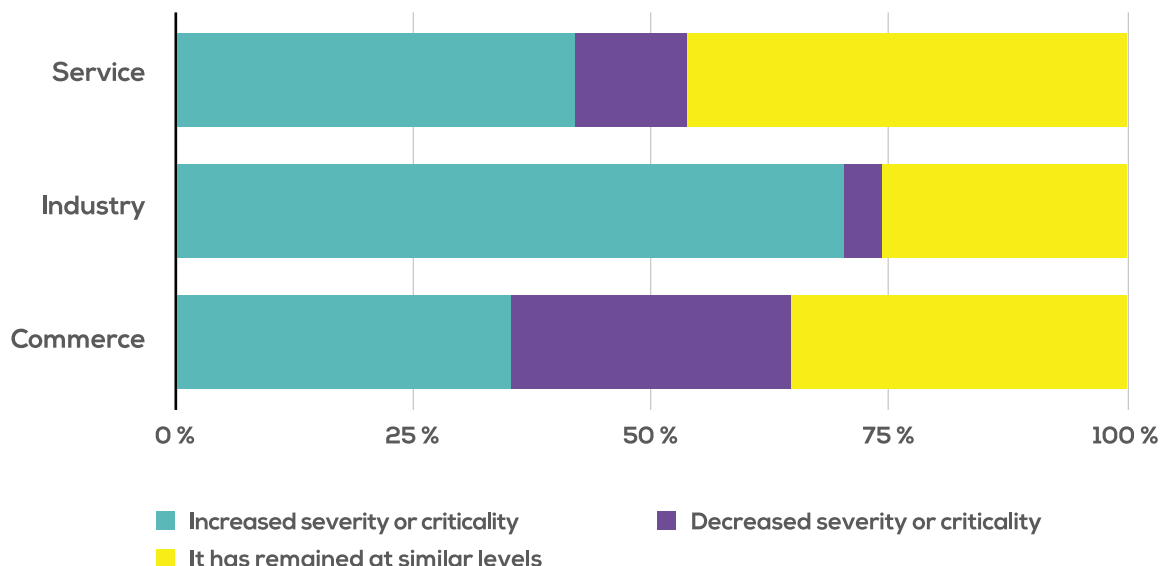
Having the ability to identify incidents is important for entities, since it is the first step to contain a malicious attack and to be able to respond. When asked: Has your entity/company noticed a change in the severity (or criticality) of cyberattacks during 2016? 70% of the Industry sector replied that they had noticed a change in the severity of the attacks compared

with the rest of the population. 35% of the commerce sector and 46% of the service sector reported that the levels of attacks remained the same. In terms of enterprise size, it was observed among the responses that a larger number of small enterprises responded having seen an increase in severity. See the comparative graphs below:

GRAPH 15: CHANGE IN THE SEVERITY OF DIGITAL INCIDENTS (2016)



HAS YOUR ENTITY/COMPANY NOTICED A CHANGE IN THE SEVERITY (OR CRITICALITY) OF CYBER ATTACKS DURING 2016?



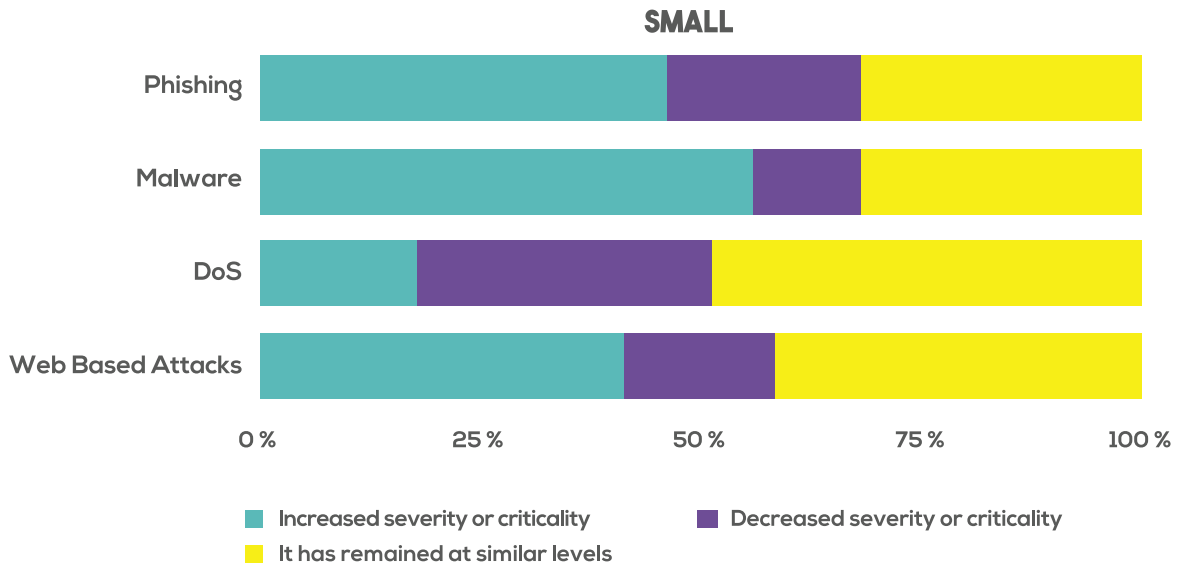
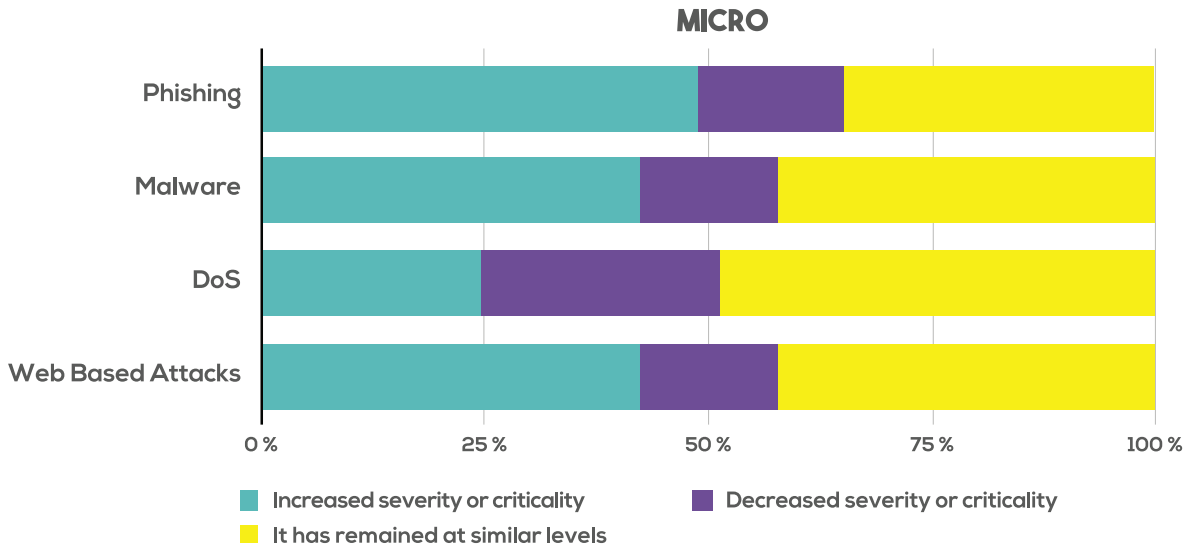
Number of Observations: 178

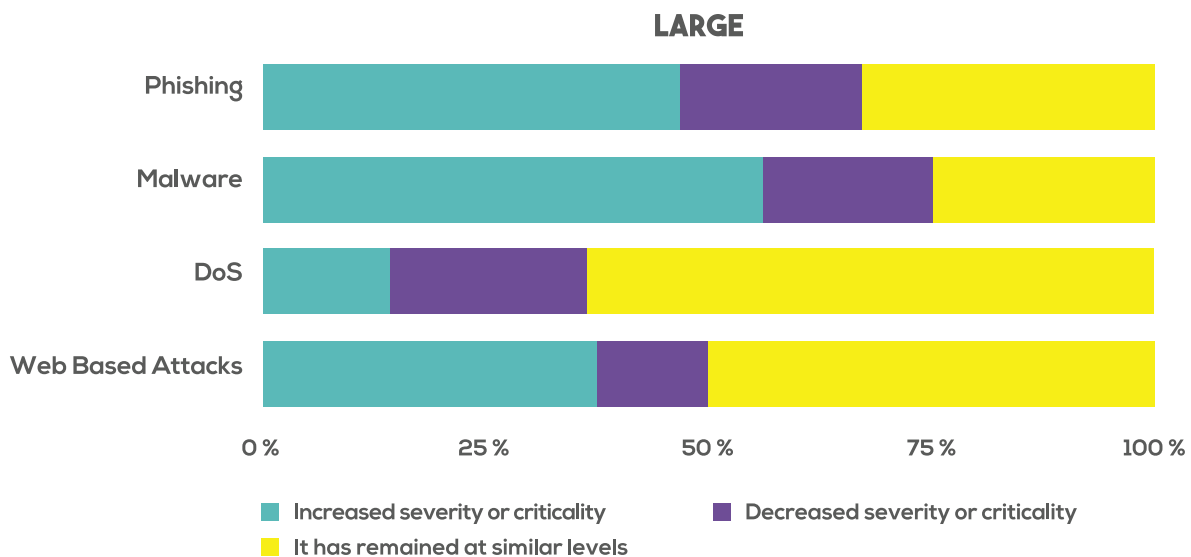
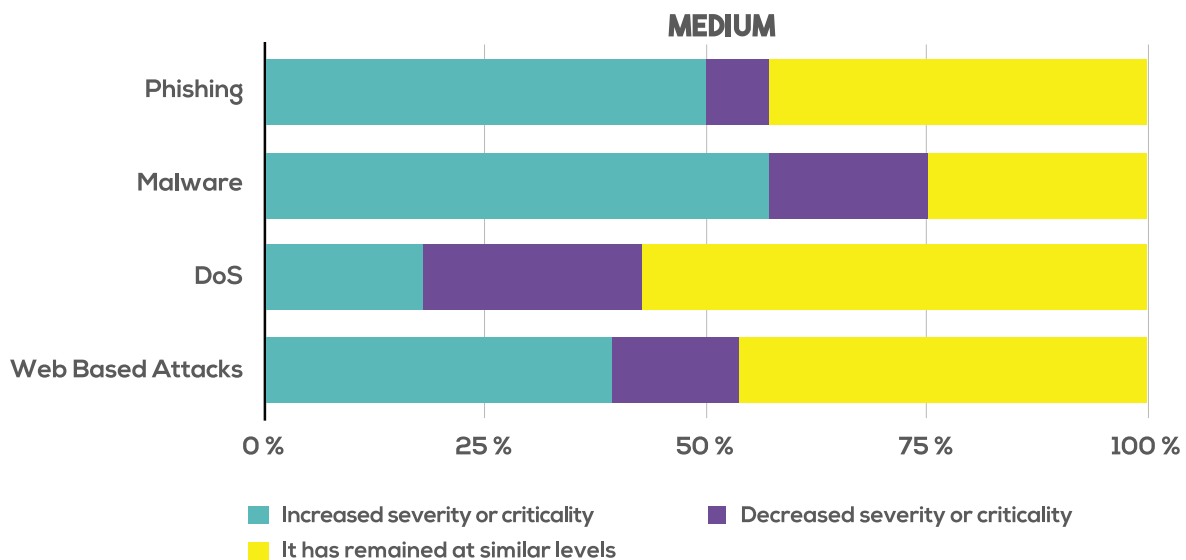
Regarding the types of incidents occurring, the study participants answered the question: ***What types of digital incidents, cyber threats or cyber-attacks has your entity/company identified during 2016?***, with malware and phishing being among the most common types of incidents. It was noted that within the Service sector, 50% of respondents noticed an increase in malware attacks, 47% phishing, 39% web-based attacks, and 18% denial of service attacks. In the Commerce sector, similar observations were made with 53% reporting an increase in malware, 41% reported an increase in phishing and 21% noticed an increase in both web-based

attacks and denial-of-service attacks. Interestingly, however, there were some variations within the industry sector in this observation, given 67% reported an increase in the severity of web-based attacks and malware and 59% reported an increase in phishing attacks.

In relation to the size of the reporting companies, the results were also similar in the response of micro, small, medium and large enterprises. See comparative graphs below:

GRAPH 16: GRAVITY OF DIGITAL INCIDENTS (2016)





Number of Observations: 178

When comparing these data with the Report of August 2017 of the Police Cyber Center (CCP, in Spanish) of Colombia, there has also been an annual increase in cyber reporting under **Reports, Law 1273-Cyber Crime in Colombia** issued for these purposes especially in relation to **Article 269E: Use of malware and Article 269G: Phishing of websites to capture personal data**. The March 2017 **Report: Cybercrime Threats in Colombia 2016-2017**, concluded that the level of information of the business sector increased from 5% to 28% in the number of reports received. The report revealed some interesting facts such as that **during 2016 there was a 114.4% increase in malware attacks in the**

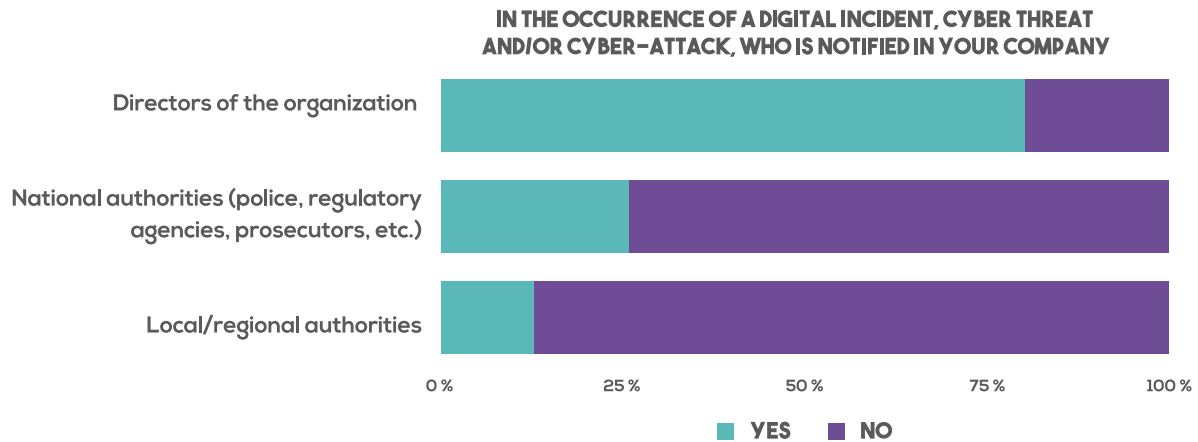
⁷ Report on Cybercrime Threats in Colombia 2016 - 2017, Accessed at <https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-ciber crimen-en-colombia-2016-2017>, Last entry: August 28, 2017

country, compared to 2015 (153 incidents reported in 2015, 328 incidents reported in 2016).

However, it is still necessary to increase the level of reports filed of digital incidents, such as when respondents were asked to respond: ***In the occurrence of a digital incident, cyber threat and/or cyber-attack, who is notified in your entity/company? Please check the options that apply***, 87% reported that they did not report digital incidents to a National Authority, compared to 80% who responded that they reported it to the organization directors.



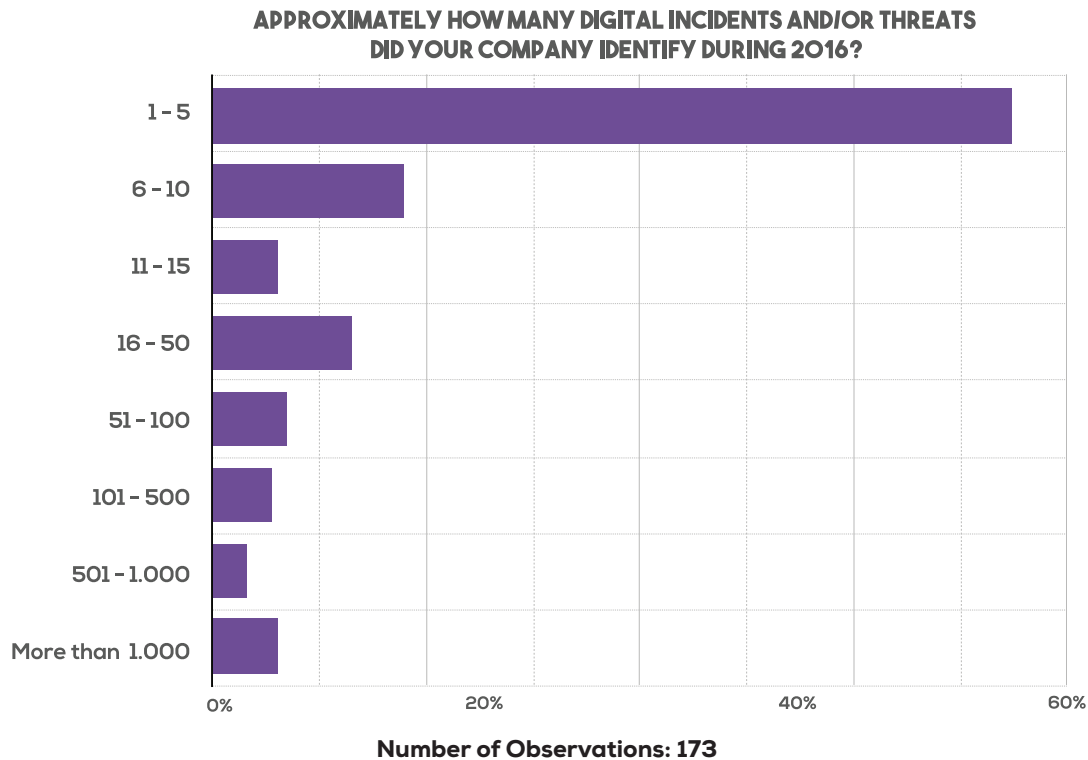
GRAPH 17: NOTICE OF DIGITAL INCIDENT (2016)



Number of Observations: 439

With respect to the number of digital incidents, it was observed that in 2016 more than 50% of the Colombian companies interviewed recorded between 1 and 5 digital incidents, and that approximately 30% between 6 and 100 digital incidents. Although the vast majority of companies are in the indicated ranges, it should be noted that 5% of the companies interviewed registered anomalous values of more than 1,000 digital incidents. In fact, in this group, there are companies that registered more than 100,000 digital incidents in 2016.

GRAPH 18: NUMBER OF DIGITAL INCIDENTS IDENTIFIED BY COMPANIES (2016)



Finally, a linear regression was performed where the logarithm of the number of digital incidents was the dependent variable (Appendix 3). The logarithm of the number of incidents was selected, in order to normalize the distribution of the variable. The following explanatory variables were included in the model: (i) company sales in 2016; (ii) the approximate budget amount designated by the company for digital security; (iii) the number of employees; (iv) the approximate percentage of staff

with access to the Internet to perform their professional activities; and (v) the percentage of the share capital of the company that is a foreign.

The model also has the following dichotomous variables: (i) if the company has an area, position (s) or role (s) dedicated to digital security; (ii) whether the enterprise implements technical security measures (e.g., vulnerability testing, maintenance of IT infrastructure); (iii) if the company adopts

digital security policies (e.g. system access policy, password update policy, awareness); (iv) whether the company implements standards (e.g., ISO 27001, other international standards); (v) if the company conducts any cyber risk assessment; and (vi) if the company is aware of any regulations and/or national or territorial legislation requiring companies in its sector to implement cyber risk management practices. In addition, the model has dichotomous variables that identify the economic sector to which the company belongs, such as industry, commerce and service, and company size.

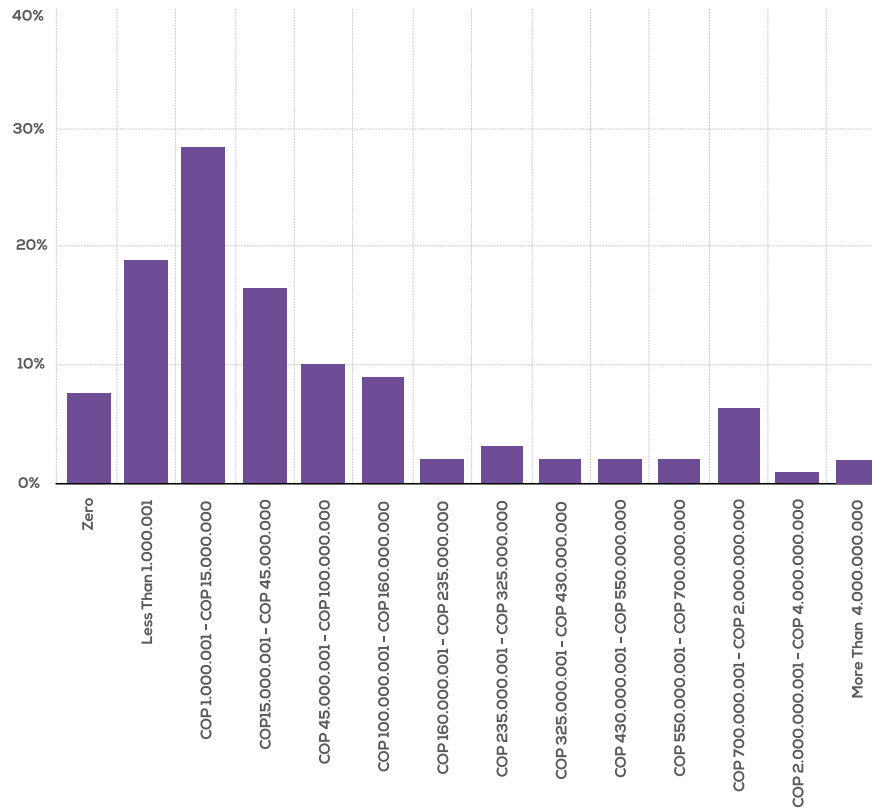
The results indicate that there is a positive and statistically significant relationship between the budget designated by the company for digital security and the number of incidents. With regard to digital safety practices, a significant and positive relationship was also observed between companies that implement technical safety measures, which perform risk assessment and adopt standards. That is, companies that implement more digital security measures tend to identify a larger number of digital incidents. This means that many companies that do not implement these measures have no knowledge that they are targets of cyber-attacks.



DIGITAL SECURITY BUDGET IN COMPANIES

It is interesting to note that the vast majority of companies that did allocate IT budget also allocated digital security budget issues: about 92% of companies that allocate IT budget also assign to digital security. Centering on the companies that allocate IT budget, the amount allocated by the companies to digital security in 2016 was verified, as indicated in Graph 19:

GRAPH 19: ANNUAL DIGITAL SECURITY BUDGET OF COMPANIES THAT ALLOCATE RESOURCES FOR IT (2016)



Number of Observations: 250

The distribution of the budget is biased to the right, so it was preferred to work with the median of the digital security budget in 2016 considering company size as well as its economic sector. It is important to note that Table 1 presents the digital security budget that is in the middle of the values provided by the companies. It should also be noted that 8% of these companies did not allocate any budget to digital security, while companies in some sectors, particularly the financial sector, invested more than COP 6,000,000,000 in digital security in 2016.

TABLE 1: MEDIAN OF THE ANNUAL DIGITAL SECURITY BY ENTERPRISE THAT ASSIGNS RESOURCES FOR IT

	COP (\$)		COP (\$)
Micro	500,000 - 1 million	Commerce	5 - 10 million
Small	5 - 10 million	Industry	45 - 60 million
Medium	15 - 25 million	Service	5-10 million
Large	120 - 140 million		

Number of Observations: 250

When analyzing the amounts allocated by the Colombian companies that assigned some budget to digital security, it was observed that the median of the digital security budget in relation to company sales was approximately 0.3% of sales in 2016. That is, when the budget was allocated to digital security, this budget did not reach 1% of the company's sales in 2016.

In addition, it was verified that, on simple average, most of the budget was allocated to platforms and technological means, while capacity generation received the least amount of resources.

Approximately 47% of the digital security budget was allocated to electronic media and platforms, and 11% to capacity building which, in turn, included topics such as training and awareness raising. It is interesting to note that the chapter on digital security practices in companies showed that the lack of awareness and knowledge on the part of the employees was among the failings that most affected the capacity of companies in the field of digital security in 2016.

TABLE 2: BUDGET ALLOCATION FOR DIGITAL SECURITY ISSUES (2016)

CATEGORIES	PERCENTAGE
Human Resources (e.g. employees, contractors)	25%
Platforms and Technological Media (e.g. hardware, software)	47%
Capacity Generation (e.g. training, awareness raising, research)	11%
Specialized Services (e.g. security management, outsourcing, support)	17%

Number of Observations: 230

Finally, a linear regression was performed with the objective of identifying the factors that drive a company to invest more in digital security. In this regression, the logarithm of the budget allocated by companies for digital security issues during 2016 was used as the dependent variable (Appendix 3). The logarithm of the digital security budget was selected, with a view to normalizing the distribution of the variable. In addition, the following independent variables were included: (i) the number of employees

of the company; (ii) the approximate percentage of company personnel with access to the Internet to carry out their professional activities; (iii) the logarithm of the company sales; (iv) the percentage of the share capital of the company that is a foreign; and (v) the logarithm of the number of digital incidents suffered by the company in 2016.

The model also has dichotomous variables that identify the economic sector to which the company belongs, such as Industry, Commerce and Service, and company size. The following dichotomous variables are also included: (i) if the company has an area, position (s) or role (s) dedicated to digital security; (ii) whether the enterprise implements technical security measures (e.g., vulnerability testing, maintenance of IT infrastructure); (iii) if the company adopts digital security policies (e.g. system access policy, password update policy, awareness); (iv) whether the company implements standards (e.g., ISO 27001, other international standards); (v) if the company conducts any cyber risk assessment; and (vi) if the company is aware of any regulations and/or national or territorial legislation requiring companies in its sector to implement cyber risk management practices.

The results indicate that there is a positive and statistically significant relationship between the number of employees, company sales and digital security budget. In other words, **the greater the number of employees and company sales, the larger the budget allocated to digital security.**

With respect to digital security practices, a significant and positive relationship between the digital security budget and the following dichotomous variables was also verified: existence of a position or

role dedicated to digital security, technical measures, digital security policies, standards, and risk assessment. In other words, companies implementing these digital security practices assign a larger digital security budget than companies that do not adopt these practices. Finally, the negatively significant relationship between microenterprises and the digital security budget should be noted. In other words, **microenterprises have the smallest digital security budgets in absolute terms.** On the other hand, **companies in the service sector (mainly in the financial sector) tend to allocate a larger budget to digital security.**

It is important to keep in mind that the digital security budget is a cost for digital incident prevention. That is, they are the resources used to cover the costs incurred in digital security practices. In the next section, the costs incurred as a result of a digital incident will be analyzed.



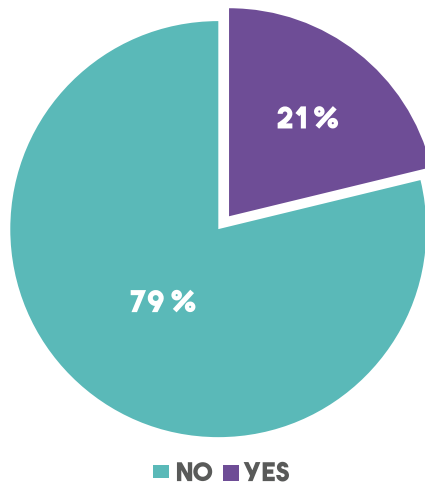


COST OF DIGITAL INCIDENTS FOR COMPANIES

When companies were asked about the estimation of the costs derived from the negative consequences caused by the occurrence of digital incidents, 79% of the companies stated that they had no estimates, as shown in Graph 20 below:

GRAPH 20: COMPANIES THAT ESTIMATED THE NEGATIVE CONSEQUENCES OF DIGITAL INCIDENTS (2016)

Has your company estimated the costs resulting from the negative consequences of the occurrence of digital incidents, cyber threats and/or cyber-attacks?



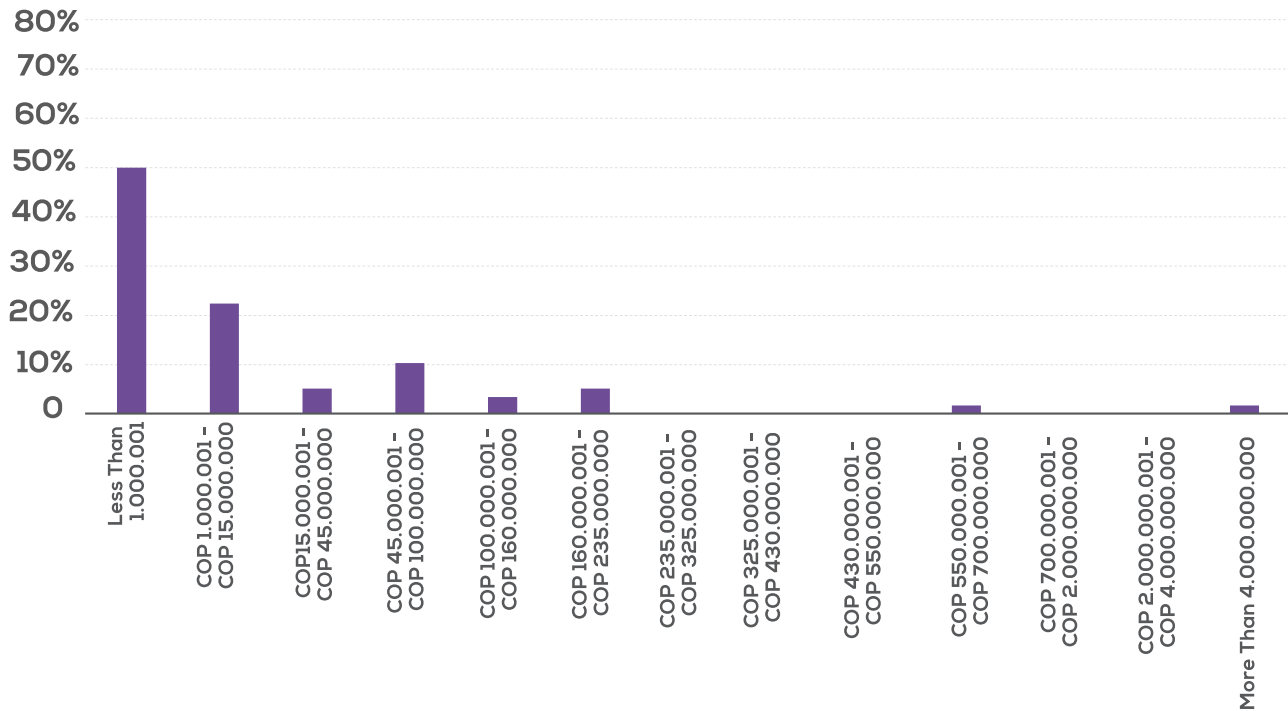
Number of Observations: 429

Taking into account the companies that estimated the costs incurred as a result of the digital incidents, the graphs below present the distribution of costs with the number of digital incidents incurred by the companies according to five cost categories: (i) disruption of normal company operations; (ii) damage to assets and infrastructure; (iii) penalties, fines and legal expenses; (iv) damage to the reputation and image of the market; and (v) loss of intellectual property or other commercially sensitive business information.

In contrast to the costs of preventing digital incidents described in the section on digital security budgeting, these five categories refer to cost estimation as a consequence of a digital incident. For example, a digital incident can lead to disruption of product production or the provision of a company service, affecting its regular activities. A digital incident can also result in theft of company data, such as commercially sensitive data and intellectual property. Some incidents seek to attack the technological infrastructure of companies and cause damage to their network and systems. Likewise, a digital incident can generate legal expenses, such as regulatory fines and compensation to customers. The aim was also to include costs to the reputation of the company, which can result in the loss of confidence of customers and, as ultimately, affect sales.

GRAPH 21: COSTS OF OPERATION DISRUPTION INCURRED BY COMPANIES THAT ESTIMATED THE IMPACT OF DIGITAL INCIDENTS (2016)

DISRUPTION OF OPERATIONS

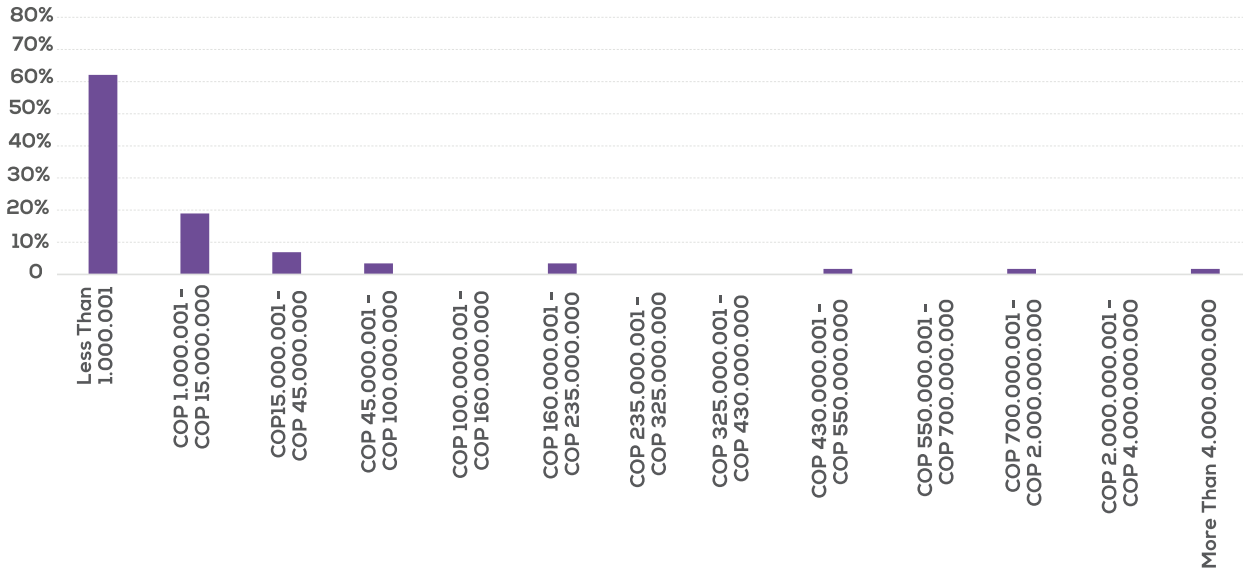


Number of Observations: 58

With respect to the cost of disruption of normal company operations, 50% of the companies incurred in costs of less than COP 1,000,001, 22% incurred in costs between COP 1,000,001 - COP 15,000,000, and approximately 25% between COP 15,000,001 - COP 235,000,000. A few companies have extreme values that move away from the dataset, with more than COP 4,000,000,000. Companies with extreme values are all large enterprises.

GRAPH 22: COSTS OF DAMAGE TO ASSETS AND INFRASTRUCTURE INCURRED BY COMPANIES THAT ESTIMATED THE IMPACT OF DIGITAL INCIDENTS (2016)

DAMAGE TO ASSETS AND INFRASTRUCTURE



Number of Observations: 58

With respect to damage to company assets and infrastructure, more than 60% of the companies incurred in costs of less than COP 1,000,001, approximately 20% incurred in costs between COP 1,000,001 - COP 15,000,000, and approximately 15% between COP 15,000,001 - COP 235,000,000. About 5% of companies presented extreme values that are far from the data set, with more than COP 4,000,000,000. In addition, companies with extreme values are all large enterprises.

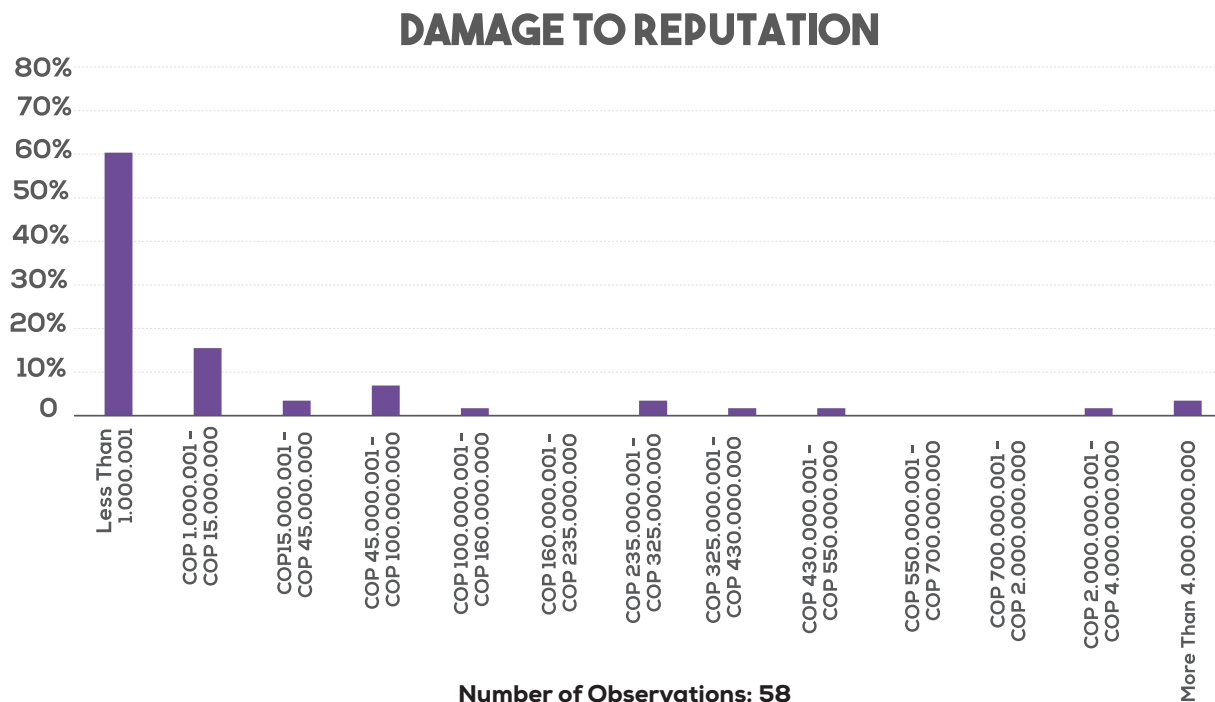
GRAPH 23: COSTS OF PENALTIES, FINES AND LEGAL EXPENSES INCURRED BY COMPANIES THAT ESTIMATED THE IMPACT OF DIGITAL INCIDENTS (2016)



Number of Observations: 58

With respect to penalties, fines and legal expenses, more than 75% of the companies incurred in costs of less than COP 1,000,001, approximately 12% incurred in costs between COP 1,000,001 - COP 15,000,000, and approximately 10% between COP 15,000,001 - COP 235,000,000. About 3% of the companies presented extreme values that are far from the data set, with more than 4 billion Colombian pesos. It should be noted that companies with extreme values were all large enterprises.

GRAPH 24: COSTS OF REPUTATIONAL DAMAGE INCURRED BY COMPANIES THAT ESTIMATED THE IMPACT OF DIGITAL INCIDENTS (2016)

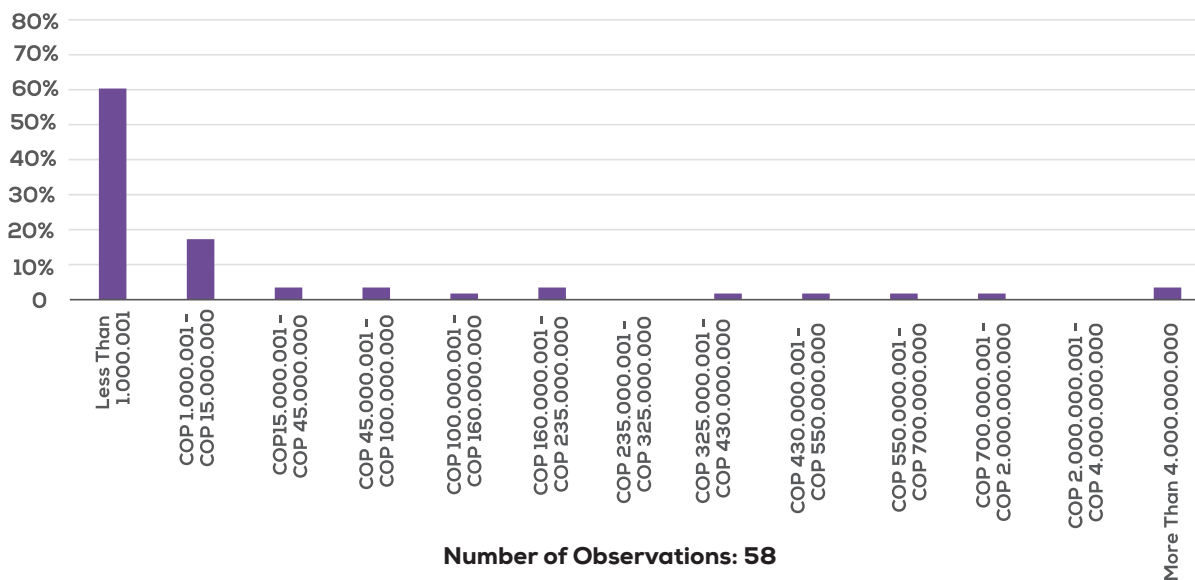


With respect to reputational damage, 60% of the companies incurred in costs of less than COP 1,000,001, approximately 16% incurred in costs between COP 1,000,001 - COP 15,000,000, and approximately 12% between COP 15,000,001 - COP 235,000,000. It is important to note that of the companies that participated in this study, there was a larger number of companies with reputational costs of more

than 325 million Colombian pesos, which corresponds to approximately 12%; while 5% reported presenting reputational damages of more than COP 2,000,000,000. In the latter group, the majority consisted of large enterprises, including firms in the commerce, communications and financial sectors.

GRAPH 25: COSTS OF INTELLECTUAL PROPERTY LOSSES INCURRED BY COMPANIES THAT ESTIMATED THE IMPACT OF DIGITAL INCIDENTS (2016)

LOSS OF INTELLECTUAL PROPERTY



Finally, with respect to the loss of intellectual property, 60% of the companies incurred in costs of less than COP 1,000,001, approximately 17% incurred in costs between COP 1,000,001 - COP 15,000,000, and approximately 12% between COP 15,000,001 - COP 235,000,000. It is interesting to note that there is a larger number of companies with costs related to the loss of intellectual property above COP 325 million: about 10% of companies, with 3% having intellectual property losses of more than COP 4,000,000,000. In the latter group, the majority consisted of

large enterprises, including firms in the Commerce and the financial sector.

It can be noted that the cost distribution among the five categories was biased towards the right, so the aim was to work with the median of the grouped cost incurred by each company, according to company size. That is, Table 3 presents the cost of digital incidents that are in the middle of the values provided by each company that estimated the impact of digital incidents.

TABLE 3: TOTAL MEDIAN COST PER COMPANY THAT ESTIMATED THE IMPACT OF DIGITAL INCIDENTS (2016)

COMPANY SIZE	COP (\$)
Micro	1.5 – 6 million
Small and Medium	10 – 20 million
Large	20 – 45 million

Number of Observations: 58

Table 4 shows the relative cost of digital incidents by sales for 2016, incurred per company according to company size. In other words, the percentage of the cost of digital incidents in relation to the sales of the company.

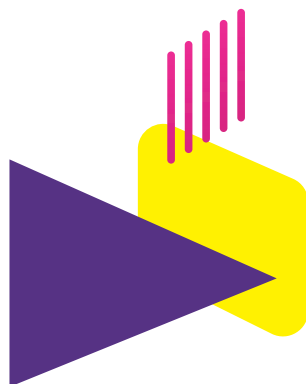


TABLE 4: TOTAL COST PER COMPANY SALES (2016)

COMPANY SIZE	(%)
Micro	1% – 5%
Small and Medium	0.5% – 1%
Large	0,005% – 0,015%

Number of Observations: 58

It can be observed that the relative cost of digital incidents decreased as companies increased in size. However, large enterprises incurred in absolute costs with digital incidents much higher than the costs incurred by a microenterprise, for example, the relative cost per digital incident of a large company was significantly smaller.

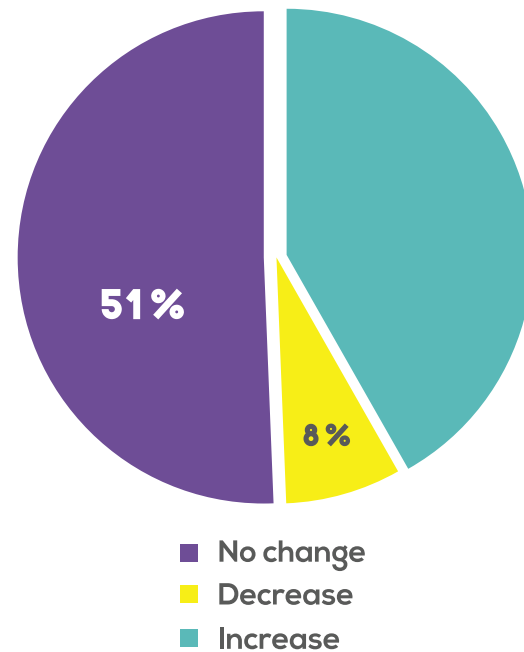
It should be noted that few companies in the Industry and Commerce sector provided information about their costs. In relation to the Service sector—which, in turn, had a more significant number of responses—it was observed that the median of its costs is between COP 5,000,000 and COP 11,000,000, with a relative cost of approximately 0.5% of sales.

Finally, the cost was estimated in relation to the number of digital incidents. A linear regression was performed where the cost of digital incidents in 2016 was the dependent variable and the number of incidents was the explanatory variable. The results indicate that there is a significant and positive relationship between cost and number of incidents. According to the model, **it is estimated that the increase of one unit in the number of incidents increases the cost incurred by companies in Colombia by approximately 500,000 Colombian pesos as a result of digital incidents.** It is important to keep in mind that this value is an estimate and that some incidents may have lower values, while others, higher.

Finally, the aim was to analyze how the cost incurred due to digital incidents in 2016 impacted the investments of companies in research, development and innovation (R&D&I), given the importance of R&D&I for the development of a digital economy, as well as for the advancement of digital security measures. As shown in Graph 26 below, 42% of the companies interviewed said that they have increased investments in R&D&I.

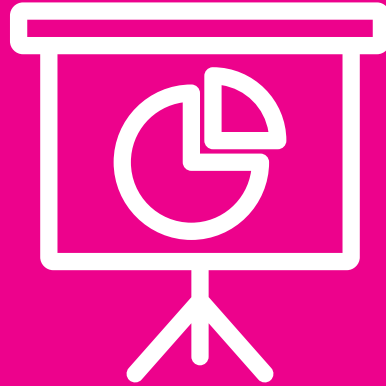
GRAPH 26: INVESTMENT IN R&D&I

How did your company's investments in research, development and innovation (R&D&I) change as a result of the digital incidents suffered?



Number of Observations: 58

Among the companies that claimed that their R&D&I investments increased as a result of digital incidents, 36% of these companies responded that their investments increased by more than 15% in 2016. It is noteworthy that awareness of the impact digital incidents in companies is driving them to invest more in R&D&I.



PART 2

ANALYSIS OF PUBLIC SECTOR ENTITIES

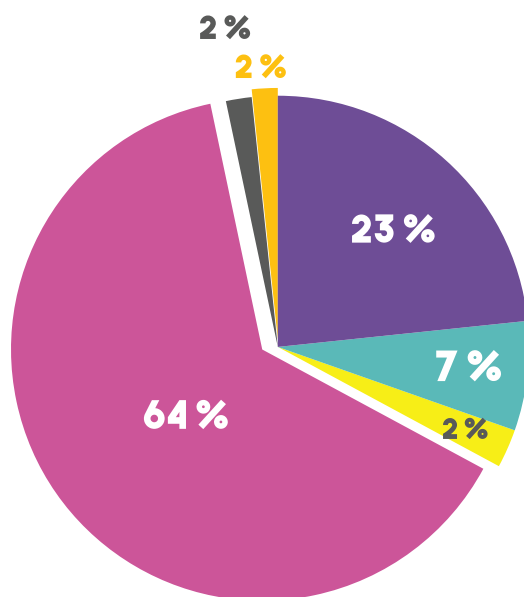


PROFILE OF THE ENTITIES

In relation to Colombian public entities, 64% of the respondents were from the Executive Branch, while 23% were Autonomous Entities. The other interviewees who constituted the other 13% were from the Electoral Body, the Judicial and Legislative Branch, and Control and Surveillance Agencies.

Of the public sector entities, 52% of respondents belonged to the Territorial-Municipal level, compared to a total of 36% of the responses being national entities and 12% of Territorial-Province level.

GRAPH 27: PUBLIC POWER BRANCH OF WHICH THE ENTITY IS PART

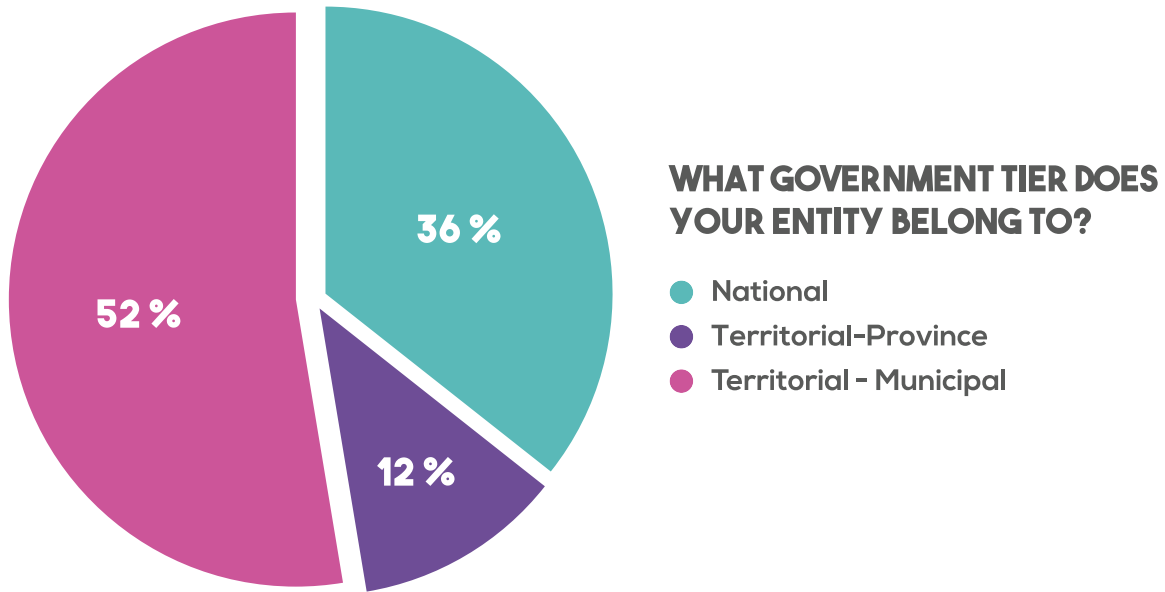


WHICH PUBLIC POWER BRANCH IS YOUR ENTITY PART OF?

- Autonomous entities
- Control and monitoring body
- Electoral body
- Executive branch
- Judicial branch
- Legislative branch

Number of Observations: 724

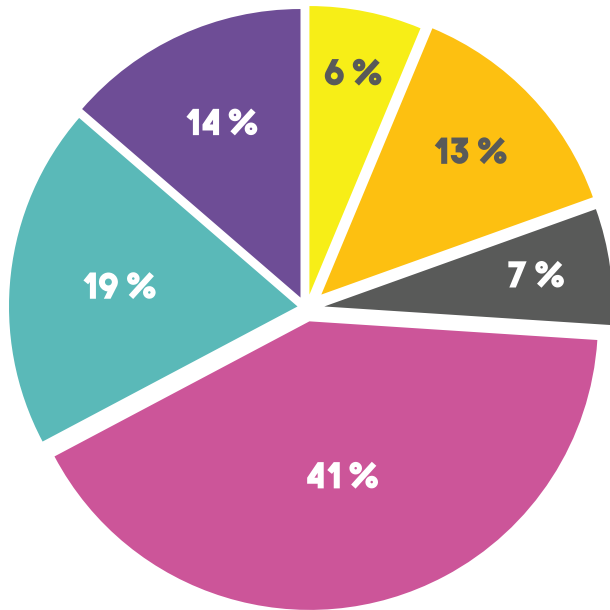
GRAPH 28: GOVERNMENT TIER OF THE ENTITY



Number of Observations: 724

As for the regional distribution of the interviewees at the territorial level (i.e. province or municipal), 41% were from the Central Region, 19% from the Eastern Region, 14% from the Pacific Region, 13% from the Atlantic Region, 7% from Bogota and the remaining 6% from the Region of the Former National Territories.

GRAPH 29: REGION WHERE THE ENTITY IS LOCATED



IF THE ENTITY IS A TERRITORIAL TIER, IN WHICH REGION IS THE ENTITY LOCATED?

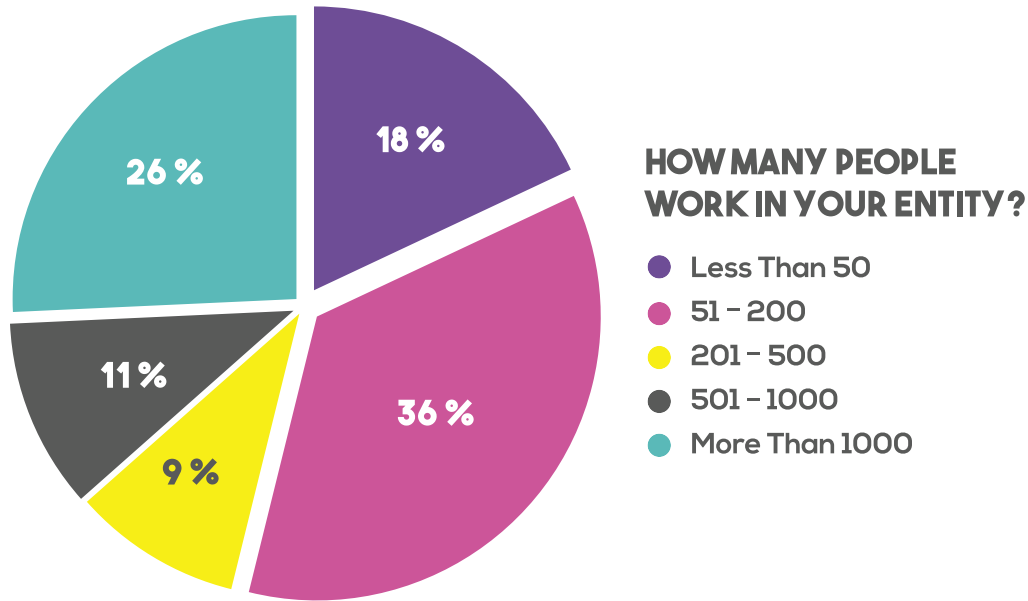
- Ancient National Territories
- Atlantic area
- Bogota
- Central
- Eastern zone
- Pacific Area

Number of Observations: 461

Public Sector entities varied in a fair range for the purposes of this study in terms of small and large entities. When answering the question: *How many people work in your organization? (Select only one response)*, 18% reported that they had

fewer than 50 employees, 36% reported that they had 51-200 employees, 9% had 201-500 employees and 11% had 501-1000 employees. The other significant response was that 26% of respondents reported that they had more than 1,000 employees.

GRAPH 30: NUMBER OF PEOPLE WORKING IN THE ENTITIES



Number of Observations: 583

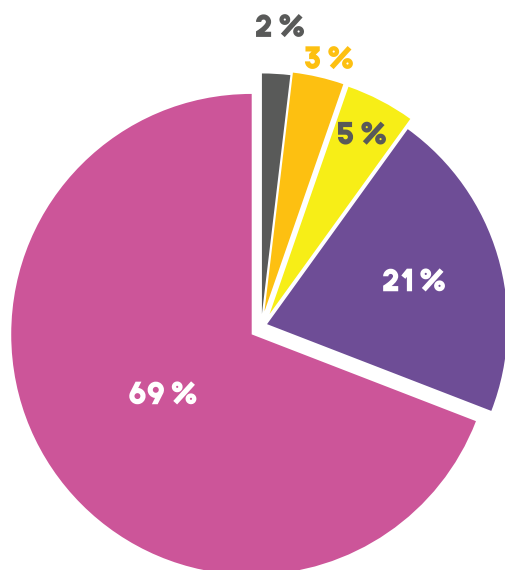
In light of the previous results, the profile of the state entity respondents could be described mainly as coming from entities from the Executive branch and the Central region; more than 46% of interviewees have 500+ employees.

Regarding Public-Sector entity employees, 41% of respondents established a BYOD policy and allowed access for the use of external USB devices and other storage devices such as external disks, databases

and files on servers. 59% of those interviewed responded that they did not. Among respondents from public sector entities, 60% responded that they did not have a BYOD policy compared to 40% that had one in operation.

More than 69% of respondents from public sector entities reported that 81% to 100% of their employees had access to the Internet at work; 21% answered that 61-80%; and 10% had 0-60%.

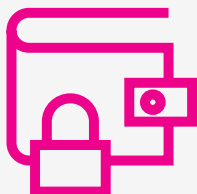
GRAPH 31: PERCENTAGE OF STAFF OF YOUR INSTITUTION WITH ACCESS TO THE INTERNET (2016)



WHAT APPROXIMATE PERCENTAGE OF YOUR ENTITY STAFF HAS ACCESS TO THE INTERNET TO DEVELOP THE ENTITY'S OWN ACTIVITIES?

- 0%-20%
- 21%-40%
- 41%-60%
- 61%-80%
- 81%-100%

Number of Observations: 583



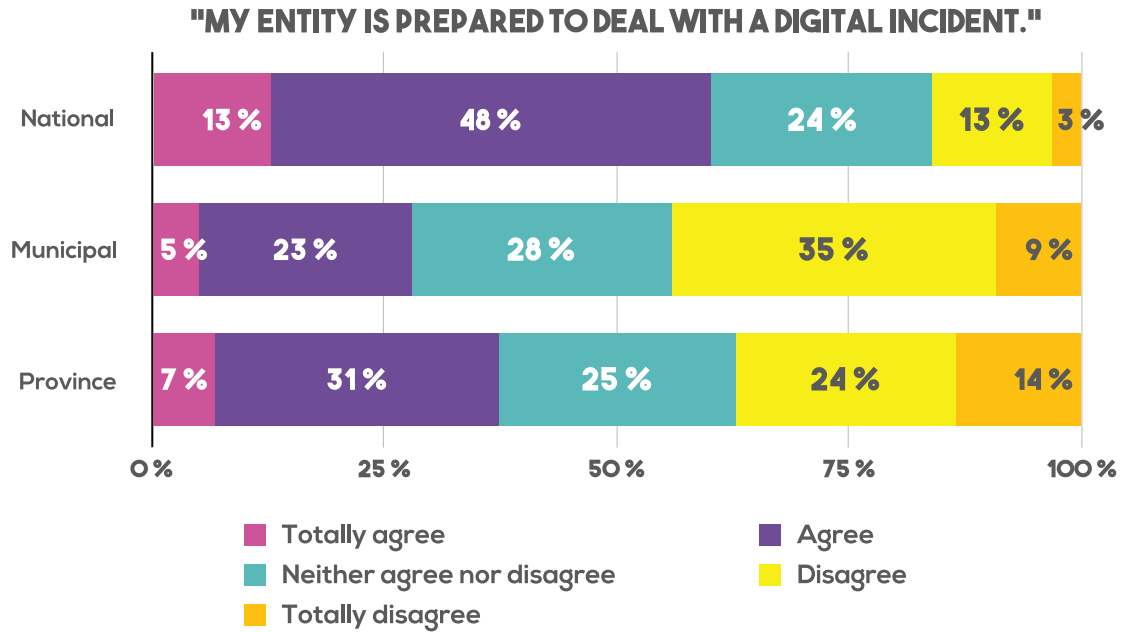
DIGITAL SECURITY PRACTICES IN ENTITIES

Having identified that most public entities allow their employees to access the Internet to carry out the activities of the entities, it is important to consider the measures that public entities have taken to protect themselves. When the question was asked: ***My entity/company is prepared to deal with a digital incident***, it was clear that most entities at the national level felt prepared. Entities reported that 13% and

48%, respectively at the national level, felt very prepared or prepared. These data, compared to the municipal and province levels, show that only 28% at the municipal level and 38% at the province level felt very prepared or prepared to handle an incident.

Some conclusions can be drawn from these results as it demonstrates that there is a higher level of confidence in national preparedness that is supported by all the initiatives being implemented by the national government in the development of a secure digital economy. On the other hand, it also indicates that it is necessary to develop these initiatives at the municipal and province level. See graph below:

GRAPH 32: LEVEL OF READINESS OF THE ENTITY TO DEAL WITH A DIGITAL INCIDENT



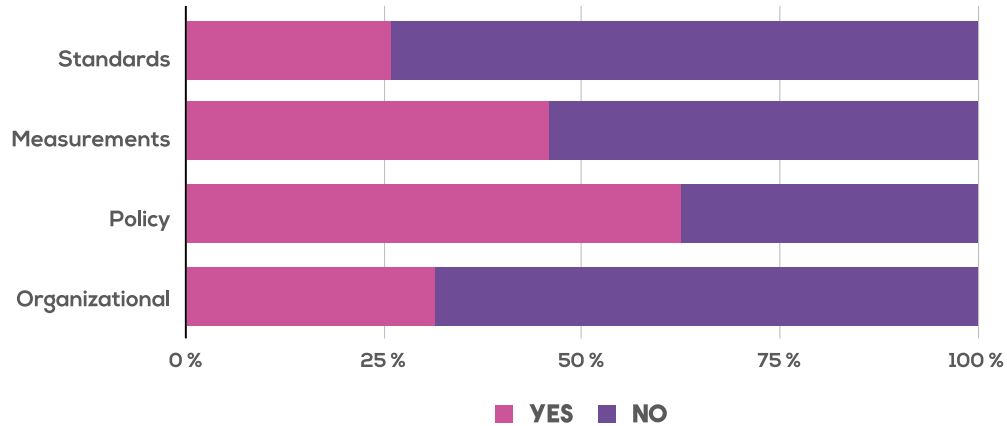
Number of Observations: 559

This led to an analysis regarding digital security practices that have been implemented by state entities in this matter. When asked, ***Which of the following practices in digital security (cybersecurity and/or information security) are implemented by your entity?***, similar to companies' response, most respondents from public entities reported that they

have policies, with lower priority standards and organizational measures. Of the total number of respondents, 62% reported that the policies were implemented, compared to 46% of the technical implementation measures, and only 31% reported that they implemented organizational measures.

GRAPH 33: DIGITAL SECURITY PRACTICES IMPLEMENTED BY ENTITIES

WHICH OF THE FOLLOWING PRACTICES IN DIGITAL SECURITY (CYBER SECURITY AND/OR INFORMATION SECURITY) ARE IMPLEMENTED BY YOUR INSTITUTION?



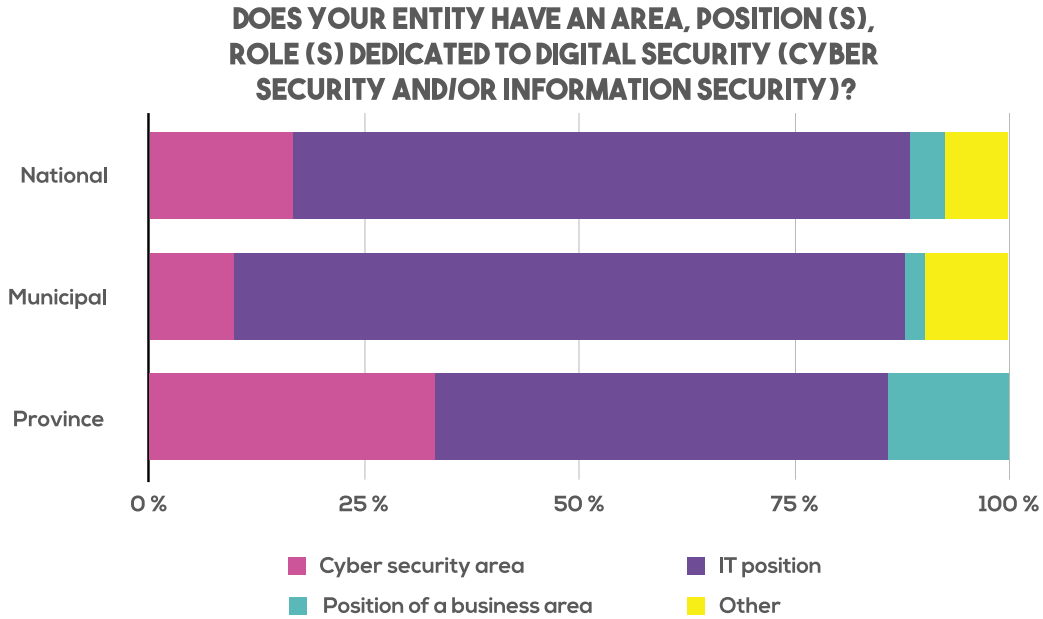
Number of Observations: 559

These results are particularly interesting when analyzed against the results of the question: ***Does your entity have an area, position (s) or role (s) dedicated to digital security (cybersecurity and/or security of the information)?***, as if the state entity placed low emphasis on implementing organizational measures, then there is a strong probability that they would not have a dedicated digital security position. Among interviewees, only 33% at national level and 10% and 17% respectively at the municipal and province level have an area dedicated to digital security within their organization.

As highlighted in the previous section on enterprises, there is a general tendency to shift responsibility for incident response and digital security under the general functions of the Information Technology Department. As such, 52% at the national level, 78% at the municipal level and 72% at the province level address the issue of

digital security under the Department of Information Technology. Only a very small percentage of respondents addressed this under the general business areas of the entities or other areas. See the graph below:

GRAPH 34: ENTITIES WITH AN AREA, POSITION (S) OR ROLE (S) DEDICATED TO DIGITAL SECURITY



Number of Observations: 246

When asked, How many people make up the team or area that is in charge of digital security (cybersecurity and/or information security) in their entity?, it is notable that 44% of those interviewed had only 1-2 employees, 27% had 3-5 people and 29% reported that they had more than 5. These results emphasize the need to examine how the issue of digital security is being

addressed within state entities. Some have argued that when the two areas are joined, the security views of an IT department vary in relation to the proactive and reactive measures that an entity must implement. According to Forbes, *‘Being a subdivision of the IT department makes security blind to important business processes and to decision making at the*

corporate and department level⁸. For example, security teams are often not part of planning processes in HR, Marketing and R&D departments, nor are they given the opportunity to review investments before they are concluded. As a result, the security teams are incorporated after the fact, and this can affect the final budget since the entities can end up spending more in recovery instead of investing, in the beginning, in a proactive security solution. However, if given a more prominent role within the organization, security teams could proactively advise the organization, thereby significantly reducing risks.

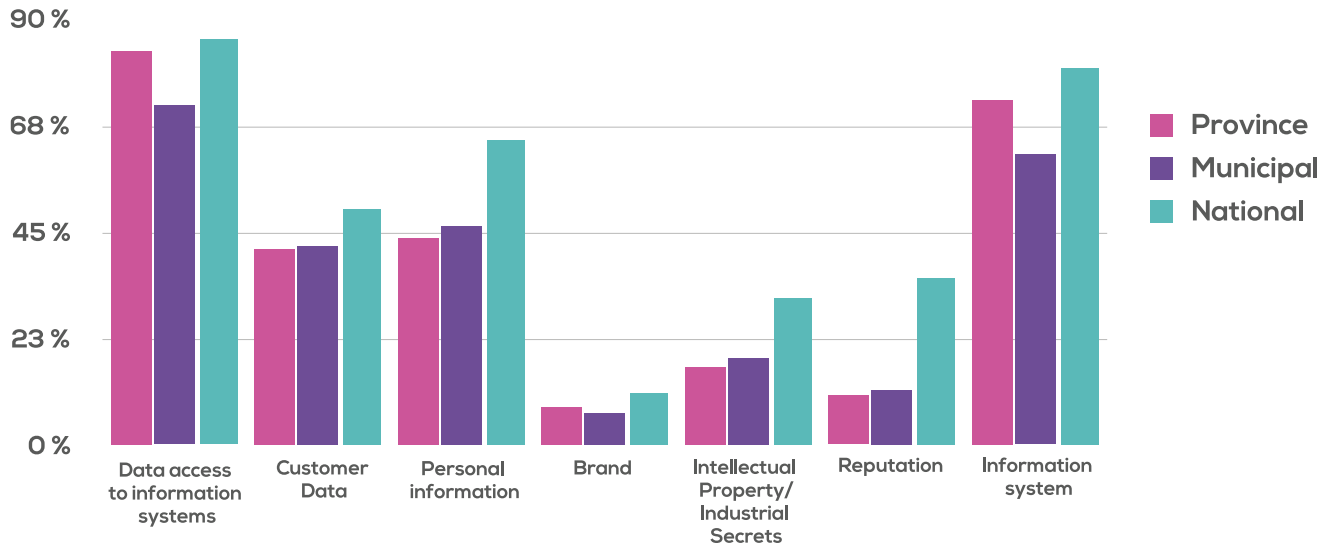
In addition, in identifying risks and implementing risk mitigation measures, state entities should consider the assets

⁸ Forbes (July 2015) Why It's Worth Divorcing Information Security From IT, accessed at: <https://www.forbes.com/sites/frontline/2015/06/22/why-its-worth-divorcing-information-security-from-it/#3ecd98c342a3>, Last entry: August 30, 2017

they believe should be prioritized for their protection. In response to the question: **Which of the data and/or information assets are prioritized by your entity?** at the national level, access to digital data in the information system and access to information systems had the highest priority in relation to personal data and following these, customer data in terms of priority. Similar results were observed at the municipal and province level. This is important since, based on what an entity prioritizes, it could be an indication of where it will invest in terms of digital security. See the graphs below:



GRAPH 35: DATA AND ASSETS PRIORITIZED BY ENTITIES



Number of Observations: 246

As mentioned above, understanding risk is important. In this study, **Digital security Risk Management has been defined as** the set of activities coordinated within an organization or among organizations to address the risk of digital security while maximizing opportunities. It is an integral part of decision-making and a comprehensive framework to manage the risk of economic and social activities. It is based on a flexible and systematic set of cyclical processes, as transparent and as explicit as possible. This set of processes

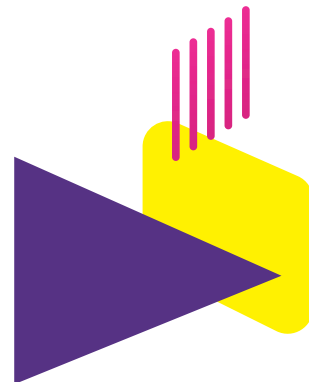
helps to ensure that digital security risk management measures (“security measures”) are appropriate for the risk and the economic and social objectives at stake. When the participants of the study answered the question: **Does your entity/ company carry out a risk assessment on the information it acquires to improve its operations?**, 89% of entities at the national level, 80% of entities at the municipal level and 88% of entities at province level responded positively.

Subsequently, when asked: ***Is your organization/company's risk management aligned with international standards?***, it is interesting to note that 87% at the national level responded positively, compared to 43% at the municipal level and 59% at the province level. Examination of these practices is important because, if an entity adopts proactive measures such as risk assessment and the application of international standards, it creates an environment for risk management and mitigation.



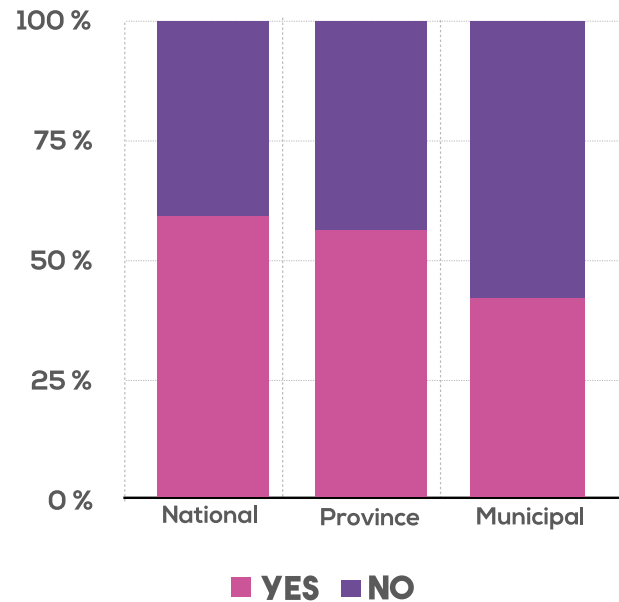
DIGITAL INCIDENTS IN ENTITIES

When the question was asked as to whether digital incidents against the organization were identified in 2016, more than half of the national and territorial-province state entities responded affirmatively. 59% of national entities identified digital incidents, while 56% of territorial-province entities responded in the same way. On the other hand, 42% of municipal entities responded that they have identified digital incidents.



HAS YOUR ORGANIZATION IDENTIFIED DIGITAL INCIDENTS AND/OR CYBER THREATS AGAINST YOUR ENTITY DURING 2016?

GRAPH 36: PERCENTAGE OF STATE ENTITIES THAT IDENTIFIED DIGITAL INCIDENTS (2016)



Number of Observations: 517

In order to understand why some state entities identified digital incidents and others did not, an equation was estimated of determinants of the probability of a public entity in Colombia identifying digital incidents and/or cybernetic threats against the company, where the dependent variable is "1" if the entity identifies digital incidents and "0" if it does not identify them.

Within the explanatory variables, four dichotomous variables were included: (i) if the public entity has an area, position (s) or role (s) dedicated to digital security; (ii) if the public entity is aware of any regulations

and/or national or territorial legislation that requires entities to implement digital security management practices; (iii) whether the entity implements technical measures (e.g., vulnerability testing, maintenance of IT infrastructure); (iv) if the entity implements digital security policies (for example, system access policy, password update policy, awareness); (v) whether the entity implements standards (e.g. ISO 27001, other international standards); (vi) if the entity makes any cyber risk assessment. In addition, we include dichotomous variables about the government tier of the entity.

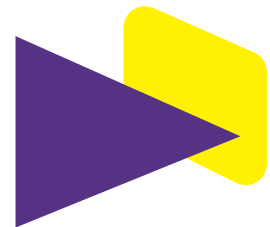
That is, national, territorial-province, or territorial-municipal.

Other explanatory variables were also included, such as the entity's total investment budget in Colombian pesos during 2016, the number of people working in the entity, the approximate percentage of entity staff with access to the Internet to develop their professional activities, as well as the approximate digital security budget value designated by the entity. Given the binary nature of the dependent variable, a estimation model is used.

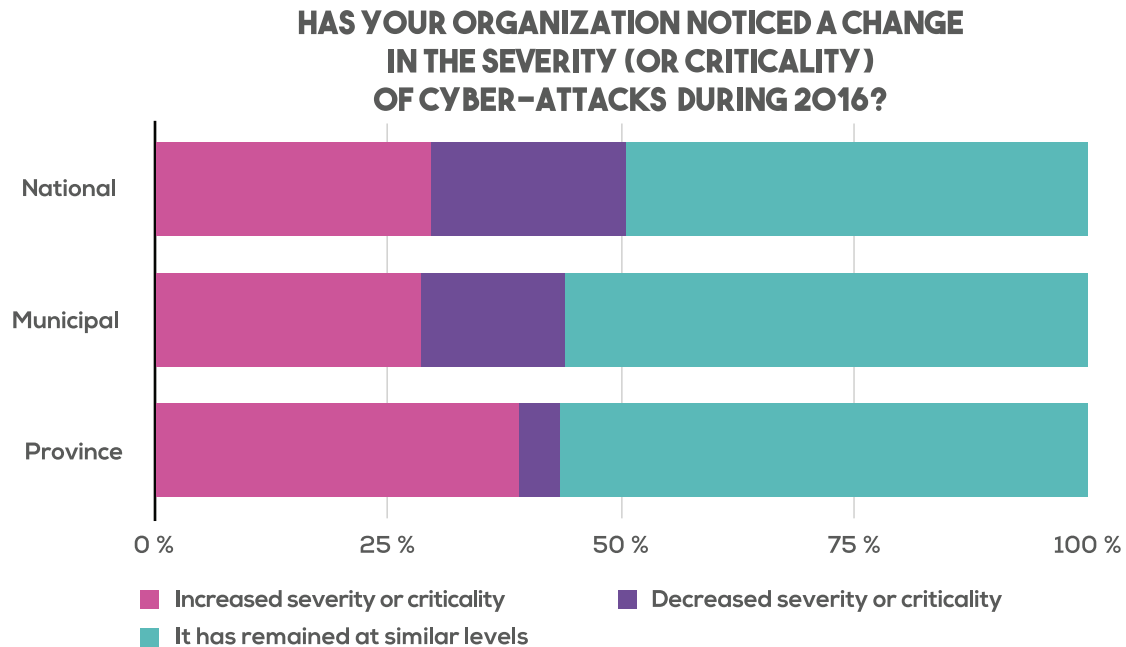
The results show that there is a statistically significant positive relationship between knowledge of some regulation and/or legislation on risk management practices and the identification of digital incidents. In fact, entities that identified digital incidents highlighted their knowledge about the National Digital Security Policy (CONPES Document 3854 of 2016), approved on April 11, 2016. There is also a statistically significant positive relationship between the implementation of technical measures, risk assessment practices and the identification of digital incidents. Likewise, there is a statistically significant positive

relationship between incident identification and the following explanatory variables: the approximate budget value designated by the entity for digital security, the number of people working in the entity, and the percentage of staff having access to Internet.

Another area examined by the study was the experience of state entities with digital security incidents. In response to the question: ***Has your entity/company noticed a change in the severity (or criticality) of cyberattacks during 2016?***, most interviewees (50% national, 56% municipal and 57% province) reported that the gravity of cyber-attacks remains the same. Only 30% at the national level, 28% at the municipal level and 39% at the province level reported that they had observed a change.



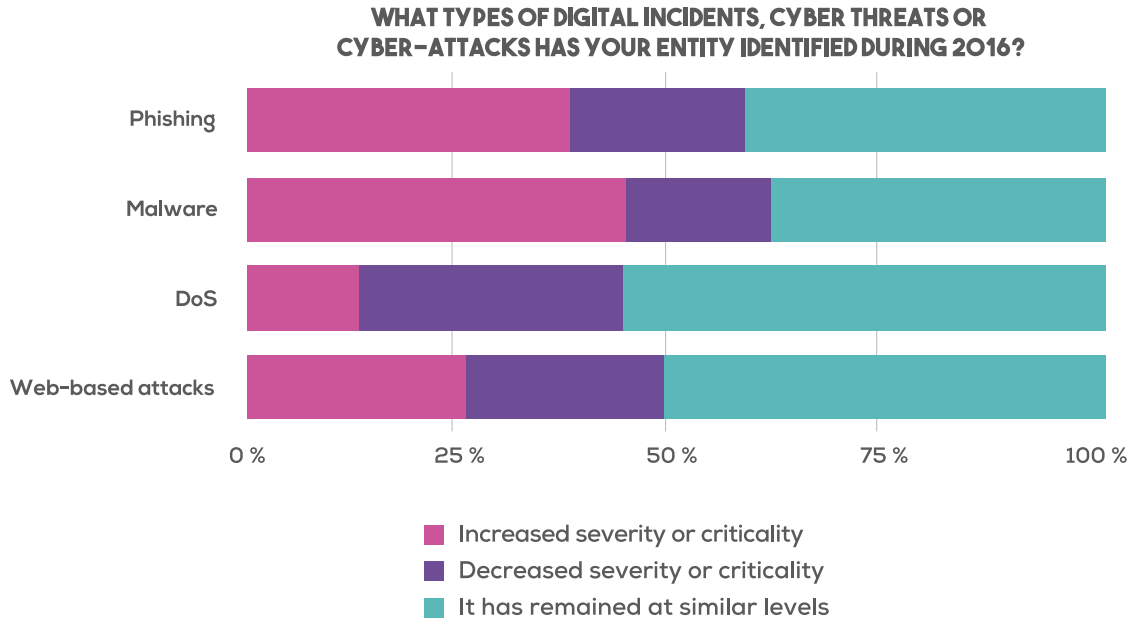
GRAPH 37: CHANGE IN THE SEVERITY OF DIGITAL INCIDENTS



Number of Observations: 240

In terms of Colombian entities that actually identify not only the increase in severity but in the type of attacks, respondents indicated that they have seen the largest increase in phishing and malware attacks. See the following graph:

GRAPH 38: SEVERITY OF DIGITAL INCIDENTS



Number of observations: 240

In this regard, when asked: In the occurrence of a digital incident, cyber-threat and/or cyber-attack, who is notified in the entity?, It was interesting that of the entities answering the question, 73% answered that they would inform the Directors of the organization with only 23% indicating that they would report to the Legal Adviser, 20% would inform the local/regional authority, 38% the national authorities (police, regulatory agencies, prosecutors, etc.) and 25% indicating that they would report to the Computer Security Incident Response

Team (CSIRT). The low indication in the notification of incidents to the national authority ultimately impacts the national government on the State's understanding of digital security incidents in Colombia. Although the State, at the national level, continues to invest in mechanisms to increase reporting, it can be inferred that it is necessary to increase these efforts within State entities.

These data, if compared to the question: *At what level is the area in charge of*

digital security (cybersecurity and/or information security) in your institution? (The highest level or hierarchy is the highest), it is worth noting that 47% at the national level, 68% at the municipal level and 57% at the province level indicated that it is at the operational level. Compared to the hierarchical (or director) level, 27% at the national level, 16% at the municipal level and 29% at the province level reported that it is at that level. What could be inferred from these results is that while digital security is not located at the director level, it is the first level within an entity to be reported of digital security incidents.

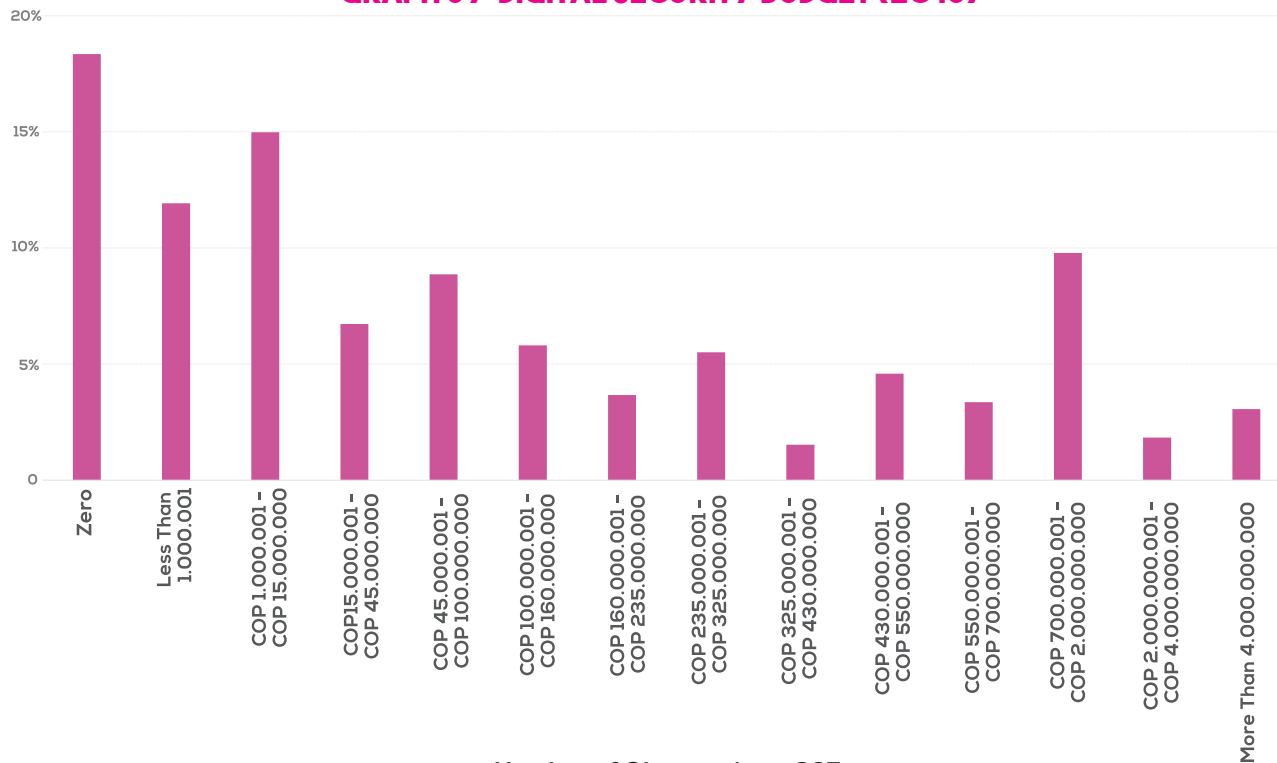
It is important to note where cyber incidents are reported and at what level digital security is located since this provides information on how an entity could strategically address incidents and related budgets. When asked: **Which of the following failings most affect your organization/company's capability in digital security (cybersecurity and/or information security)? Please rate: 1 (affecting less or does not affect) to 5 (affecting more)**, most interviewees identified **Lack of dedicated staff and Lack of budget** as the two reasons that affect them the most.



DIGITAL SECURITY BUDGET IN ENTITIES

It should be noted that most entities that allocated IT budgets in 2016 also did so for digital security issues: about 82% of state entities that allocated budget for IT also allocated for digital security in 2016. Considering the companies that allocated IT budget, the amount allocated by the state entities in 2016 was verified as indicated in Graph 39.

GRAPH 39: DIGITAL SECURITY BUDGET (2016)



Since the budget distribution is biased to the right, Table 5 presents the median digital security budget in 2016 considering the government tier of the state entities. It is important to note that Table 5 presents the digital security budget that is in the middle of the values provided by the national entities. However, it was noted that 18% of the state entities that allocated IT budget did not allocate any resources to digital security, particularly municipal and territorial-province entities. On the other hand, it was observed that some entities invested more than COP 6,000,000,000 Colombian pesos, the majority at the national level, but there were also isolated cases of entities at the municipal and territorial-province level.

TABLE 5: MEDIAN OF THE DIGITAL SECURITY BUDGET BY ENTITY THAT ASSIGNED IT

GOVERNMENT TIER	COP (\$)
Municipal	1 - 5 million
Province	25 - 35 million
National	235 - 265 million

Number of Observations: 327

When analyzing the digital security budget amounts allocated by the state entities, it was observed that **the median of the digital security budget in relation to the investment budget was approximately 0.05% of investments in 2016**. In addition, it was verified that, on average, most of the budget was allocated for platforms and technological means, while capacity

building received the least amount of resources. Approximately 46% of the digital security budget was allocated to electronic media and platforms, and 9% to capacity building which, in turn, included topics such as training and awareness raising.

TABLE 6: ALLOCATION OF THE DIGITAL SECURITY BUDGET BY ENTITY THAT ALLOCATED RESOURCES TO IT (2016)

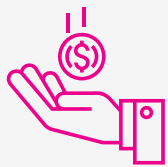
CATEGORIES	PERCENTAGE
Human Resources (e.g. employees, contractors)	30%
Platforms and Technological Media (e.g. hardware, software)	46%
Capacity Building (e.g. training, awareness raising, research)	9%
Specialized Services (e.g. security management, outsourcing, support)	15%

Number of Observations: 327

Finally, a linear regression was performed with the purpose of identifying the factors that drive a state entity to invest more in digital security. A linear regression was performed where the logarithm of the budget allocated by the entities for digital security issues during 2016 was the dependent variable (Appendix 3). We selected the logarithm of the digital security budget, with the aim of normalizing the distribution of the variable. In addition, the following independent variables were included: (i) the number of personnel; (ii) the approximate percentage of staff of the entity with access to the Internet to carry out its professional activities; (iii) the logarithm of the investment budget; and (iv) the logarithm of the number of digital incidents suffered by the public entity in 2016.

In addition, the model has dichotomous variables that identify the government tier of the public entity, such as national, territorial-province and territorial-municipal. The following dichotomous variables are also included: (i) if the entity has an area, position (s) or role (s) dedicated to digital security; (ii) whether the entity implements technical security measures (e.g., vulnerability testing, maintenance of IT infrastructure); (iii) if the entity adopts digital security policies (e.g., system access policy, password update policy, awareness); (iv) whether the entity implements standards (e.g. ISO 27001, other international standards); (v) if the entity conducts any cyber risk assessment; and (vi) if the entity is aware of any national or territorial regulations and/or legislation that require public entities to implement cyber risk management practices.

The results indicate that there is a positive and statistically significant relationship between the number of staff, staff with Internet access, state entity investment budget and the digital security budget. With regard to digital security practices, a significant and positive relationship was also observed between the digital security budget and the following dichotomous variables: existence of an area, position (s) or role (s) dedicated to security digital, implementation of technical measures and implementation of standards. In other words, public entities that implement these digital security practices assign a larger digital security budget than entities that do not adopt these practices. Finally, we should highlight the positively significant relationship between the entities at the national level and their digital security budget. In other words, national public entities have larger digital security budgets.

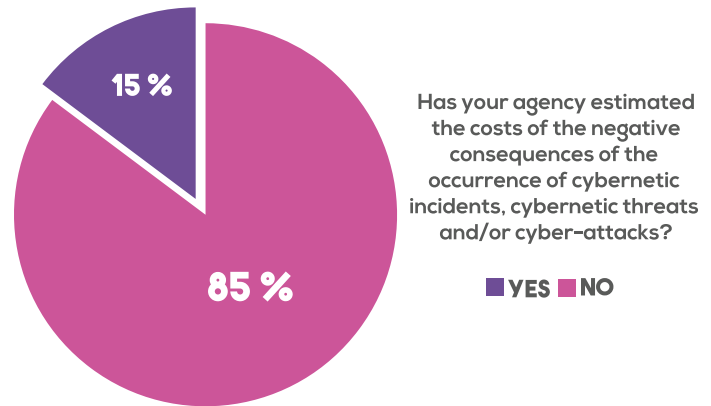


COST OF DIGITAL INCIDENTS FOR ENTITIES

When asked the question about the estimation of the costs derived from the negative consequences caused by the occurrence of digital incidents, 85% of the state entities affirmed that they do not

make any estimation, as seen in Graph 40 below:

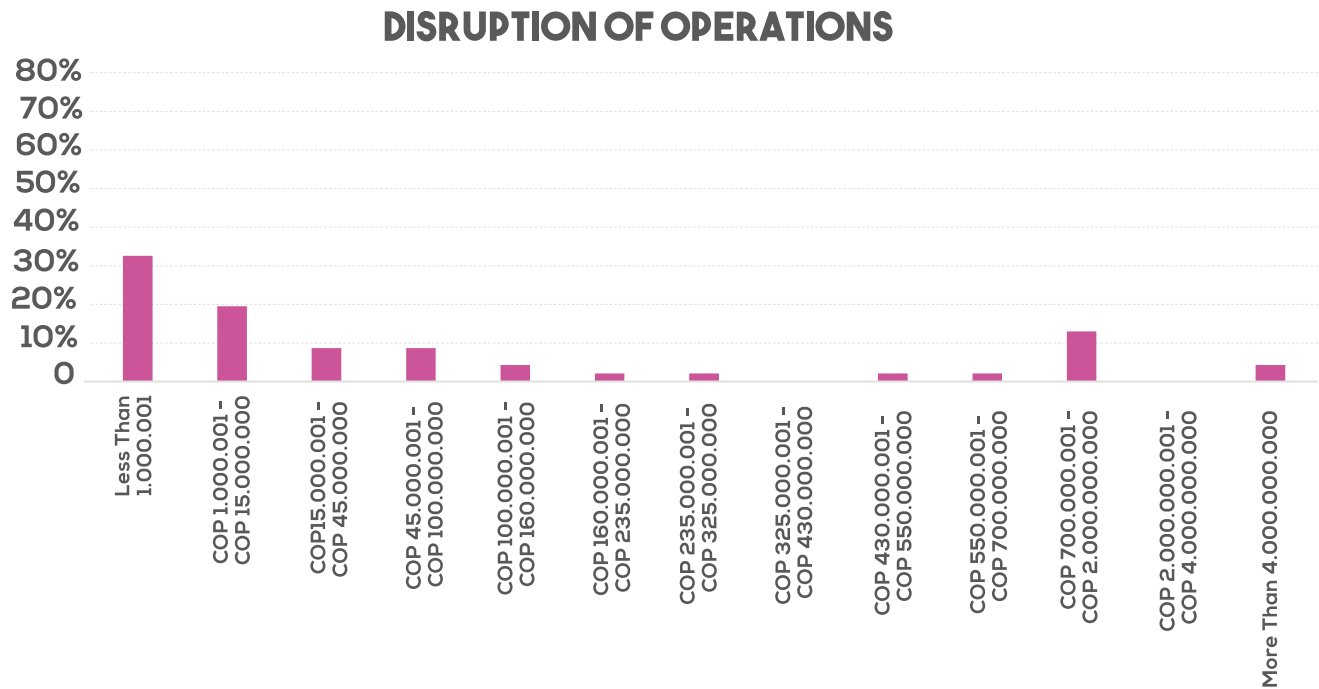
GRAPH 40: ENTITIES THAT ESTIMATED THE NEGATIVE CONSEQUENCES OF DIGITAL INCIDENTS (2016)



Number of Observations: 474

Taking into account the entities that estimated the costs incurred as a result of the digital incidents, the following graphs present the distribution of digital incident costs incurred in 2016 by state entities according to five cost categories: (i) discontinuation of normal company operations; (ii) damage to assets and infrastructure; (iii) penalties, fines and legal expenses; (iv) damage to reputation and image; and (v) loss of intellectual property or other sensitive information.

GRAPH 41: INFORMATION DISRUPTION COSTS INCURRED BY STATE ENTITIES THAT ESTIMATED THE IMPACT OF DIGITAL INCIDENTS (2016)

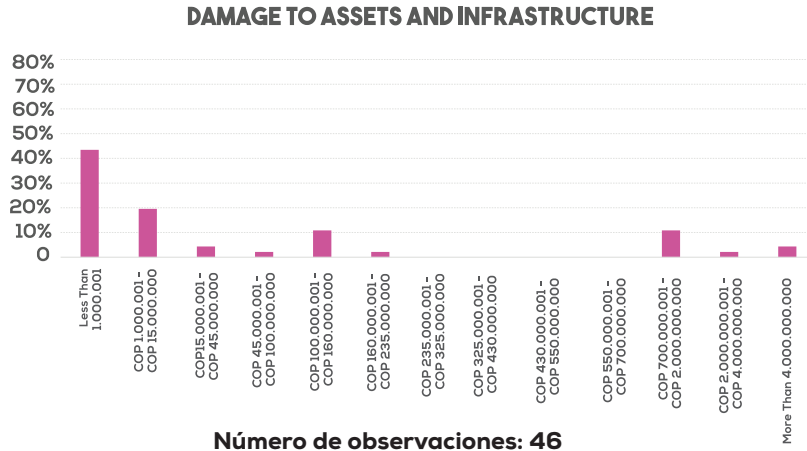


Number of Observations: 46

With respect to the cost of disrupting normal state entity operations, 33% of entities incurred in costs of less than COP 1,000,001, 20% incurred in costs of COP 1,000,001 - COP 15,000,000, and

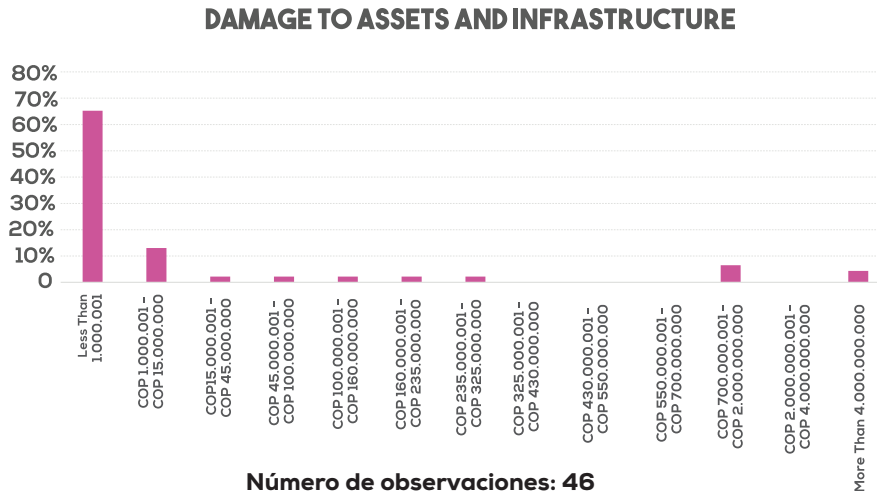
approximately 24% of COP 15,000,001 - COP 235,000,000. There are some entities with extreme values that are far from the data set, with more than 4 billion Colombian pesos.

GRAPH 42: COSTS OF DAMAGE TO ASSETS AND INFRASTRUCTURE INCURRED BY STATE ENTITIES THAT ESTIMATED THE IMPACT OF DIGITAL INCIDENTS (2016)



With respect to damage to the entity assets and infrastructure, more than 40% of the entities incurred in costs of less than COP 1,000,001, 20% incurred in costs of COP 1,000,001 - COP 15,000,000, and approximately 20% of COP 15,000,001 - COP 235,000,000. However, about 17% of the entities presented costs related to asset damage of more than 700 million Colombian pesos in 2016.

GRAPH 43: COSTS OF PENALTIES, FINES AND LEGAL EXPENSES INCURRED BY STATE ENTITIES THAT ESTIMATED THE IMPACT OF DIGITAL INCIDENTS (2016)

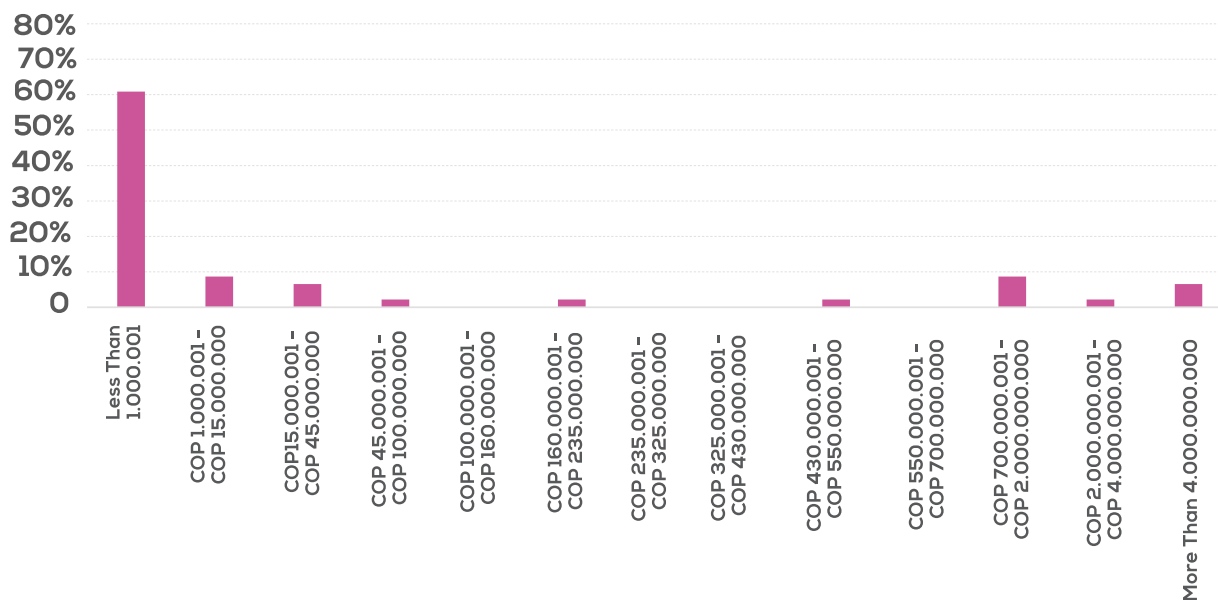


With respect to penalties, fines and legal expenses, 65% of the entities incurred in costs of less than COP 1,000,001, approximately 13% incurred in costs of COP 1,000,001 - COP 15,000,000, and approximately 10% of COP 15,000,001 - COP 235,000,000. About 11% of the

entities had costs higher than 700 million Colombian pesos, with some territorial-province entities costing more than 4 billion Colombian pesos.

GRAPH 44: REPUTATIONAL DAMAGE INCURRED BY STATE ENTITIES THAT ESTIMATED THE IMPACT OF DIGITAL INCIDENTS (2016)

DAMAGE TO REPUTATION



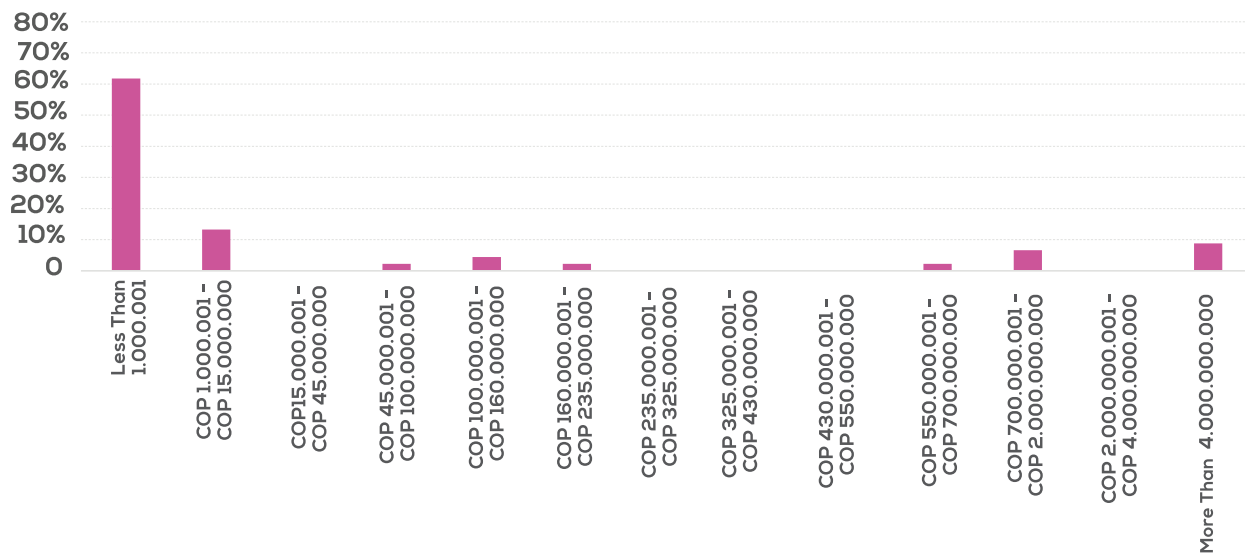
Número de observaciones: 46

With respect to reputational damage, approximately 60% of entities incurred in costs lower than COP 1,000,001 in 2016, approximately 9% incurred in costs of COP 1,000,001 - COP 15,000,000, and approximately 11% of COP 15,000,001 -

COP 235,000,000. On the other hand, it is interesting to note that 17% of the entities presented a cost higher than 700 million Colombian pesos.

GRAPH 45: COSTS OF LOSS OF INTELLECTUAL PROPERTY AND SENSITIVE INFORMATION INCURRED BY STATE ENTITIES THAT ESTIMATED THE IMPACT OF DIGITAL INCIDENTS (2016)

LOSS OF INTELLECTUAL PROPERTY AND SENSITIVE INFORMATION



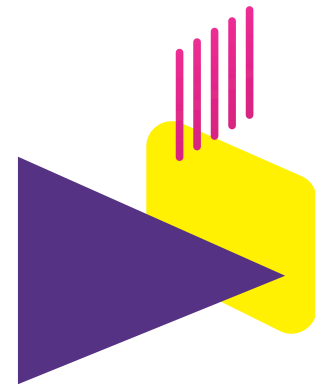
Number of Observations: 46

Finally, with respect to loss of intellectual property and sensitive information, 61% of the entities incurred in costs lower than COP 1,000,001, approximately 13% of COP 1,000,001 - COP 15,000,000, and approximately 9% of COP 15,000,001 - COP 235,000,000. On the other hand, it is observed that 15% presented costs higher than 700 million Colombian pesos, and others over COP 4,000,000,000: 9% of the entities.

It can be seen that the cost distribution among the five categories is biased to the right, so the aim was to work with the median of the grouped cost incurred. In relation to national state entities, the cost interval is 20 - 40 million Colombian pesos, representing approximately less than 0.5% of entities' investment. The national entities that provided the cost data are, for the most part, in the executive branch

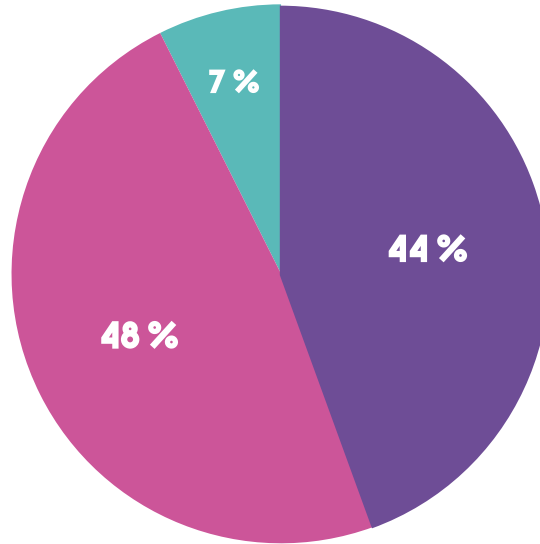
or are autonomous entities. In this context, it should be taken into account that these data reflect the situation of public entities with these characteristics. In addition, no significant number of territorial entities responded the cost information.

Finally, there was an analysis on how the costs incurred from digital incidents in 2016 impacted state entities' investments in research, development and innovation (R&D&I). As shown in Graph 46 below, 48% of the state entities interviewed said that they have increased their investments in R&D&I.



GRAPH 46: INVESTMENT IN R&D&I OF ENTITIES ESTIMATING THE IMPACT OF DIGITAL INCIDENTS (2016)

HOW DID YOUR ORGANIZATION'S INVESTMENTS IN RESEARCH, DEVELOPMENT AND INNOVATION (R&D&I) CHANGE AS A RESULT OF DIGITAL INCIDENTS IT SUFFERED?



■ Increase ■ Decrease ■ No change

Number of Observations: 46

Among the entities that stated that their investments in R&D&I had increased as a result of digital incidents, 46% of these entities responded that their investments increased by more than 15% in 2016. It should be noted that these entities are mostly national, in the executive branch, or they are autonomous entities or control and monitoring agencies.



APPENDIX 1



SITUATIONAL ANALYSIS



OVERVIEW OF DIGITAL SECURITY IN COLOMBIA

In 2011, the Government of Colombia, through the National Council for Economic and Social Policy (CONPES), established the Policy Guidelines for digital security and cyber-defense, Document CONPES 3701, with the support of the Ministry of Information and Communications Technologies MinTIC), the Ministry of National Defense, the National Planning Department (DNP) and other key national institutions. This strategy focused on the establishment of national institutions necessary for the development of cybernetic capacity in Colombia.

In 2014 there was a significant development where the national Government carried out an in-depth review of CONPES Document 3701 and requested international support in the revision and development of a new digital national security strategy. In April 2016, the new National Digital Security Policy, CONPES 3854 was approved, which articulated a strategic vision where Colombians are encouraged to make

responsible use of the digital environment and strengthen their capacities to identify, manage, treat and mitigate the risks of digital security. This new CONPES 3854 document fed from the successes of its predecessor and focused on promoting and securing a digital Colombia.

In the context of digital security based on risk management, CONPES 3854 promotes the participation of multiple actors, especially in the cross-sectional functions. As a direct result, Colombia is the first country in Latin America and one of the first in the world to fully incorporate the recommendations and best international practices in risk management and digital security recently issued by the Organization for Economic Co-operation and Development (OECD).

DIGITAL SECURITY RISK MANAGEMENT FOR ECONOMIC AND SOCIAL PROSPERITY; OECD RECOMMENDATION

The OECD promotes policies and instruments for innovation and trust in the digital economy and the issuance of recommendations on digital security risk management for economic and social prosperity (2015), and provides guidance

for the development of national strategies based on the management of digital security risks and the optimization of the economic and social benefits derived from the digital opening. The OECD recommendations include the promotion of general principles on knowledge, skills and training, responsibility, human rights and fundamental values, cooperation, risk assessment and treatment cycle, security, innovation and preparation measures and continuity. These guided recommendations were incorporated into various aspects of the development process and the content of the CONPES Document 3854. As such, in the review of the progress made in the implementation of this national policy under the situation analysis, the observations would be taken into account on the alignment of public policies with the OECD recommendation.

The process of joining the OECD has been described as having a positive impact on Colombia's public policymaking process⁹. In May 2013, Colombia was invited to begin the formal accession process to the OECD. The invitation included a road map¹⁰. Colombia would have to demonstrate to

9 Why Good Policy-Making Matters: The Accession Case of Colombia to the OECD Source: <https://www.hertie-school.org/the-governance-post/2016/03/why-good-policy-making-matters-the-accession-case-of-colombia-to-the-oecd/> Accessed August 25, 2016

10 [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=C\(2013\)110/FINAL&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=C(2013)110/FINAL&docLanguage=En)

23 OECD technical committees that it has made significant reforms to comply with OECD standards, since these committees would have to present formal opinions on Colombia's accession to the Council.

In the OECD *Economic Outlook*¹¹, Volume 2016, Number 1, the OECD generally concluded that macroeconomic policies [in Colombia] were appropriate, but structural reforms were needed to increase productivity. Despite the impact of global financial market volatility and declining oil prices, the OECD foresaw that, by bringing the peace process to fruition, it could improve corporate confidence and capital inflows. In addition to the accession process to the OECD, Colombia participates in the work of many of the organization's specialized committees.

It is pertinent to consider the OECD process when examining the development and implementation of public policies, including the CONPES Document 3854, given it takes into account OECD recommendations for the management of digital security risks. As part of the OECD, Colombia could receive ongoing study and evaluation of the effectiveness of its policies. This ongoing evaluation process,

11 Last consulted on September 8, 2016 at: Profile of Colombia- http://www.keepeek.com/Digital-Asset-Management/oecd/economics/oecd-economic-outlook-volume-2016-issue-1/colombia_eco_outlook-v2016-1-11-en#page1 Full Version: http://www.oecd-ilibrary.org/economics/oecd-economic-outlook-volume-2016-issue-1/colombia_eco_outlook-v2016-1-11-en

known as peer review, has proved to be effective and useful, because it exposes reform programs to discussion by good researchers (OECD staff), as well as by experts in the formulation of real policies in the specific area (members of each committee)¹².

IMPLEMENTATION OF THE CONPES DOCUMENT 3854

The increasing use of the digital environment in Colombia to develop economic and social activities generates uncertainties and risks inherent in digital security that must be managed permanently. Failure to do so may result in the materialization of cyber threats or attacks, with undesirable economic or social effects for the country, and affecting the integrity of citizens in this environment.

The focus of the digital security and cyber-defense policy had been, until 2015, counteracting the increase in cyber threats under the objectives of (i) the country's defense; and (ii) the fight against cybercrime. Although such a policy approach had positioned Colombia as one of the leaders in the field at the regional

12 Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. Consulted on September 8, 2016. Available at: <http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf>

level, it had also left out risk management in the digital environment. The approach, essential in a context of increasing use of ICT for economic and social activities, has brought with it new and more sophisticated ways of affecting the normal development of ICT in the digital environment. This fact demands greater planning, prevention and attention by the countries.

Taking into account the above, the following problems were identified in the country: (i) there is no strategic vision in digital security based on risk management; (ii) multiple stakeholders do not maximize their opportunities when developing socio-economic activities in the digital environment; (iii) strengthened digital security capabilities are required with a digital security risk management approach; (iv) there is a need to strengthen cyber-defense capabilities with a digital security risk management approach; and (v) national and international cooperation, collaboration and assistance efforts related to digital security are not sufficient and need to be articulated.

In order to address this problem and to adopt international best practices, the Government of Colombia issued the ***National Digital Security Policy*** (Document CONPES 3854 of 2016) in April 2016, led by the Ministry of Information and Communications Technologies and the Ministry of National Defense of Colombia.

The main objective of this public policy is the strengthening of the capacities of all the stakeholders (national and territorial governments, public and private organizations, the Public Force, owners or operators of national critical cybernetic infrastructures, academia and society civil society) to identify, manage, treat and mitigate the risks of digital security in their socio-economic activities in the digital environment, within a framework of cooperation, collaboration and assistance at national and international level, in order to contribute to the growth of the national digital economy and maximize the benefits obtained from greater economic, political and social prosperity of the country.

The issuance of this new public policy was the result of a process of participation among representatives of the country's multiple stakeholders and it is one of the first national policies in the world and first in the Latin American region to adopt the risk management recommendations issued in September 2015 by the Organization for Economic Co-operation and Development, OECD. The contributions made by the representatives of the Companies, the national Government, civil society, national critical infrastructure operators and academia were taken into account. Also incorporated were the recommendations of other international organizations such as the Organization of American States, OAS, the International Telecommunication

Union, ITU, and the North Atlantic Treaty Organization, NATO.

Colombia's National Digital Security Policy: (i) clearly differentiates the objectives of economic and social prosperity from the country's defense objectives and the fight against crime in the digital environment, (ii) includes components such as governance, education, regulation, international and national cooperation, research and development, and innovation; and (iii) changes the traditional approach by including risk management as one of the most important elements for addressing digital security. This is done under four (4) fundamental principles, focusing on safeguarding human rights and fundamental values of citizens in Colombia, actively involving all stakeholders, and ensuring a shared responsibility among them. These principles are reflected in five (5) dimensions where this policy will act, which determine the strategies to achieve the main objective.

Finally, in 2017, a **National Digital Security Agenda** will be built in Colombia, together with multiple stakeholders, in order to prioritize national interests around the issue, identifying impact variables (for example, economic losses, impact on people, environmental consequences or relationship of the effects with other parties), under the framework of the fundamental principles of the **National**

Digital Security Policy. Formulation of the following is also expected:

1. Strategic documents for policy implementation: Multi-stakeholder Coordination Mechanisms, International Strategic Agenda for Cooperation, Collaboration and Assistance, and National Strategic Agenda for Cooperation, Collaboration and National Assistance.
2. Plans to strengthen institutional, operational, administrative, human and physical and technological infrastructure capacities of the current institutions.
3. Technical feasibility studies for the creation of new digital security and cyber-defense instances or projects.
4. Specialized educational content to train officials responsible for digital security in Colombia.
5. Complementary educational contents related to the management of digital security risks tailored to students of basic, middle and higher education as well as to teachers.



PROGRESS IN THE NATIONAL DIGITAL SECURITY CAPACITY MATURITY MODEL

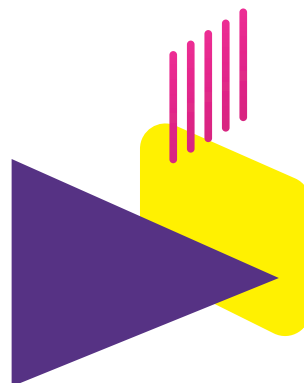
The National Digital Security Capacity Maturity Model (CMM) developed by Oxford University's Global Cybersecurity Capacity Centre was the basis for the **Cybersecurity Report: Are we prepared in Latin America and Caribbean?** This model assesses the maturity of a country's digital security in 5 main dimensions: (1) Policy and Strategy; (2) Culture and Society; (3) Education; (4) Legal frameworks; and (5) Technologies. This report included a country profile for Colombia, which shows a high level of digital security capacity maturity in the country, as assessed.

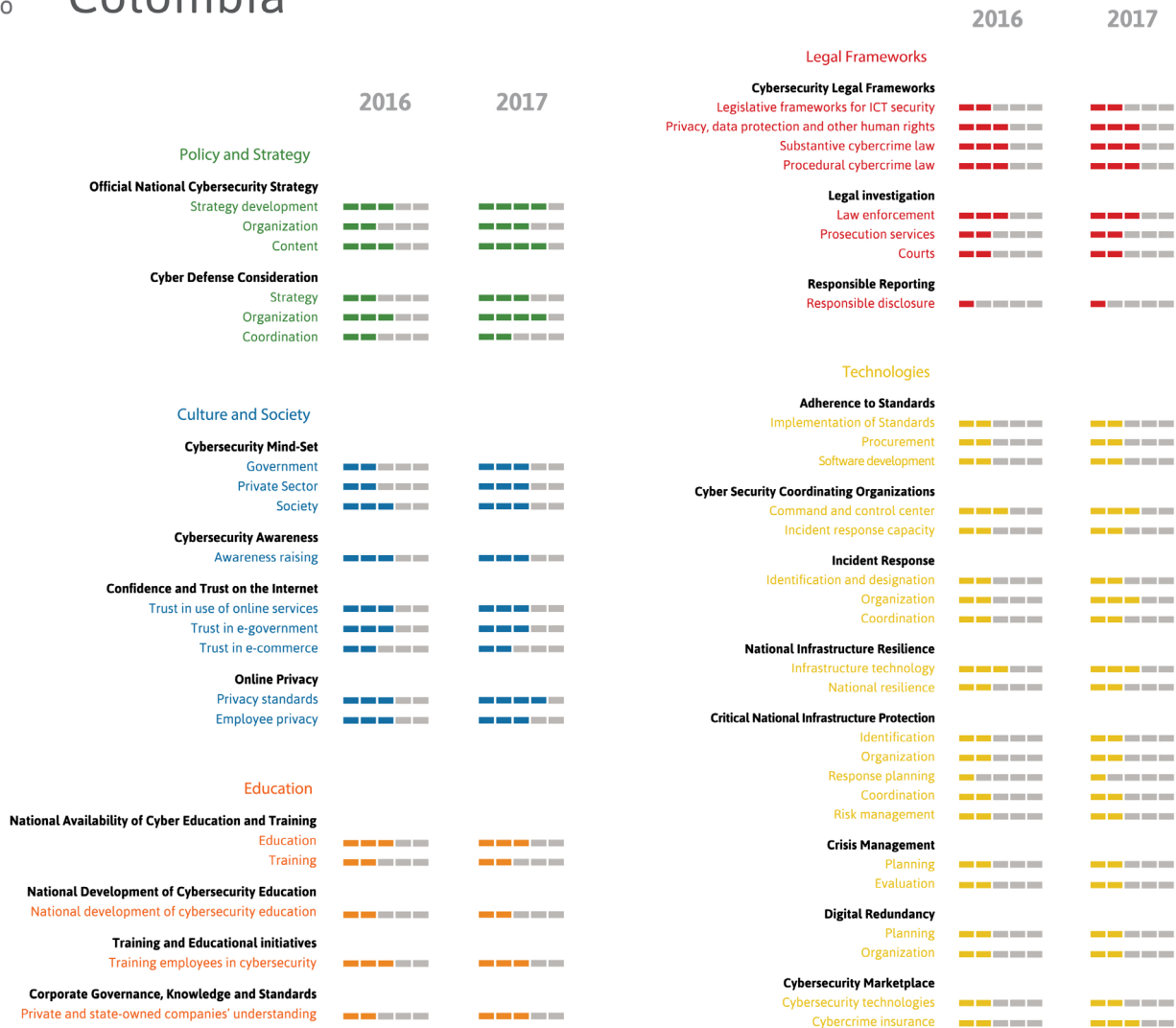
Colombia is the first country to conduct an evaluation of the improvements made in relation to the first CMM evaluation. As such, the analysis below provides a parallel comparison of the progress achieved since

the approval and implementation of the CONPES 3854 Document in its issuance in April 2016.

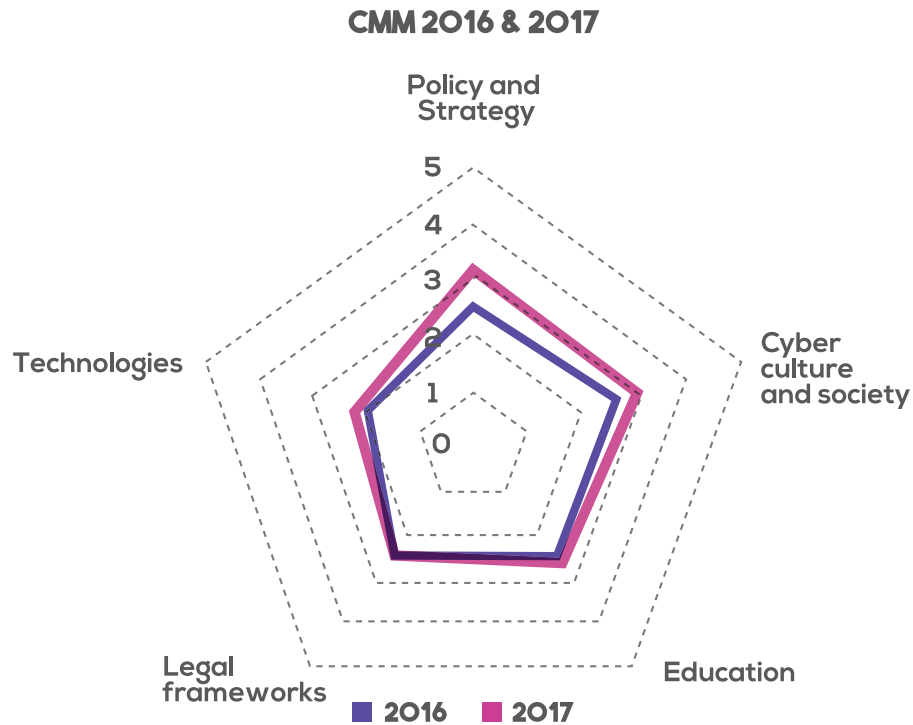
In general, most indicators have had improvements with significant movement in Dimension 1. It was observed during this period that the implementation of the CONPES 3854 Document of 2016 allowed Colombia to experience a significant level of maturity in terms of stakeholder participation, coordination with national development policies and the incorporation of risk management as part of the implementation framework.

In addition, Dimensions 2 (Culture and Society) and 3 (Education) also had a notable improvement in the last year.





GRAPH 47: COMPARISON OF CMM RESULTS (2016 AND 2017)



Dimensions

In relation to **Dimension 1 (Policy and Strategy)**, the new **National Digital Security Policy** (CONPES Document 3854, 2016) is currently being implemented in Colombia, which seeks to involve multiple stakeholders in the management of digital security risk, so they can assume their responsibility according to their role and

function and actively participate both in the construction phase of the elements included in this document and in the implementation of the policy. To this end, the National Digital Security Coordinator will design and implement, during the second half of 2017, a dynamic coordination

mechanism that defines (i) the roles, responsibilities and functions of multiple stakeholders; and (ii) a communication and follow-up matrix between the National Digital Security Coordinator, the highest level of government (National Digital and State Information Commission) and the multiple stakeholders, in order to address the digital security issues in Colombia.

The National Digital Security Policy includes an Action and Follow-up Plan (PAS, in Spanish) which includes all the actions that will be implemented in order to achieve both the general objective and the specific objectives of the Policy. Specifically, this PAS establishes measurement processes and metrics for each action as follows: responsible for the execution, time of execution, relative importance of the action, relation with other actions, compliance indicators, cost of the action, allocated financial resources for the action and its sources and follow-up to the implementation through annual progress cut-offs. This PAS is periodically reviewed by the National Planning Department (DNP) together with the National Digital Security Coordinator, in order to renew, if necessary, the provisions of the National Digital Security Agenda (an instrument for prioritizing national interests around the matter, identifying impact variables).

Within the framework of strategies and actions established in the PAS, it is

worth noting that the Ministry of National Defense will carry out and participate in national and international simulation and training exercises that will develop the skills and abilities for the multiple stakeholders responsible for national cyber and national defense critical infrastructures in the digital environment, in order to strengthen the capacities of those responsible for ensuring national defense in the digital environment.

Within the framework of the National Digital Security Policy (Document CONPES 3854 of 2016) a clear institutional framework is established around digital security in Colombia. To this end, the highest levels of coordination and superior guidance on digital security are created in the national government, and sectoral liaison figures are established in all entities of the executive branch at the national level. In particular, the position of National Digital Security Coordinator was created, to direct the implementation of the national digital security policy and to continuously monitor it, together with the National Planning Department.

Finally, the National Digital Security Coordinator will perform inter-institutional and intersectoral coordination in all digital security issues in the country. Additionally, in the long term, the aim is to create a Digital Security and Cyber Defense Directorate, under the Deputy Ministry of Defense for International Affairs and Policies, as a

relevant element to implement escalation levels for the reporting of digital incidents and ensure the participation of multiple stakeholders in the management of digital security risks. In the short term, the implementation of the strengthening plan for colCERT will be the beginning. This will develop the necessary capacities to implement a multi-stakeholder participatory governance scheme and define escalation levels for the reporting of digital incidents.

In relation to **Dimension 2 (Culture and Society)**, a digital security risk management model is currently being designed and administrative mechanisms will be created so that all the administrative entities and departments of the executive branch adopt and implement it, permanently. Programs, projects and awareness-raising and sensitization campaigns, as well as training, exchange and transfer workshops on best practices in digital security for all multi-stakeholders are also carried out. The actions made in front of public organizations, in particular all public entities in the executive sector, are highlighted. Likewise, awareness days are being held for local entities.

The national government continues to implement and strengthen its e-government strategy called "**Gobierno en línea**", in order to build a more efficient, transparent and more participatory State

through Information and Communication Technologies (ICT). Within the framework of this strategy, activities are carried out under the following themes: i) **ICT for Open Government**: seeks to build a more transparent and collaborative State, where citizens are actively involved in ICT decision-making; ii) **ICT for services**: seeks to create the best procedures and services online to respond to the most pressing needs of citizens, iii) **ICT for management**: seeks to give strategic use of technology to make management more effective, and iv) **Security and privacy of the information**: seeks to safeguard the citizens' data as a treasure, guaranteeing the security of the information.

Online privacy is also being addressed. In keeping with the principles recommended by the OECD and the recommendations of agencies such as the OAS, Colombia's National Digital Security Policy is governed by four fundamental principles defined according to the national context. Human rights and the fundamental values of citizens in Colombia are safeguarded, actively involving all stakeholders, and ensuring a shared responsibility among them. These principles are reflected in the dimensions where this policy acts, which determine the strategies to achieve the main objective.

The first fundamental principle was established as follows: "**Safeguarding human rights and fundamental values of**

citizens in Colombia, including freedom of expression, free flow of information, confidentiality of information and communications, protection of privacy and personal data and privacy, as well as the fundamental principles enshrined in the Political Constitution of Colombia. In case of limitation to these rights, it must be under exceptional measures and be in accordance with the Political Constitution and applicable international standards. These measures must be proportional, necessary and be framed in legality”.

In relation to **Dimension 3 (Education)**, Colombia has made significant progress in the generation of academic offer specialized in digital security. In 2011, Colombia had twelve academic programs at the national level, from the technical level to the masters’ level, while to date it has more than fifty programs and a wide range of informal education courses, including international recognition certificates.

In addition, one of the functions assigned to the National Digital Security Coordinator is to ensure that the programs, projects and awareness raising campaigns, as well as the training provided by the different entities, are designed on the basis of guidelines issued by the National Digital and State Information Commission, in order to avoid duplication of effort and guarantee efficiency in the management of resources.

The policy addresses the national development of digital security education and it also proposes strategies such as strengthening the instances and entities responsible for digital security, evaluating the creation of new instances where training, research and innovation is developed, especially in relation to technical capabilities inherent in digital security. To ensure the relevance of the creation of new instances, the Ministry of National Defense will carry out feasibility studies for the creation of a **Center of Excellence for Digital Security**, among others.

Likewise, the capacities of those responsible for ensuring national defense in the digital environment will be strengthened. The Ministry of National Defense will design specialized educational content and train the multiple stakeholders responsible for ensuring national defense in the digital environment. The Ministry will carry out and participate in national and international simulation and training exercises that will develop skills and abilities for multiple stakeholders responsible for national critical cybernetic infrastructures and national defense in the digital environment. These activities would involve the multiple stakeholders responsible for national critical cyber infrastructures and national defense in the digital environment.

Finally, taking into account the background of the implementation of digital security

and cyber-defense guidelines in the country (CONPES Document 3701 of 2011), the decision-making bodies of state and private companies in Colombia are now aware that their organizations may be at risk and generally make investment decisions on reactive security measures.

In addition, in relation to **Dimension 4 (legal frameworks)**, while the level of maturity remains stable, the new National Digital Security Policy establishes a set of actions aimed at providing the legal and regulatory framework that supports all aspects necessary to comply with the policy objectives. For this purpose, the policy provides that the different instances will submit the proposals of adjustment and of new regulations that are required, to the consideration of the Ministry of Justice and Law of Colombia and it will verify constitutional and legal coherence. In addition, the Communications Regulatory Commission (CRC) will adjust the regulatory framework for the ICT sector in 2017 taking into account issues necessary for the management of digital security risks, such as the protection of communications users or the quality regime of telecommunications.

The framework of crimes established in Law 1273 of 2009 was made considering essential aspects of the characterization of crimes defined in the Convention on

Cybercrime (Budapest Convention), however, the legislative process required to achieve adherence to this convention is still underway. For this purpose, the policy provides that the different instances will submit the proposals of adjustment and of new regulations that are required, to the consideration of the Ministry of Justice and of the Law of Colombia. The country has made progress in its incorporation into information networks related to cybercrime and response teams and, mainly through the Police Cyber Center (CCP, in Spanish), it actively collaborates in research processes in this area.

Finally, in relation to **Dimension 5 (Technologies)**, the National Digital Security Policy establishes actions for digital security risk management capabilities, including adoption of good practices and standards by all stakeholders. National Resilience is very important. The construction of the National Digital Security Policy approved last year by the Government of Colombia, as well as existing spaces such as Critical Infrastructure, Operational Risk and Cyber Defense meetings, have generated a dynamic of interaction between the public and private sectors. In fact, the work tables specifically prepared to address critical infrastructure issues, led by the country's defense sector, do so regularly (once a month).

In the framework of the working groups, talks are held on the vulnerabilities to which information assets of Critical Infrastructure are exposed. However, a protocol or mechanism to ensure periodic reporting of vulnerabilities and the extent to which reporting should be carried out has not been consolidated. Talks are also held to sensitize operators of Critical Infrastructures on digital security. Colombia has a growing offer of specialized training in digital security (certified courses and even master's programs) which have been accessed by some of the operators of Critical Cybernetic Infrastructure.

In relation to software development, the new National Policy establishes actions for the strengthening of digital security risk management capabilities in all stakeholders. In particular, the Government of Colombia is promoting the development of the Information Technology industry and digital entrepreneurship through different initiatives. Some of them even promote security certificate programs for company personnel, as well as funding certificate programs in maturity models, widely known as CMMI.

In relation to cybercrime insurance, in Colombia there are insurance companies that offer insurance policies (with additional and optional protections) intended for companies and natural persons in their decision-making bodies, in order to: i) cope with responsibility **for the use and processing of information** (derived from data protection, management and handling of personal data and the consequences of loss of corporate information); and ii) to deal with **data security liability** (damages and defense costs associated with contamination of third party data by a virus, improper or erroneous denial of access rights to the data to an authorized third party, theft of an access code of the company premises, a computer system, or an employee, destruction, modification, corruption, damage or deletion of data stored on any computer system, theft of hardware to a company, containing personal or corporate data or disclosure of data as a result of a data security breach).

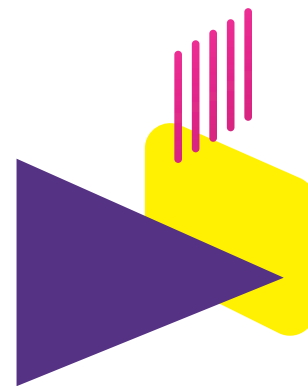


SWOT ANALYSIS

A SWOT analysis (strengths, weaknesses, opportunities, and threats) was applied to the data collected to date, as a way to gain a deeper understanding of digital security capability in Colombia. This SWOT analysis took into account documentary research, information gathered during consultations with stakeholders and publicly available data on Colombia, including its economic and political realities, as well as its economic development objectives. However, the SWOT analysis does not intend to conduct a comprehensive national analysis, but it focuses on the impact that external

factors may have on the implementation of the CONPES 3854 Document, the development of new digital security initiatives and the improvement of maturity of digital security in Colombia.

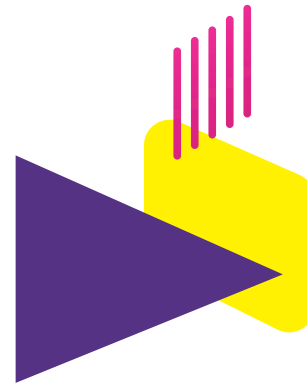
The implementation of a SWOT analysis of national digital security capability takes into account internal factors, including resources and expertise available and under country



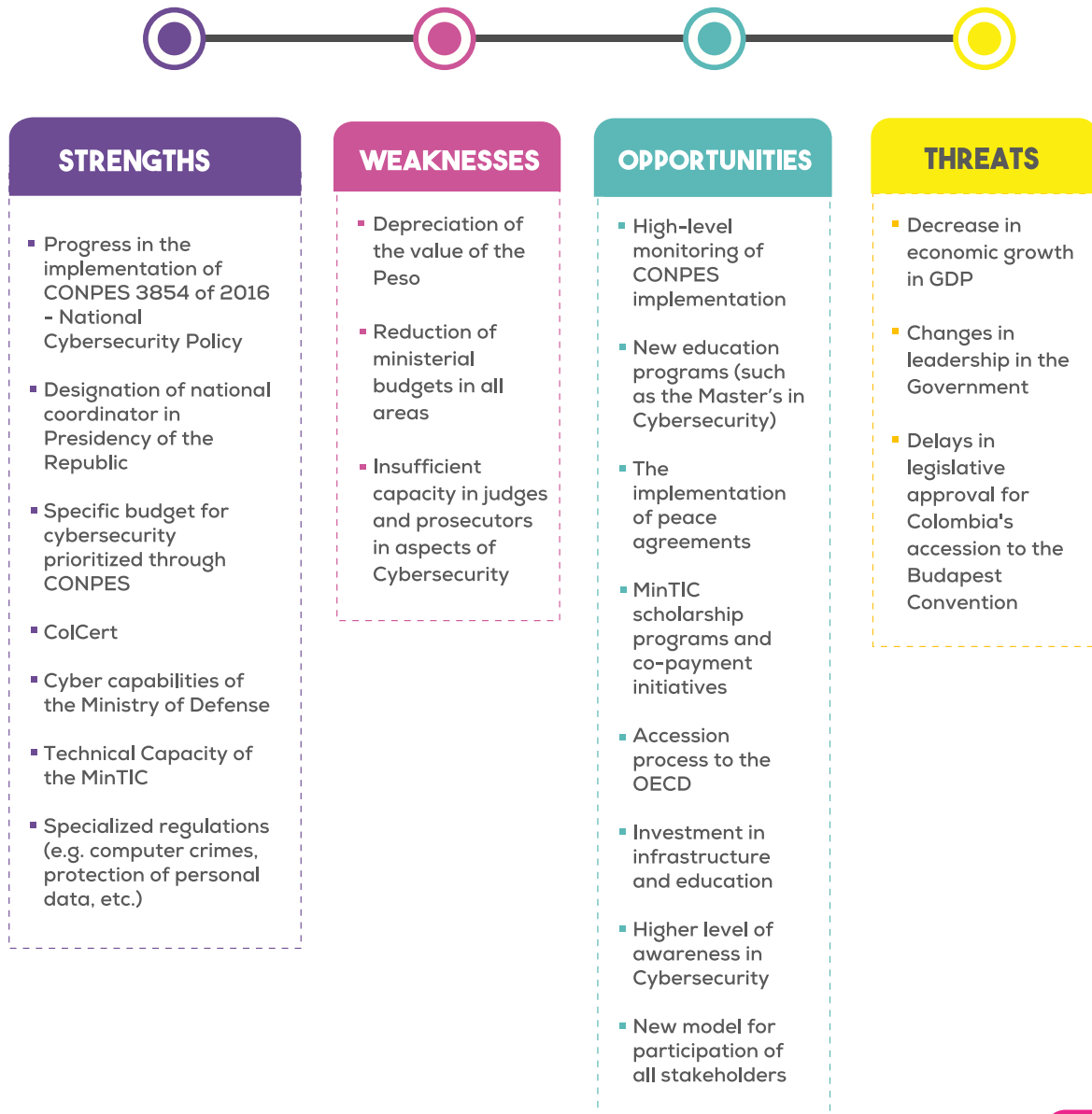
control that could be classified according to strengths and weaknesses. On the other hand, external factors are also identified (regardless of whether or not they are connected directly or indirectly), which can be presented as opportunities and threats. Some of the issues examined were:

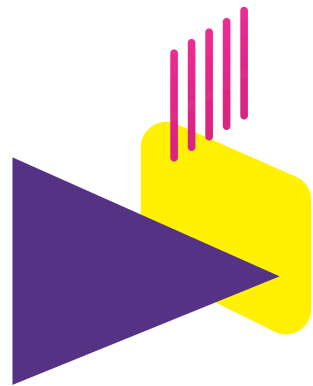
1. Strengths - What are the factors, from an internal perspective and from the point of view of external actors, which make the country strong in that area.
2. Weaknesses - From an internal and external basis, what do external stakeholders consider to be perceived weaknesses that could be avoided or improved.
3. Opportunities - Based on the strengths and weaknesses identified, what are the opportunities and can they help reduce or eliminate weaknesses.
4. Threats - What current external factors and obstacles are beyond country control and could threaten its success? Can economic considerations threaten the country's digital security position?

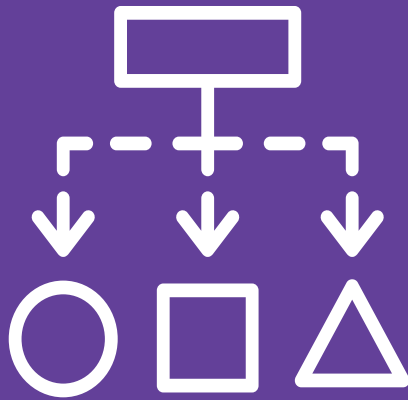
The advantage of the SWOT analysis is that its results can be taken into account in the ongoing planning and implementation of CONPES 3854, since it not only identifies the threats and weaknesses that affect the effectiveness of the digital security strategy, but also the opportunities and strengths that can be used to achieve success.



SWOT

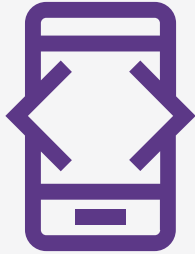






APPENDIX 2

METHODOLOGY



DEVELOPMENT OF THE INSTRUMENT

To gather information on the various digital incidents, two (2) types of instruments were developed for the following analysis: 1) Situational Analysis (style of the interview); and 2) Impact analysis (online).

The development process began with the research and review of various publicly available studies and reports on digital security and the impact analysis of cybercrime. Although several documents were reviewed, no attempt was made to summarize the applications of those studies. Overall, it was concluded that most of the available studies focused on the overall estimation of the economic impact of cybercrime and, to a lesser extent, on cyber incidents. These studies were carried out both at the transnational level with several countries involved and at the national level, but with a small sample of the various industries.

The instrument was developed over a period of six months and it involved several stages. The Pilot Phase was one of the Project's significant milestones as participants were asked to apply the instrument to their entities/institutions in the context of testing the applicability of the terms and definitions used, the understanding of the questions asked and the usability and logic of the online instrument.

With regard to Situational Analysis (Appendix 1), the results of the implementation tool developed by the OAS, the IDB and the Global Cybersecurity Capacity Centre, Oxford University were used as a reference point, summarized in the report "**Cybersecurity: Are We Ready in Latin America and the Caribbean?**", to develop a questionnaire that was completed by relevant stakeholders of the national government around five main areas: 1) Policy and Strategy; (2) Culture and Society; (3) Education; (4) Legal Frameworks; and (5) Technologies. The answers facilitated the analysis of the main strengths, weaknesses, opportunities and threats (SWOT analysis) for the country in terms of developing its digital security capabilities, as well as an update of the various dimensions and indicators.

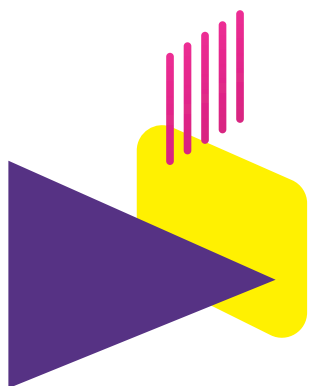
ANALYSIS OF RESPONSES

With the analysis of the responses of the public and private sector entities that participated in the instrument in Colombia, this study provides a summary of the estimated costs related to cyber incidents at the macro level and possible losses incurred. There were several factors and limitations that had to be taken into account. Many companies, for example, hide their losses while others do not have the skills to identify their losses. In addition, in the data collection methodology, namely, the use of an instrument, some of the results may not be accurate, because, since ranges were used for value estimates, the respondents selected the results and some of the answers were based on a perception of self, which some interviewees may distort. Therefore, the analysis of this study considered and took into account several factors in reaching its conclusions: 1) several economic sectors that are included; 2) size of sectors; 3) number of respondents; 4) variation between the interviewees who completed the instrument and those who

did not complete it; and 5) control factors, such as 'yes'/'no' to ensure that apples were measured with apples.

A total of 1,606 organizations started the instrument, but only a total of **1,098 respondents** (515 Companies and 583 public sector entities) completed the profile section. In response to how they learned about the instrument, 37% responded that it was through an official letter from the national government, 24% reported that it was through a national government website and 23% said it was another website. It was noted that 16% was informed as a result of the dissemination with industry associations and guilds. No quota was established by industry and company size (income), but rather a reasonable margin, and representative answers were obtained from companies of different sizes and economic sector.





APPENDIX 3

ANÁLISIS
ESTADÍSTICO
COMPLEMENTARIO



TABLE 7: ESTIMATION OF THE LIKELIHOOD THAT A COMPANY WILL IDENTIFY DIGITAL INCIDENTS (2016)

Estimation model: logit

Dependent variable: 1 if the company identifies digital incidents, 0 if it does not identify them.

VARIABLES	MARGINAL EFFECT (DY/DX)*	STANDARD ERROR	Z	P > Z	\bar{x}
Digital security budget	1.2e-10	9.01E-11	1.240	.215	1.47E+08
Number of employees	0.0003791	0.0001581	2.40	0.017**1	50.0771
Staff with internet access	-0.000852	0.0010589	-0.800	.421	64.31776
Sales	5.82E-163	.78E-15	0.15	0.877	2.03E+12
Foreign capital	0.0005361	0.0011843	0.45	0.6518	.418224
d_digital security positions	0.0801065	0.0603055	1.330	.1840	.4509346
d_technical measures	0.1329351	0.0622521	2.14	0.033**0	.4929907
d_digital security policies	-0.0211699	0.0632615-	0.33	0.738	0.6051402
d_standards	0.0451697	0.0686568	0.66	0.5110	.2429907
d_valuation of risk	0.1430716	0.0629847	2.27	0.023**0	.4252336
d_legislation	-0.0054669	0.0641935	-0.090	.932	0.2616822
d_industry	-0.0668821	0.1018324	-0.66	0.5110	.1121495
d_service	0.00679120	.067205	0.10	0.920	0.6775701
d_micro	-0.12042110	.0671351	-1.790	.073*	0.4182243
d_medium	0.0796988	0.0945996	0.84	0.400	0.1214953
d_large	-0.0621638	0.1070584	-0.580	.561	0.2242991

(*) the discrete change of the dummy variable from 0 to 1

Number of Observations = 428
 LR chi
 Prob > chi2 = 0.0000
 Log-Likelihood = -243.5582
 Pseudo R2 = 0.1542

***Significant variables at 1%

**Significant variables at 5%

*Significant variables at 10%

**TABLE 8: REGRESSION RESULTS –
NUMBER OF INCIDENTS (2016)**

Linear Regression Model

Dependent variable: logarithm of the number of incidents

VARIABLES	COEFFICIENT	ROBUST STANDARD ERROR	T	P > T
Digital security budget	5.42E-101	.74E-103	.110	.002***
Number of employees	0,00038520	,0006597	0.58	0.560
Staff with internet access	0,00111430	,0027034	0.41	0.680
Sales	-7.30E-155	.68E-15-	1.29	0.199
Foreign capital	-0,0037696	0,0041925	-0.900	.369
d_digital security positions	0,0649893	0,19196060	.340	.735
d_technical measures	0,5166059	0,1724034	3.00	0,003***
d_digital security policies	-0,0027982	0,1667429	-0.020	.987
d_standards	0,4788695	0,2640027	1.81	0,070*
d_valuation of risk	0,3383868	0,1761986	1.92	0,055*
d_legislation	0,20839570	,2382764	0.87	0.382
d_industry	0,0598495	0,40633260	.150	.883
d_service	0,0328707	0,21814840	.150	.880
d_micro	-0,2104846	0,1693744-	1.24	0.215
d_medium	0,21474670	,3611340	.590	.552
d_large	0,02505050	,379239	0.07	0.947

Number of Observations = 428

R² = 0.1712

***Significant variable at 1% **Significant variable at 5% *Significant variable at 10%



TABLE 9: REGRESSION RESULTS – COMPANY – ASSIGNED DIGITAL SECURITY BUDGET (2016)

Linear Regression Model

Dependent variable: Logarithm of the budget assigned by the company for digital security

VARIABLES	COEFFICIENT	STANDARD ERROR	T	P > T
Number of employees	0,0049112	0,0018714	2.62	0,009***
Staff with internet access	0,0079542	0,012715	0.63	0.532
Sales Logarithm	0,1399672	0,0567257	2.47	0,014**
Foreign capital	0,0108605	0,0143105	0.76	0.448
Logarithm of number of incidents	0,2919303	0,1823273	1.60	0.110
d_digital security positionsdigit	1.930772	0,7623268	2.53	0,012**
d_technical measures	2.061519	0,7886683	2.61	0,009***
d_digital security policies	1.603038	0,7658178	2.09	0,037**
d_standards	2.148676	0,8688742	2.47	0,014**
d_valuation of risk	2.151299	0,7983848	2.69	0,007***
d_legislation	0,8557661	0,7844744	1.09	0.276
d_industry	0,5255468	1.23481	0.43	671
d_service	1.502679	0,8042185	1.87	0,062*
d_micro	-1.597504	0,8421082	-1.90	0,059*
d_medium	0,5863965	1.216569	0.48	0.630
d_Jarge	0,7025586	1.345639	0.52	0.602

Number of Observations = 428
R2 = 0.4251

***Significant variable at 1% **Significant variable at 5% *Significant variable at 10%

TABLE 10: REGRESSION RESULTS – COST WITH DIGITAL INCIDENTS (2016)

Linear Regression Model

Dependent variable: cost with digital incidents

VARIABLES	COEFFICIENT	STANDARD ERROR	T	P > T
Number of incidents	531651	190266.32	.790	.008*

* Significant variable at 1%

Number of Observations = 42

R² = 0.1633

TABLE 11: ESTIMATION OF THE LIKELIHOOD THAT A PUBLIC ENTITY WILL IDENTIFY DIGITAL INCIDENTS (2016)

Estimation model: logit

Dependent variable: 1 if the entity identifies digital incidents, 0 if it does not identify them.

VARIABLES	MARGINAL EFFECT (DY/DX)*	STANDARD ERROR	Z	P > Z	\bar{x}
Digital security budget	8.01E-11	4.34E-11	1.85	0,065*	2.92E+08
Number of staff	0.0001993	0.0000785	2.54	0,011**	325.4097
Staff with Internet access	0.0047247	0.0016747	2.82	0,005***	72.07505
Investment budget	1.59E-15	3.91E-15	0.41	0.684	7.00E+11
_digital security positions	-0.0862007	0.0610058	-1.41	0.158	0.4381339
d_technical measures	0.1214568	0.056219	2.16	0,031**	0.4604462
d_digital security policies	0.0695837	0.0568544	1.22	0.221	0.6308316
d_standards	0.0745173	0.0743717	1.00	0.316	0.2636917
d_valuation of risk	0.151459	0.0608966	2.49	0,013**	0.3853955
d_legislation	0.1359538	0.0530307	2.56	0,010***	0.4685598
d_national	-0.146032	0.1024856	-1.42	0.154	0.356998
d_municipal	0.0074466	0.0947813	0.08	0.937	0.5557809

(*) dy/dx corresponds to the discrete change of the dummy variable from 0 to 1.

***Significant variables at 1%

**Significant variables at 5%

*Significant variables at 10%

Number of Observations = 493

LR chi

Prob > chi2 = 0.0000

Log-Likelihood = -298.91209

Pseudo R2 = 0.1247

**TABLE 12: REGRESSION RESULTS – BUDGET
ALLOCATED BY THE PUBLIC ENTITY FOR DIGITAL
SECURITY (2016)**

Linear Regression Model

Dependent variable: logarithm of the budget assigned by the public entity for digital security

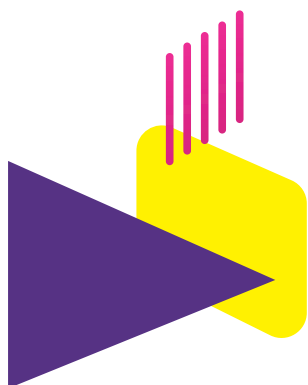
VARIABLES	COEFFICIENT	STANDARD ERROR	T	P > ITI
Number of staff	0,005017	0,0010813	4.64	0,000***
Staff with Internet access	0,0716088	0,020742	3.45	0,001***
Logarithm of the investment budget	0,1234978	0,0619476	1.99	0,047**
Logarithm of the number of incidents	0,0091293	0,1740777	0.05	0.958
d_digital security positions	1.588953	0,8025929	1.98	0,048**
d_technical measures	2.396737	0,767671	3.12	0,002***
d_digital security policies	1.120887	0,7730728	1.45	0.148
d_standards	1.984836	1.013148	1.96	0,051**
_valuation of riskrisk	0,7157857	0,8250376	0.87	0.386
d_legislation	0,6282294	0,73377	0.86	0.392
d_national	5.451329	1.356875	4.02	0,000***
d_municipal	1.14657	1.237875	0.93	0.355

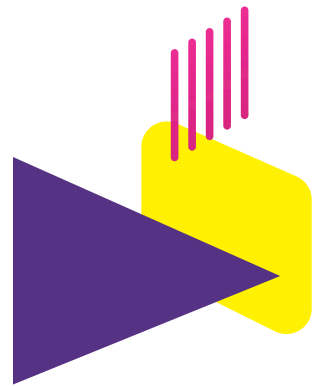
Number of Observations = 453
R2 = 0.4379

***Significant variable at 1%

**Significant variable at 5%

*Significant variable at 10%





IMPACT OF DIGITAL SECURITY INCIDENTS IN

COLOMBIA 2017



ISBN 978-0-8270-6675-5