



OAS | More rights
for more people



COMISIÓN NACIONAL
BANCARIA Y DE VALORES

THE STATE OF CYBERSECURITY IN THE **MEXICAN** FINANCIAL SYSTEM



THE STATE OF
CYBERSECURITY
IN THE **MEXICAN**
FINANCIAL
SYSTEM

COPYRIGHT © (2019) Organization of American States. All rights reserved under the International and Pan American Conventions. No portion of the content of this material may be reproduced or transmitted in any form, nor by any electronic or mechanical means, in whole or in part, without the express consent of the Organization.

Prepared and published by the Cybersecurity Program of the Inter-American Committee against Terrorism (cybersecurity@oas.org)

The contents expressed in this document are presented exclusively for informational purposes and do not represent the official opinion or position of the Organization of American States, its General Secretariat or its Member States.

THE STATE OF
CYBERSECURITY
IN THE **MEXICAN**
FINANCIAL
SYSTEM



OAS | More rights
for more people



COMISIÓN NACIONAL
BANCARIA Y DE VALORES

Luis Almagro

Secretary General

Organization of American States

Adalberto Palma Gómez

President

Comisión Nacional Bancaria y de Valores

Farah Diva Urrutia

Secretary of Multidimensional Security

Organization of American States

David Esaú López Campos

Technical Vice-president

Comisión Nacional Bancaria y de Valores

Alison August-Treppel

Executive Secretary

Inter-American Committee against Terrorism
Organization of American States

CNBV Technical Team

Elena Calatayud Hernando
Karla Mendoza Morales
Arturo Murillo Torres
Gerardo Hernández Sánchez
Ricardo Javier Jimenez Piña
Salvador Ayala Castro
Edgar Valdovinos González

OAS Technical Team

Belisario Contreras
Orlando Garcés
Jorge Bejarano
Kerry-Ann Barrett
Miguel Angel Cañada
David Moreno
Mariana Cardona
Diego Subero
Jaime Sources
Geraldine Vivanco
Barbara Marchiori
Gonzalo García-Belenguer



THE STATE OF
CYBERSECURITY
IN THE **MEXICAN**
FINANCIAL
SYSTEM

TABLE OF CONTENTS

1	Executive Summary	06
2	Prologue	11
3	Cybersecurity In The Mexican Financial System Entities And Institutions	15
3.1	Characterization of the Financial Entity/Institution	18
3.2	Digital Security Risk Management	24
3.3	Impact of Digital Security Incidents	55
4	Cybersecurity recommendations for the Mexican Financial System	70
4.1	For the Financial Entities and Institutions of the Mexican Financial System	70
4.2	For the Financial System Authorities and Regulatory Bodies and Law Enforcement Authorities of the Government of Mexico	74
5	Bibliography	76
Annex 1.	Information on the Sample of Entities and Institutions of the Mexican Financial System	77
Annex 2.	Comparative Analysis Between Sectors of the Mexican Financial System	80

EXECUTIVE SUMMARY

This study is a contribution by the General Secretariat of the Organization of American States (OAS), with the aim to provide reliable information on the State of Cybersecurity in the Mexican Financial System. This document is yet another effort by the OAS in its charge of strengthening the capacities and level of awareness of the growing threats to digital security in the Latin America and the Caribbean region.

The information in this study originates in a database of 240 financial entities and institutions in the Mexican Financial System¹. In order to conduct this analysis, the OAS designed, with the support of financial system experts, a targeted collection and information instrument. The main findings, based on that instrument, are presented below.

Significant findings about digital security in financial entities and institutions of the Mexican Financial System:

- In relation to digital security preparedness and governance, on average 58% of the financial entities and institutions in the country have one (1) hierarchical level between the CEO and the main person responsible for digital security. The number of hierarchical levels that exist between the CEO and the head of digital security (including aspects of information security, cybersecurity and fraud prevention using digital means) also depend on the size of the organization. In reference to the number of areas in charge of these issues, on average, there is one single area responsible for digital security in 70% of the entities of the commercial or multiple banking sector in Mexico, which is a similar percentage to that registered in the banks of the Latin American and Caribbean region, which is 74% (Organization of American States, 2018).
- Regarding the support to information security (including cybersecurity) risk management by the top management of the financial entity and institution, it is highlighted that 58% of the total of the financial entities and institutions in the country demonstrate this by promoting awareness, education and training, and 49% by *promoting information security plans*. Particularly, in the commercial or multiple banking sector in Mexico, it is highlighted that 73% of the total banking institutions in the country demonstrate this by *promoting information security plans* and 55% by

¹. The total assets of the participating financial entities and institutions are worth close to US\$682.4 billion (approximately 87% of the total assets of the analyzed sectors) and accumulate net profits of US\$7.15 billion (December 31, 2018). According to their size they are distributed as follows: 3% large entities, 22% medium-sized entities and 75% small entities; and according to establishment, they are: 78% private entities, 15% public entities and 6% mixed entities.

promoting awareness, education and training and assigning greater budget, while in the banking sector in Latin America and the Caribbean, it is more common to demand the *adoption of good security practices (65%), promotion of training and awareness in digital security (63%) and promotion of plans for digital security (60%)* (Organization of American States, 2018).

- In 50% of the Mexican financial entities and institutions, the Board of Directors receives periodic reports about risks in information security (including cybersecurity) and fraud using digital means, while 65% of those who answered the survey considers that getting the top management of the organization to invest in digital security solutions is moderately or very difficult, despite the relevance of investments, especially in terms of prevention and capacity building. In this same sense, when comparing the commercial or multiple banking sector of Mexico with the average of the Latin American and Caribbean region, it is observed that in this sector, in 85% of the banking entities, the Board receives periodic reports about risks in information security (including cybersecurity) and fraud using digital means, a figure higher than that reported in the region (72%) (Organization of American States, 2018).
- The security frameworks and/or international standards most implemented in financial entities and institutions are Information Security Management System (ISMS) - ISO/IEC 27001 and Information Technology Infrastructure Library (ITIL) & IT Service Management (ITSM) (in 27% and 15% of financial institutions, respectively).
- Regarding the formation of teams of professionals in information security (including cybersecurity) for each financial entity and institution in Mexico, it is observed that these comprise, on average, nine (9) members. However, this figure varies depending on entity size.
- It is highlighted that 68% of financial entities and institutions surveyed in the country consider

it appropriate for the team to grow in the short term, which is a recognition of the growing management needs in this aspect, which it is ultimately responsible for. These growing needs, in many cases, require outsourcing processes, and the activity that is most frequently hired refers to the *performance of security tests/vulnerability analysis*, with 34%, followed by the *monitoring of the security infrastructure*, with 31%.

- In terms of capabilities for detecting and analyzing information security (including cybersecurity) events, which are vital for the systematic management of this type of risk, percentages ranging between 75% and 85% of financial entities and institutions in the country focus on the implementation of firewalls and automated updates of antiviruses and systems. Topics such as the application of artificial intelligence and cognitive computing for the detection and analysis of security events are still very incipient, with levels lingering below 10% of the financial entities and institutions.
- The information security risks considered to deserve greater attention from Mexican financial entities and institutions, regardless of organization size, are: i) loss/theft of classified information assets (confidential or sensitive); ii) ransom for information; and iii) compromise of privileged user credentials.
- 100% of the Mexican financial entities and institutions state that they identified some kind of digital security event (successful attacks and unsuccessful attacks) against them. The most commonly identified digital security events during 2018 were: i) *malware* (56% of all entities); ii) phishing targeting the entity's access systems (47% of total entities); and iii) violation of clear desk policies (31% of all entities). It is highlighted that 19% of financial entities and institutions identify the occurrence of *malware* events on a daily basis.
- According to the Mexican financial entities and institutions, the type of digital security events

(successful attacks and unsuccessful attacks) used most frequently by cybercriminals against financial service clients (partners, associates or users) were: i) phishing, ii) spyware (*malware* or Trojans), and iii) social engineering. It is also important to note that the main motivators for carrying out these attacks are economic reasons (74%), and, to a lesser extent, political reasons, hacktivism, personal reputation as hackers and the theft of personal information.

- Regarding digital security incident management, response and recovery, at least one third of the financial entities and institutions in the country had management, response and recovery strategies for incidents in information security (including cybersecurity).

- As part of the digital security risk management strategies, 40% of financial entities, on average, perform maturity assessments under some information security methodology. Financial entities and institutions that fail to conduct this type of assessment note that the main reasons are: i) insufficient specialized staff (39% of entities not assessed), and ii) lack of budget allocation (28% of entities not assessed).

- Regarding the communication of digital security incidents, the majority (55% of financial institutions) offers a mechanism for their internal users (employees and contractors) to report digital security incidents (successful attacks) and 41% have a communications plan that allows them to inform their financial service customers when their personal information has been compromised. 44% of financial institutions report the attacks to a law enforcement authority in Mexico.

- In terms of training and awareness, 57% of financial entities and institutions have preparedness, response and training plans on information security (including cybersecurity) matters for their collaborators, which are conducted mostly annually. The most effective mechanism that has spawned greater awareness

in financial institutions regarding digital security risks is the use of the internal communication media and the development of internal training.

- On average, the return on investment in information security (including cybersecurity) and fraud prevention using digital means is approximately 10.94%, which most believe is a high return.

- With the values obtained from the study, it is estimated that the total annual cost of response and recovery from digital security incidents against Mexican financial entities and institutions in 2018 was approximately US\$107 million.

Table 1. Main Results by Size of Financial Entity/Institution of the Mexican Financial System

LARGE FINANCIAL ENTITIES AND INSTITUTIONS	MEDIUM-SIZED FINANCIAL ENTITIES AND INSTITUTIONS	SMALL FINANCIAL ENTITIES AND INSTITUTIONS
In 57% there is one single area responsible for digital security	In 53% there is one single area responsible for digital security	In 76% there is one single area responsible for digital security
In 50% there are two (2) hierarchical levels between the CEO and the head of digital security	In 54% there is one (1) hierarchical level between the CEO and the head of digital security	In 60% there is one (1) hierarchical level between the CEO and the head of digital security
Most large entities (29%) have a team consisting of 121-300 members	The majority of the medium-sized entities (75%) has a team consisting of 1-5 members	Most small entities (93%) have a team consisting of 1-5 members
They are subject to attacks of all kinds of digital security events, highlighting the identification of almost all, by the majority in the country	They are subject to attacks of all kinds of digital security events, highlighting the identification of some, by the majority in the country	They are subject to attacks of some types of digital security events, highlighting the identification of few, by the majority in the country
43% identifies the occurrence of <i>malware</i> events daily	24% identify occurrence of <i>malware</i> events daily	14% identifies occurrence of <i>malware</i> events daily
The majority (71%) detects 61% - 80% of events with their own systems	The majority (43%) detects 0% - 20% of events with their own systems	The majority (58%) detects 0% - 20% of events with their own systems
43% says they have been victims of successful attacks	15% says they have been victims of successful attacks	6% says they have been victims of successful attacks
43% conducts a maturity assessment and perform the corresponding actions	30% performs maturity assessment and performs the corresponding actions	19% performs a maturity assessment and performs the corresponding actions
86% offers a mechanism for their clients to report incidents to the entity (successful attacks)	40% offers a mechanism for their clients to report incidents to the entity (successful attacks)	36% offers a mechanism for their clients to report incidents to the entity (successful attacks)
100% has a communications plan to inform their financial services clients when their personal information has been compromised	34% has a communications plan to inform their financial services clients when their personal information has been compromised	41% has a communications plan to inform their financial services clients when their personal information has been compromised
71% reports incidents to law enforcement authorities in Mexico	64% reports incidents to law enforcement authorities in Mexico	37% reports incidents to law enforcement authorities in Mexico
20% states that the digital security budget is equivalent on average to less than 1% of EBITDA of the previous fiscal year	47% states that the digital security budget is equivalent on average to less than 1% of EBITDA of the previous fiscal year	55% states that the digital security budget is equivalent on average to less than 1% of EBITDA of the previous fiscal year

LARGE FINANCIAL ENTITIES AND INSTITUTIONS	MEDIUM-SIZED FINANCIAL ENTITIES AND INSTITUTIONS	SMALL FINANCIAL ENTITIES AND INSTITUTIONS
The budget allocated to digital security is equivalent to approx. 2.30% of EBITDA of the previous year	The budget allocated to digital security is equivalent to approx. 2.51% of EBITDA of the previous year	The budget allocated to digital security is equivalent to approx. 2.04% of EBITDA of the immediately preceding year
In 57% the digital security budget increased compared to the immediately previous fiscal year	In 43% the digital security budget increased compared to the immediately previous fiscal year	In 35% the digital security budget increased compared to the immediately previous fiscal year
The budget allocated in 2018 to an average member of the digital security team is approximately US\$67,674	The budget allocated in 2018 to an average member of the digital security team is approximately US\$49,453	The budget allocated in 2018 to an average member of the digital security team is approximately US\$12,488
The return on investment in digital security is approximately 15.00%	Return on investment in digital security is approximately 9.58%	The return on investment in digital security is approximately 10.36%
100% states that the total cost of response and recovery from incidents is equivalent on average to less than 1% of EBITDA of the previous fiscal year	71% state that the total cost of response and recovery from incidents is equivalent on average to less than 1% of EBITDA of the previous fiscal year	59% states that the total cost of response and recovery from incidents is equivalent on average to less than 1% of EBITDA of the previous fiscal year
The total cost of response and recovery from digital security incidents per entity in 2017 is approx. 1.00% of EBITDA of the immediately previous year (US\$2,357,221 in 2018 approx.)	The total cost of response and recovery from digital security incidents per entity in 2017 is approx. 1.54% of EBITDA of the immediately previous year (US\$634,689 in 2018 approx.)	The total cost of response and recovery from digital security incidents per entity in 2017 is approx. 1.73% of EBITDA of the immediately previous year (US\$317,615 in 2018 approx.)

The detail of the study can be consulted in section 3 of this document.

PROLOGUE




Luis Almagro
Secretary General
**Organization of
American States**



OAS | More rights
for more people

The General Secretariat of the Organization of American States (OAS), through the Cybersecurity Program attached to the Secretariat of the Inter-American Committee against Terrorism (CICTE), promotes and coordinates cooperation between OAS Member States, and among them, the Inter-American System and other organizations in the international system. The purpose is to access, prevent, confront, and respond effectively to threats to security, and therefore be the main point of reference in the Hemisphere to develop cooperation and capacity building in the OAS Member States.

The financial sector has shown very high digitization rates in comparison to other sectors. Every day more clients in the financial sector use non-physical means to carry out their operations, conduct transactions over the Internet or make payments through mobile devices. The adaptation of new business models and leveraging of digital channels intend to make the most of technologies, but this intention is countered by the emergence of new risks that must be prevented in order to mitigate potential attacks and fraud situations to which the sector and, of course, its users are currently exposed.



The purpose of this OAS study is to present the results and analysis of incidents in information security (including aspects of cybersecurity and fraud prevention using digital means) that emerged after conducting the corresponding surveys within various financial entities and institutions of the Mexican Financial System. This document structures a study on the state of Cybersecurity in the Mexican Financial System.

The study was supported on an information-collection instrument that was divided into three (3) sections. The first section offers information on the profiles of the characteristics of financial entities and institutions; the second refers to aspects associated with digital security risk management; and the third deals with aspects relating to how the incidents impact them. The instrument was applied to financial entities and institutions, which delivered information that enabled a better understanding of their management of digital security risks and impact.

The OAS is grateful to the *Comisión Nacional Bancaria y de Valores* (National Banking and Securities Commission) for the support and facilities provided in contacting the entities of the different sectors that participated filling out the instrument. The *Comisión* also provided contributions and comments for the definition and focus of the instrument content, adjusting it to the current environment of the Mexican Financial System. The contributions provided by the Mexican financial institutions, as well as the support of the CNBV, were vital for the technical team of the OAS to prepare this final report.

Based on the foregoing and the research grounded on the references addressed in the study, we aim to offer relevant conclusions and recommendations to the Mexican Financial System, as well as to the financial system regulatory authorities and bodies, and law enforcement authorities of the Government of Mexico. The purpose is to have a more reliable and secure digital environment for the services offered by this vital sector for that country.



Adalberto Palma Gómez

President
**National Banking and
Securities Commission**



COMISIÓN NACIONAL
BANCARIA Y DE VALORES

The mission of the National Banking and Securities Commission (Comisión Nacional Bancaria y de Valores - CNBV) is the supervision and regulation of the entities that make up the financial system in Mexico, in order to ensure the system's stability and proper functioning, as well as to maintain and promote its healthy and stable development, protecting the interests of the users.

A risk for the stability of financial systems worldwide is currently represented by cyber threats, increasingly organized, frequent, disruptive and with a broader scope; and their motivations range from economic, political (hactivism) to personal.

In this environment, and seeking to realize its mission, the CNBV endeavors to promote a financial system that is better prepared and more resilient in the face of cyber-attacks. Its incessant work centers on the updating of regulatory requirements applicable to the entities supervised, on the improvement of cybersecurity policies, controls, processes and culture, as well as the supervision of information security.


The financial industry and the Government sector have historically been among the most attacked, and costs are rising.

The human factor is still one of the weak links: 64% of the organizations in the United States said they had suffered successful Phishing² events and have declared to be vulnerable to new technologies (Cloud, IoT) and threats, particularly of ransomware.

In the past two years, attacks to financial entities in Mexico have focused on payment infrastructures and ATMs much more frequently, resulting in substantial losses.

The Organization of American States (OAS), through the Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE),

².CheckPoint 2018 Security Report



has conducted an analysis of the cybersecurity situation in Mexico, which assisted the Presidency of the Republic in the launch of the National Cybersecurity Strategy (ENC) in 2017.

In January 2018, CICTE reached out to us for support in asking the banks to participate in the “Study on Cybersecurity in the Banking Sector in Latin America and the Caribbean,” conducted by the OAS using an online questionnaire. The request was answered by 35 of the 51 banks in Mexico.

The need to have more in-depth understanding of the particular situation in Mexico urged the OAS to start a new survey in 2018, targeting financial entities, involving relevant sectors, in addition to credit institutions, such as savings and loan cooperatives, popular financial corporations, credit unions, brokerage houses and FINTECH companies.

The information contained in this report as a result of said survey, as well as the data disaggregated by sector, will be very useful to broadly identify opportunity areas and sectors to guide the CNBV efforts, with the aim of using the resources efficiently while it performs its duties of information security supervision and regulation.

The CNBV acknowledges and appreciates the OAS undertakings in recent years, the results of which enrich the functions of this Commission.



CYBERSECURITY IN THE MEXICAN FINANCIAL SYSTEM ENTITIES AND INSTITUTIONS

According to the World Economic Forum's Global Risks Report 2019, large-scale cyber-attacks and the breakdown of networks and essential information infrastructure (collapse of the essential information infrastructure) are considered technological risks on a world scale which, should they occur, can have a significant negative impact on several countries and industries within the next ten years. "Technology continues to play a profound role in shaping the global risk landscape" for individuals, governments and companies. In the GRPS, "fraud and massive data theft" ranks fourth on global risk for probability, in a 10-year term, with "cyber-attacks" ranking fifth. This keeps a pattern that was registered last year, with the consolidation of the cyber risks position, together with the environmental risks in the high impact and high probability quadrant of the global risk scenario." (WEF, 2019).

These risks are currently managed by highly-digitized segments such as the financial sector which, in turn, faces major structural challenges amid solid digital transformation processes. Cybersecurity is therefore a critical aspect today, and financial entities and institutions must be prepared for unprecedented attacks that not only intend to secure their economic resources—and those of their clients (partners, associates or users)—but also, and gradually more, information about them.

Honing in on this sector, the Mexican Financial System envelops the following: i) financial system authorities and regulatory bodies, ii) financial entities and institutions from various sectors that provide services to different segments of the population, and iii) financial instruments (financial assets) and markets.

On the one hand, the Mexican Financial System authorities and regulatory bodies are public institutions that ensure the stability and development of the financial system and perform authorization, regulation, supervision and sanction functions, among others, on the various sectors and entities and institutions that make up said system, as well as the individuals and legal entities that conduct activities provided in the laws relative to it.

Figure 1. Mexican Financial System Authorities



Source: GS/OAS, based on information collected from CNBV

This is the list of the authorities and organizations that currently make up this system in Mexico:

- *Secretaría de Hacienda y Crédito Público (SHCP)* - Ministry of Finance and Public Credit: Its mission is to propose, direct and control the Federal Government's policy on financial, fiscal, expenditure, revenue and public debt, with the purpose of consolidating a country, with quality, equitable, inclusive and sustained economic growth, strengthening the well-being of Mexicans.
- *Comisión Nacional Bancaria y de Valores (CNBV)* - National Banking and Securities Commission: It is a decentralized body of the SHCP, with powers of authorization, regulation, supervision and sanction on the various sectors and entities that make up the Mexican Financial System, as well as on individuals and legal entities that carry out activities foreseen in the laws related to the financial system.
- *Comisión Nacional de Seguros y Fianzas (CNSF)* - National Insurance and Bonding Commission: It is a decentralized body of the SHCP, in charge of supervising that the operation of the insurance and surety sectors comply with the regulatory framework, preserving the solvency and financial stability of the insurance and surety institutions, to guarantee the interests of the user public, as well as to promote the healthy development of these sectors with the purpose of extending the coverage of their services to as much of the population as possible.
- *Comisión Nacional de Sistemas de Ahorro para el Retiro (CONSAR)* - National Commission of Savings Systems for Retirement: Its main task is to regulate the Retirement Savings System (SAR) which gathers the individual accounts in the name of the workers who manage the Administradoras

de Fondos para el Retiro (AFORE) - Funds Administrator for Retirement.

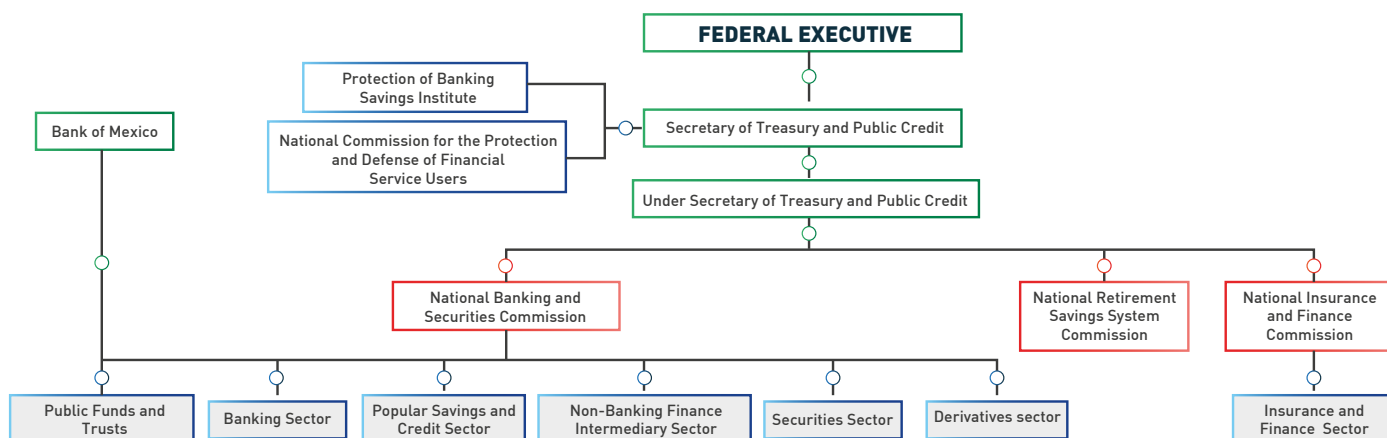
- *Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF)* - National Commission for the Protection and Defense of Financial Services Users: It is a public institution under the Ministry of Finance and Public Credit, which defends and promotes the rights and interests of Mexicans as users of financial products and services, besides promoting financial education.

- *Instituto para la Protección al Ahorro Bancario (IPAB)* - Institute for the Protection of Bank Savings: It is the institution of the Federal Government in charge of administering the Bank Deposit Insurance for the benefit and protection of Mexican savers.

- *Servicio de Administración Tributaria (SAT)* - Tax Administration Service: It is a decentralized body under the SHCP, to carry out specific tasks in order to apply the tax and customs legislation to the country's natural and legal persons.

On the other hand, financial entities and institutions capture, manage and channel financial resources and direct Mexicans' savings and investment in various sectors such as: banking sector, the popular savings and credit sector, the non-banking financial intermediaries' sector, the securities market, among others.

Figure 2. Sectors of the Mexican Financial System



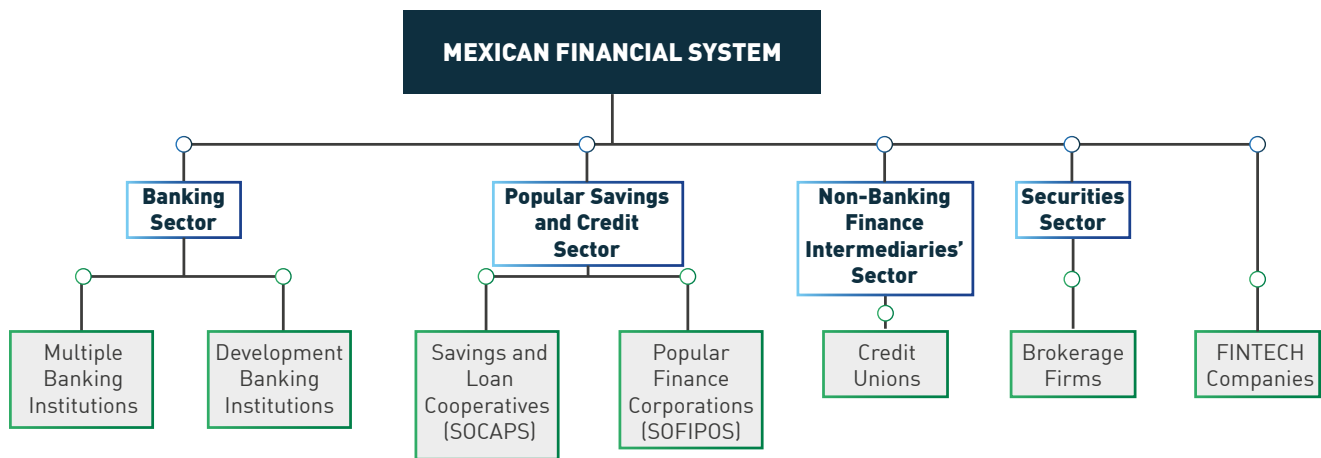
Source: GS/OAS based on information collected from CNBV

Below are the financial entities and institutions of the Mexican Financial System considered for this report:

- Multiple Banking Institutions (Banking Sector)
- Development Banking Institutions (Banking Sector)
- Savings and Loan Cooperatives, SOCAP (Popular Savings and Credit Sector)
- Popular Financial Companies, SOFIPO (Popular Savings and Credit Sector)
- Credit Unions (Non-Banking Financial Intermediaries' Sector)
- Brokerages Firms (Securities Sector)
- FINTECH companies³

³. This report includes this type of financial entity and institution, considering that the CNBV authorizes, regulates and supervises the financial technology institutions (ITF) created by the *Law to Regulate Financial Technology Institutions and reforms, adds or repeals provisions of various financial laws*, approved by Congress and the Decree and published in the Official Gazette on March 9, 2018 (FINTECH Law).

Figure 3. Sample of the entities and institutions of the Mexican Financial System for the preparation of the report



Source: GS/OAS based on information collected from CNBV

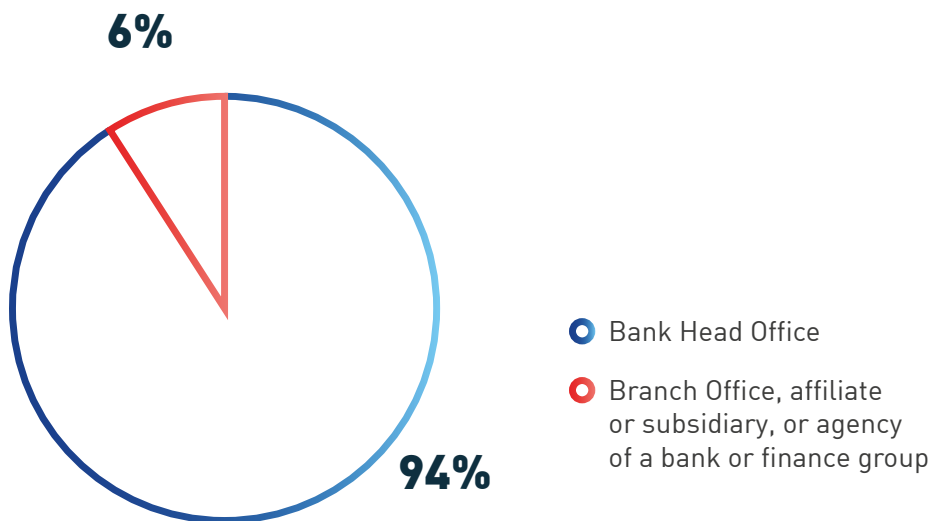
3.1. Characterization of the Financial Entity/Institution

Out of a total of 282 responses received during the publication period of the information collection instrument (months in the fourth quarter of 2018), a database was established with records of 240 financial entities and institutions covering the thirty-two (32) Mexican states. It is estimated that the sample of financial entities and institutions included in the results of this study reaches assets of US\$682.4 billion and net profits of US\$7.1 billion as of December 31, 2018.

The instrument's questions were designed to be answered by the financial entity/institution employing the respondent officer locally (ie, in the entity operating in the country), even if the financial entity/institution was: i) the parent company of the financial entity/institution or a financial group, or ii) a branch, affiliate or subsidiary, representative office or agency of the financial entity/institution or a financial group. For clarification purposes, each question specified the scope of application in detail.

It was seen that 94% of the financial entities and institutions interviewed were a parent company of the financial entity and institution or a financial group, while 6% correspond to a branch, affiliate or subsidiary, representation office or agency of the financial entity and institution or of a financial group.

Figure 4. Parent Company or Branch, Subsidiary, Representation Office or Agency of the Financial Entity/Institution or a Financial Group



Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

In order to classify Mexican financial entities and institutions by size, the methodology in the 2014 study by the Inter-American Development Bank (IDB) and the Latin American Bank Federation (FELABAN) (IDB & FELABAN, 2014) was considered. This was also used by the Organization of American States (OAS) in the “State of Cybersecurity in the Banking Sector in Latin America and the Caribbean” study, published in 2018 (Organization of American States, 2018), which considers a small entity as one having less than 300 employees, or more than 300 employees, but with up to 10 branches; a medium-sized entity is one with 301 - 5,000 employees and 11 - 150 branches; and a large entity as one that has more than 150 branches.

Below is the classification of the 240 financial entities and institutions, with the number of employees and branches of the entity hiring the official who filled out the questionnaire (in the federal state where the official was located). For example, it shows that 84 financial entities and institutions out of the total sample have less than 300 employees and have up to 10 branches, and that 4 entities have more than 5,000 employees, with more than 151 branches.

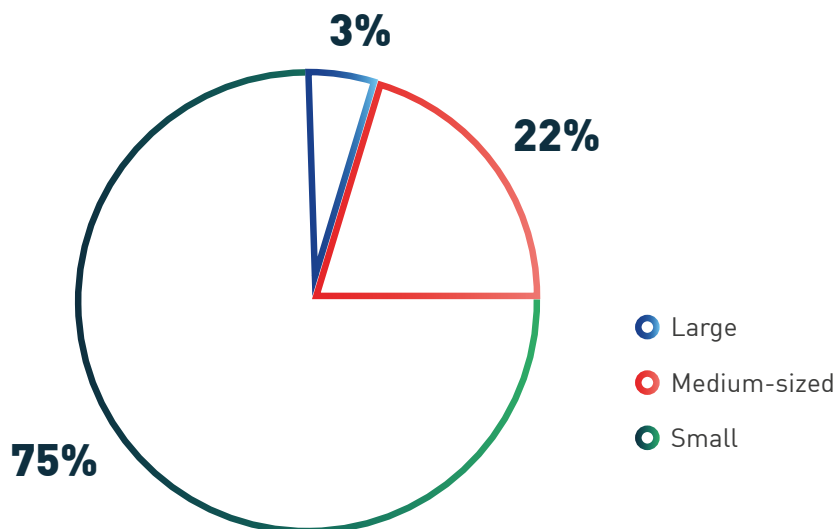
Table 2. Distribution of Financial Entities and Institutions by Number of Employees and Branches

Number of Employees	Number of Branches					
	No. of branches	Up to 10 branches	11 - 50 branches	51 - 150 branches	More than 151 branches	Total
Up to 300 employees	89	84	23	2		198
301 - 999 employees	2	5	11	3		21
1,000 - 4,999 employees	3	1	6	4	2	16
More than 5,000 employees			1		4	5
TOTAL	94	90	41	9	6	240

Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

With the above information, financial entities and institutions are classified by size: 75% of the sample is considered to be small entities, 22% to be medium-sized entities and 3% to be large entities. This classification is paramount since all the analysis, conclusions and recommendations regarding the management of digital security risks and the impact of digital security incidents in this chapter take into account organization size.

Figure 5. Distribution of Financial Entities and Institutions by Size (Large, Medium-sized and Small)



Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

It can be seen that 47% of the financial entities and institutions interviewed provide services in the popular savings and credit sector (SOCAP and SOFIPO), 25% provides services in the non-banking financial intermediaries' sector, 18% provides services in the banking sector (commercial or multiple banking and development banking), 7% provides services in the FINTECH sector and 4% provides services in the securities sector.

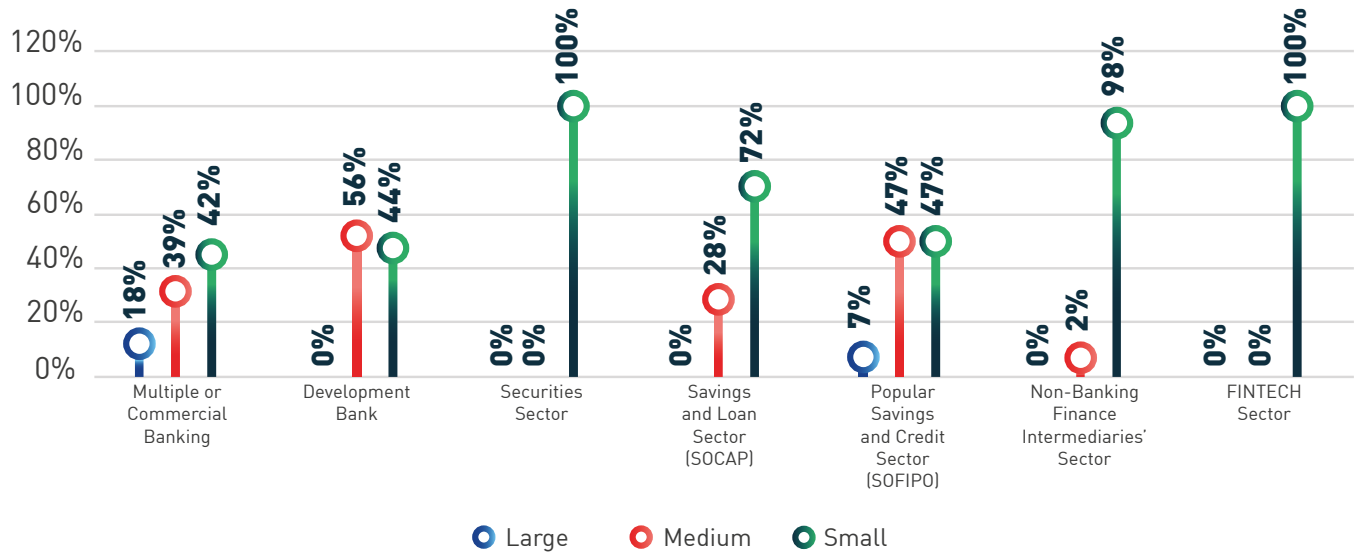
Table 3. Distribution of Financial Entities and Institutions by Type of Actor

	Large	Medium	Small	Total	%
Commercial or Multiple Banking	6	13	14	33	14%
Development Banking		5	4	9	4%
Securities Sector			9	9	4%
Popular Savings and Credit Sector (SOCAP)		27	71	98	41%
Popular Savings and Credit Sector (SOFIPO)	1	7	7	15	6%
Non-Banking Financial Intermediaries' Sector		1	58	59	25%
FINTECH Sector			17	17	7%
MEXICAN FINANCIAL SYSTEM	7	53	180	240	100%

Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

When analyzing by entity size, and by sector type, it is apparent that the three (3) size categories (large, medium-sized and small) are represented for commercial or multiple banks and for popular financial corporations (SOFIPOs). On the other hand, there is representation of medium-sized and small entities for development banks, cooperative savings and loan companies (SOCAPs) and credit unions. Lastly, the sample had responses from small brokerage firms and small FINTECH companies.

Figure 6. Type of Actor in the Sample of the Mexican Financial System




Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

From the total of the sample, it is estimated that the financial entities and institutions surveyed provide their services to more than 46 million financial service clients (partners, associates or users) in the country. It is highlighted that 78% of said clients are users of commercial or multiple banking services.

Table 4. Distribution of Financial Service Clients (Partners, Associates or Users) of the Sample

	Large	Medium	Small	Total
Commercial or Multiple Banking	26,500,000	9,528,000	59,500	36,087,500
Development Banking		4,807,000	20,000	4,827,000
Securities Sector			74,500	74,500
Popular Savings and Credit Sector (SOCAP)		2,328,000	1,821,500	4,149,500
Popular Savings and Credit Sector (SOFIPO)	500,000	475,000	15,500	990,500
Non-Banking Financial Intermediaries' Sector		1,000	76,500	77,500
FINTECH Sector			169,500	169,500
MEXICAN FINANCIAL SYSTEM	27,000,000	17,139,000	2,237,000	46,376,000

Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions



Taking into account the type of capital of the financial entity and institution hiring the employee who answered the survey, it can be seen that 78% of the total of the sample are private financial entities and institutions (100% private capital), 15% are public financial entities and institutions (100% public capital) and 6% are mixed financial entities and institutions (containing public and private capital).

When analyzing by size, 100% of large financial entities and institutions are private financial entities and institutions while only 17% of medium-sized financial entities and institutions are public. Similarly, while 14% of large financial entities and institutions are mixed capital, only 6% of the medium-sized and 6% of small financial entities and institutions have both public and private capital.

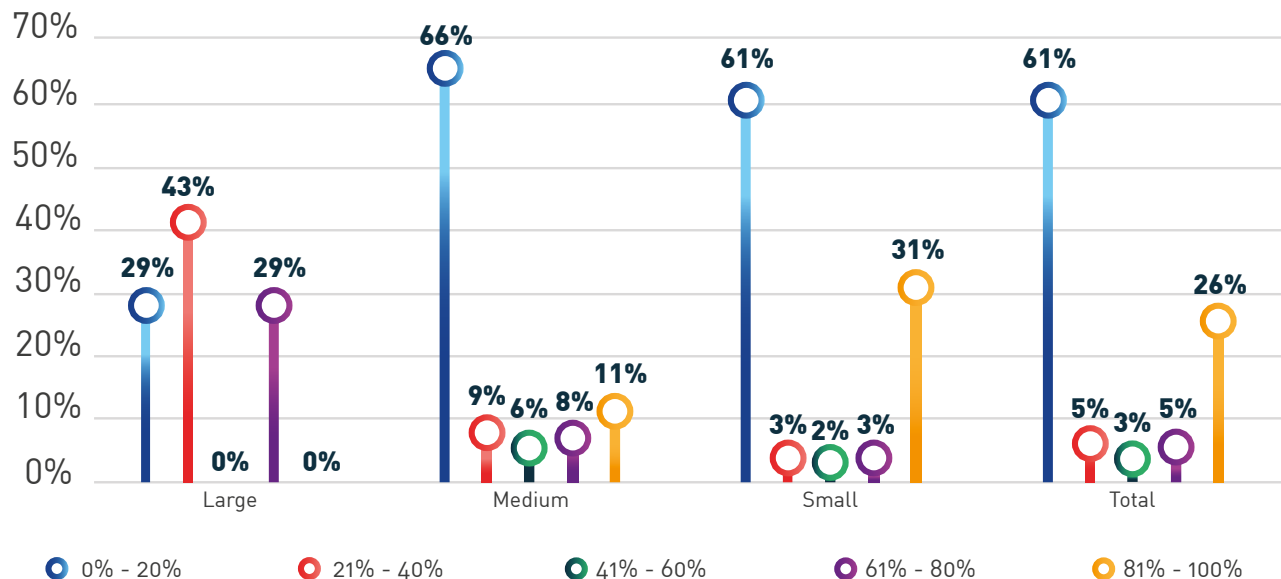
In addition, 95% of the financial entities and institutions interviewed showed that they contain a majority of national share capital, while only 5% contain a majority of foreign capital.

When analyzing the percentage of operations performed in the financial institution/entity through non-face-to-face transactional channels (Internet, electronic transactions, ATMs, automatic payments, mobile applications and interactive voice response -IVR), of the entity's total 2018 operations, it can be seen that 61% of the financial entities and institutions in the sample have between 0% and 20% of their operations through non-face-to-face transactional channels.

When analyzing the financial entities and institutions by size, it can be seen, for example, that more than 60% of both medium-sized and small entities carry out 0% - 20% of their operations through non-face-to-face transactional channels while 29% of large entities perform operations in that range. It is important to note that in sectors such as FINTECH, an average of 76% of financial entities and institutions perform between 81% and 100% of their operations through non-face-to-face transactional channels. It is also observed that in the same range of operations, 21% of commercial or multiple banking sector institutions conduct their operations through non-face-to-face transactional channels⁴, which doubles the average registered by banking entities in Latin America and the Caribbean, which is 10% (Organization of American States, 2018).

⁴. Figure 34 of Annex 2 presents the comparison of the result of *Percentage of transactions carried out through non-face-to-face transactional channels* between the different sectors analyzed in the Mexican Financial System.

Figure 7. Percentage of Operations Carried Out Through Non-Face-To-Face Transactional Channels



Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

3.2. Digital Security Risk Management

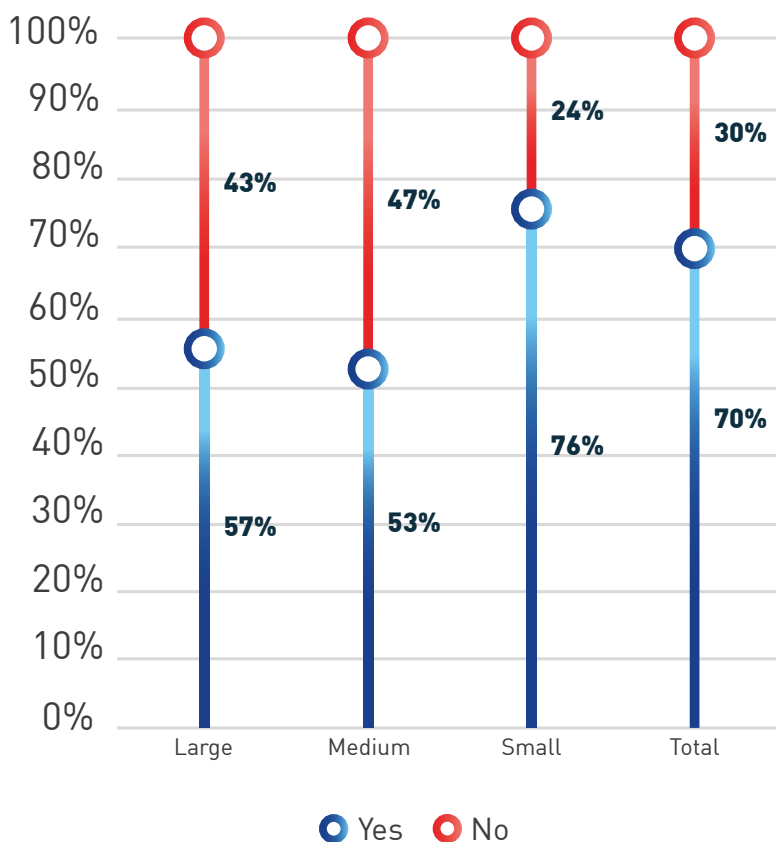
As part of this study, a series of questions were posed regarding digital security risk management. These questions were formulated with the purpose of evaluating the main aspects and issues related to the following topics:

- Preparedness and Governance
- Detection and Analysis of Digital Security Events
- Management, Response and Recovery from Digital Security Incidents
- Reports of Digital Security Incidents
- Training and Awareness

3.2.1. Preparedness and Governance

The majority of the financial entities and institutions interviewed (70%) mention that there is one single area in their organization responsible for information security (including cybersecurity) and fraud prevention using digital means. It is worth noting that as the financial entity and institution grows, the areas responsible for digital security increase, since 76% of small entities have one single area compared to 57% of large entities.

Figure 8. Single Area Responsible for Digital Security in the Financial Entity/Institution



Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

These differences are further accentuated in sectors such as non-banking financial intermediaries where it is evident that in 90% of the financial entities and institutions there is one single area responsible for information security (including cybersecurity) and fraud prevention using digital means⁵. In addition, in 60% of the financial entities and institutions of the Mexican banking sector (commercial or multiple banking and development banking) there is one single responsible area, while in the Latin American and Caribbean region, the banking entities register an average of 74% (Organization of American States, 2018).

With the premise that the CEO of the financial entity/institution is considered the head of the entity, and based on the results obtained, it is concluded that the hierarchical levels that exist between the CEO and the head of information security (including cybersecurity) and fraud prevention occurring through

digital means also depend on the organization size in the country. For example, in 60% of small entities, the head of the department reports directly to the CEO, that is, it is one (1) single level under the CEO, while large entities do not show this organization model. In 50% of large entities there are two (2) levels between the CEO and the head of digital security. As the entity grows, the number of hierarchical levels separating the CEO and the person responsible for digital security increases.

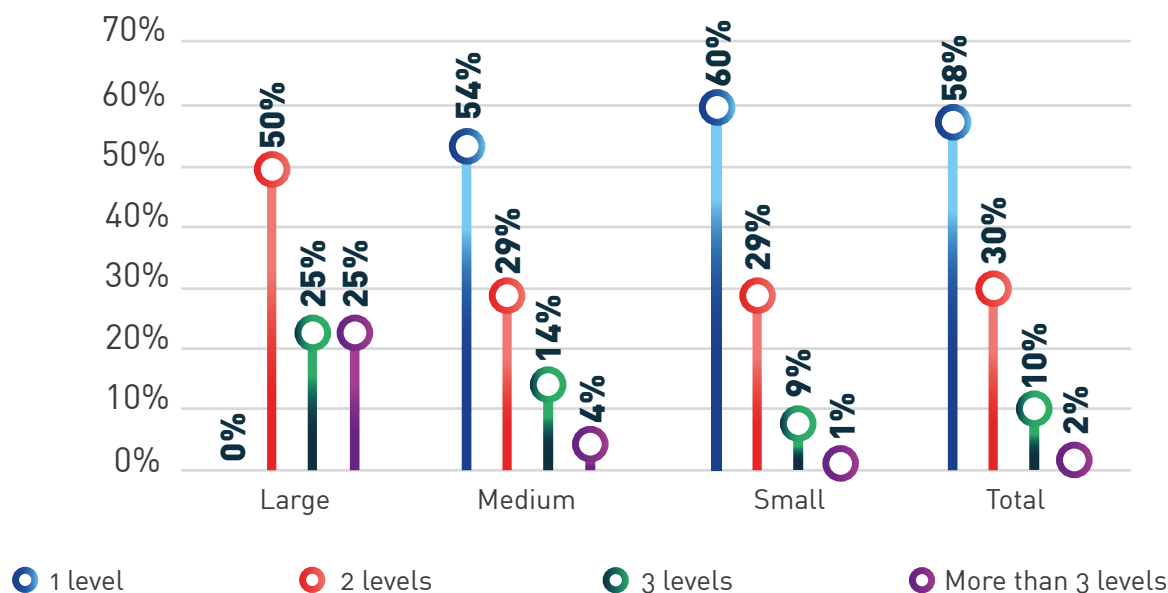
When analyzing the complete sample, it can be seen that in 58% of financial entities and institutions there is one (1) hierarchical level between the CEO and the head of digital security⁶.

When comparing the Mexican banking sector (commercial or multiple banking and development banking) to the average in the Latin America and the Caribbean region, it is observed that in this sector, 33% of small banks report directly to the CEO, while the region registers an average of 46% of small banks, where the head of digital security reports directly to the CEO (Organization of American States, 2018).

⁵ Figure 35 of Annex 2 presents the comparison of the result: *Single area responsible for digital security in the financial entity/institution* between the different sectors analyzed in the Mexican Financial System.

⁶ Figure 36 of Annex 2 presents the comparison of the result: *Number of hierarchical levels between the CEO and the head of digital security* between the different sectors analyzed in the Mexican Financial System.

Figure 9. Number of Hierarchical Levels Between the CEO and the Head of Digital Security



Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

In the Mexican Financial System, the most common denomination of the position held by the head of information security (including cybersecurity) is the *Chief Information Security Officer (CISO)*, which is the same for large financial entities and institutions (42%). For its part, the *IT Manager (ITM)* position is also common for medium-sized entities (17%) and for small entities (19%). However, within the Mexican banking sector (commercial or multiple banking and development banking), as well as in the banking sector of the Latin America and the Caribbean region, the most common position held by the head of digital security (including aspects of information security, cybersecurity and fraud prevention using digital means) is an *Information Security Officer (ISO)* (Organization of American States, 2018).

An important aspect regarding digital security preparedness and governance is the outsourcing of activities related to information security (including cybersecurity) and fraud prevention using digital means by the organization. On average and regardless of financial entity/institution size, the most outsourced services of the organization are: *Security Tests/Vulnerability Analysis* (34% of the total), *Security Infrastructure Monitoring* (31% of the total), *regulatory compliance management* (18%) and *Cloud Security Services* (18% of the total).

It is highlighted that in the Mexican banking sector (commercial or multiple banking and development banking), the outsourcing of *Security Testing/Vulnerability Analysis* activities reaches 76%, coinciding with what is registered in the Latin America and Caribbean region, where on average and without distinction by bank size, the most outsourced services by banking entities in the region are: *Security Tests* (65% of the total).

With respect to the size of the team that handles processes associated with information security (including cybersecurity) and fraud using digital means, it can be seen that, on average, one financial

entity and institution in Mexico has a team made up of nine (9) people. However, this value varies significantly depending on entity size and sector, because while in commercial banking the average is thirty-seven (37) professionals, in sectors such as popular savings and loans (SOCAP and SOFIPO) it is only three (3).

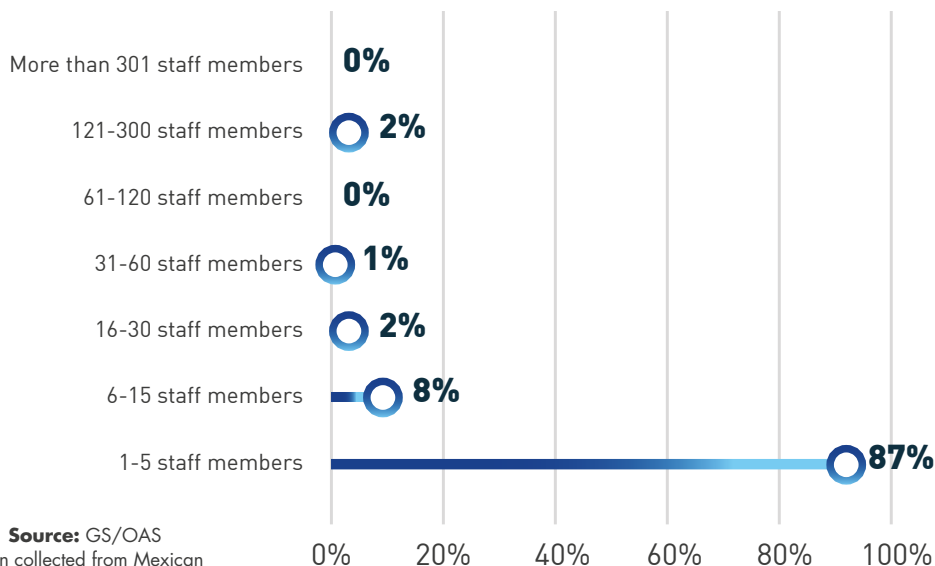
Table 5. Average of Information Security (Including Cybersecurity) Professionals by Sector and Size of Financial Entity/Institution in Mexico

	Large	Medium	Small	Total
Commercial or Multiple Banking	91	25	24	37
Development Banking		10	7	9
Securities Sector			36	36
Popular Savings and Credit Sector (SOCAP)		4	3	3
Popular Savings and Credit Sector (SOFIPO)	3	3	3	3
Non-Banking Financial Intermediaries' Sector		3	3	3
FINTECH Sector			4	4
MEXICAN FINANCIAL SYSTEM	79	9	7	9

Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

When estimating said personnel by financial entity/institution size, the following is obtained: a team of seventy-nine (79) people on average in a large entity, a team of nine (9) people on average in a medium-sized entity and a team of seven (7) people on average in a small entity.

Figure 10. People that Make Up the Total Teams that Handle Processes Associated with Information Security (Including Cybersecurity) and Fraud Using digital means



Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

It is noted that, in the banking sector in Latin America and the Caribbean, the average is forty-nine (49) people in a large bank, sixteen (16) people in a medium-sized bank and four (4) people in a small bank (Organization of American States, 2018).

Despite the presence of teams responsible for digital security in this type of organizations, 68% of Mexican financial entities and institutions considers it appropriate for this team to grow in the short term, while 82% of banking entities in the region of Latin America and the Caribbean thinks the same (Organization of American States, 2018). When analyzing by size, it is seen that 100% of the large entities, 89% of the medium-sized entities and 60% of the small entities considers that the size of the team should increase. It is also identified that the only sector that mostly considers that it is not appropriate for the team to grow in the short term (56%) is the non-banking financial intermediaries' sector.⁷

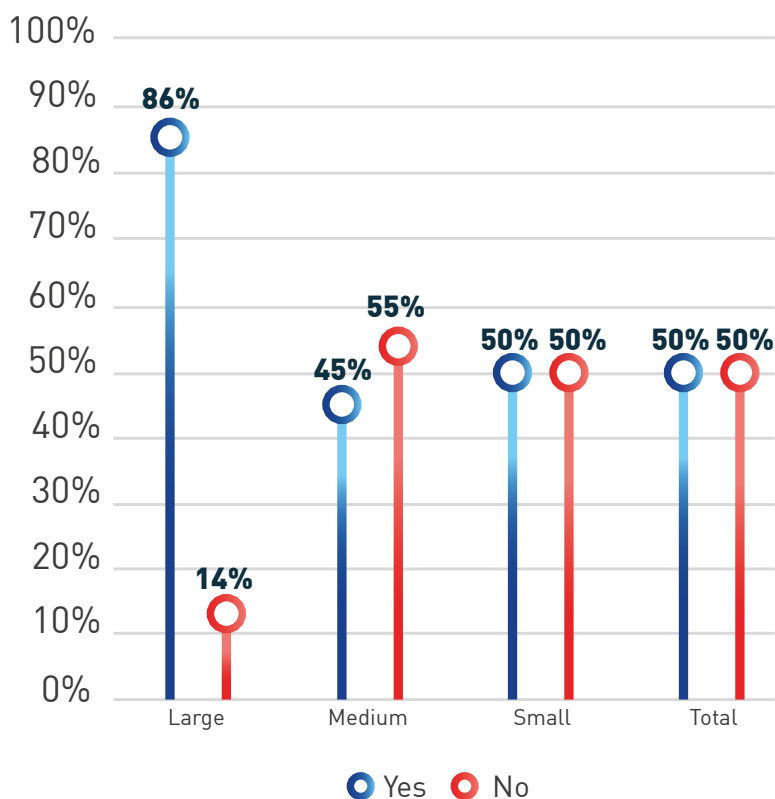
As part of the governance model of financial entities and institutions, the Board of Directors, or similar, of 50% of the financial entities and institutions in the country receives periodic reports on indicators, risks and risk management in information security (including cybersecurity) and fraud using digital means. The difference between large entities and medium-sized entities is of note, where it can be seen that while 86% of the former conducts this practice, only 45% of the latter does so.

Sectors such as securities stand out where 100% of financial entities and institutions states that the Board of Directors, or similar, receives these reports periodically,⁸ while 83% of Mexican banking sector (commercial or multiple banking and development banking) receives them, surpassing the average of the banking sector in the Latin America and the Caribbean region with an average of 72% of banks that perform this practice (Organization of American States, 2018).

⁷. Figure 37 of Annex 2 presents the comparison of the result: *Is it considered appropriate for this team to grow in the short term?* between the different sectors analyzed in the Mexican Financial System.

⁸. La Figure 38 of Annex 2 presents the comparison of the result: *Does the Board of Directors, or similar, receive periodic reports about information security risks (including cybersecurity) and fraud using digital media?* between the different sectors analyzed in the Mexican Financial System.

Figure 11. Does the Board of Directors, or similar, Receive Periodic Reports About Risks in Information Security (Including Cybersecurity) and Fraud Using Digital means?



Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

According to the results, management of information security (including cybersecurity) and fraud prevention using digital means in most of the Mexican financial entities and institutions is prepared within the framework of a Risk Committee (25% of the total). In the financial entities and institutions of the country there are also other strategic management cases such as the *Audit Committee* (23% of the total) or a *Technical or Technology Committee* (13% of the total).

It is highlighted that in the Mexican banking sector (commercial or multiple banking and development banking), the *Risk Committee* is mostly used, showing 36%, similar to that reported by banking entities in the Latin America and the Caribbean region where 39% of information security management is prepared within the framework of said Committee (Organization of American States, 2018).

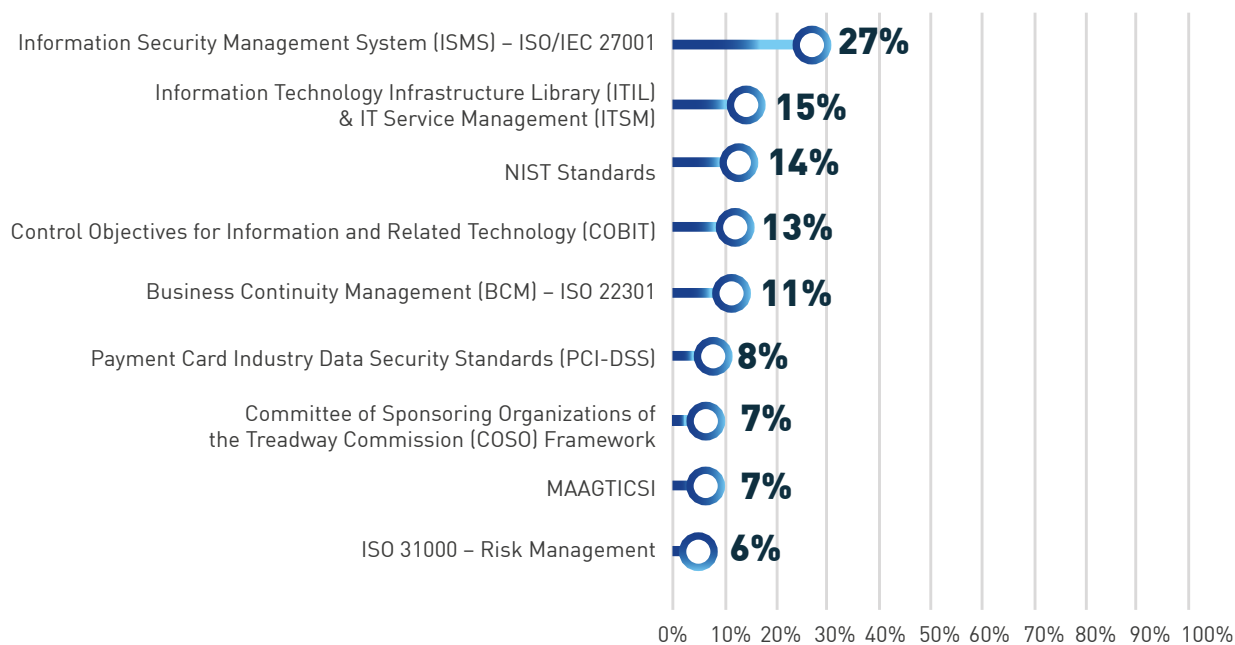
Regarding the support by top management (General Management or the Presidency) for the management of risks in information security (including cybersecurity) and fraud using digital means, it stands out that 58% of the total financial entities and institutions demonstrate this by promoting digital security training and awareness, while 49% do so by promoting information security plans.

Another aspect identified is that, while top management support to information security risk management in the banking sector of the Latin America and the Caribbean region occurs mainly (65%) *demanding the adoption of good security practices* (Organization of American States, 2018), the Mexican banking sector (commercial or multiple banking and development banking) registers barely an average of 36% for this item.

The role played by top management and the board of the organizations regarding digital security is fundamental. At a country level, this study finds that for most financial entities and institutions (48% of the total), it is fairly difficult to get the organization's top management to make investment decisions in digital security solutions, while only 17% of organizations consider it highly difficult. The fact that sectors such as FINTECH and the popular savings and credit sector (SOFIPO) find mostly (both with 53%) that it is not very difficult for top management to make investment decisions in digital security solutions is of note.

Lastly, in matters of preparedness and governance, the adoption of security frameworks and/or international standards regarding information security (including cybersecurity) by the financial entities and institutions of the country is worth highlighting. 27% of all financial entities and institutions mention that they have adopted the *Information Security Management System (ISMS) - ISO 27001* standards, 15% have adopted the *Information Technology Infrastructure Library (ITIL) & IT Service Management (ITSM)*, 14% the NIST Standards and 13% the *Control Objectives for Information and Related Technology (COBIT)*.

Figure 12. Security Frameworks and/or International Standards Adopted



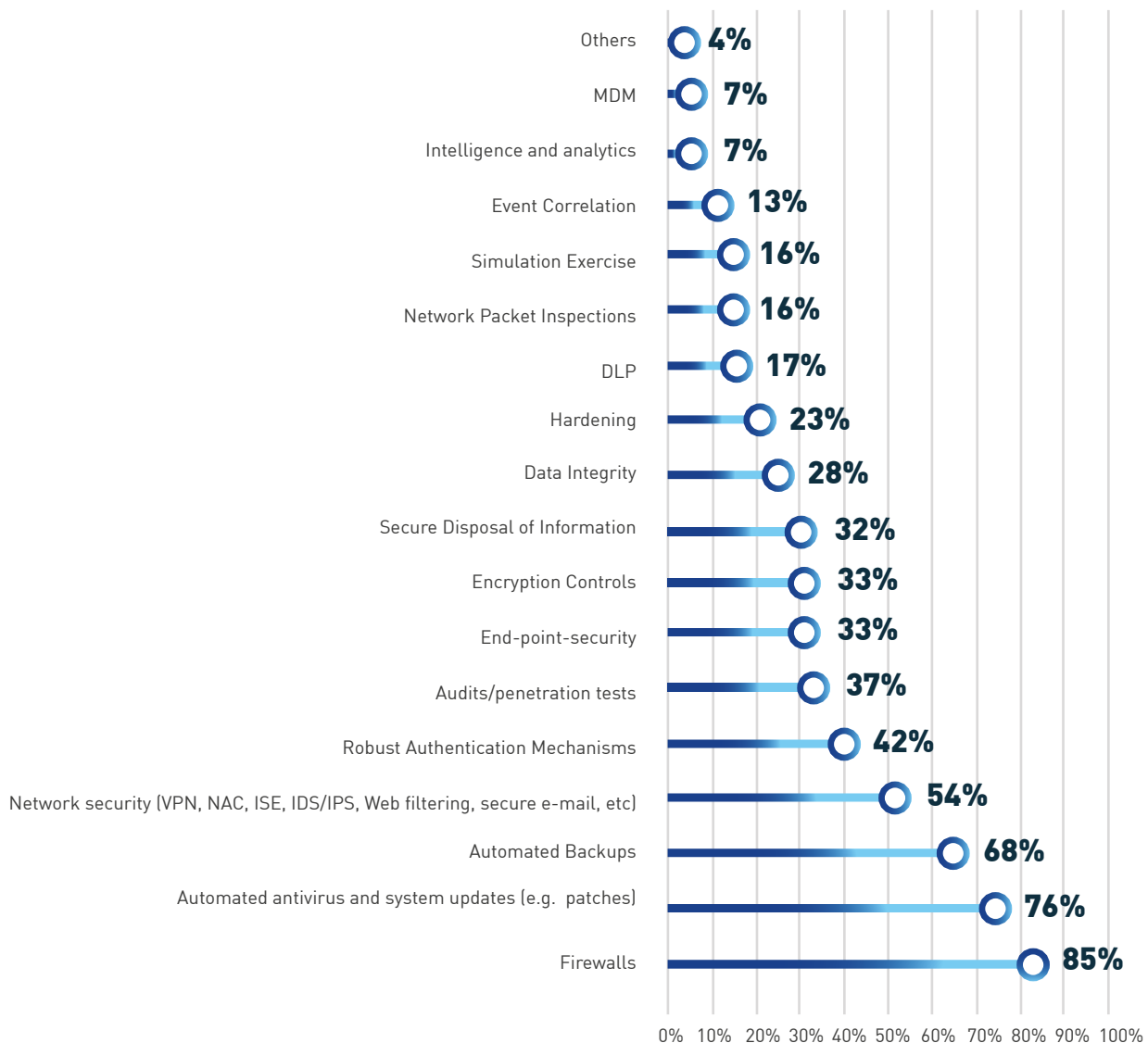
Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

It is highlighted that the application of practices and adoption of standards around *Information Security Management System (ISMS) - ISO 27001* in the Mexican banking sector (commercial or multiple banking and development banking) records an average of 71%, in accordance to what happens in the banking sector of the Latin America and the Caribbean region where 68% of the total number of banking entities mention that they have adopted said standards (Organization of American States, 2018).

3.2.2. Detection and Analysis of Digital Security Events

The actions of detection and analysis of digital security events are fundamental in the framework of systematic management of this type of risk. The main information security (including cybersecurity) actions and technical measures that Mexican financial entities and institutions perform are: i) firewalls (85% of the total), ii) automated antivirus and system updates (for example, patches, etc.) (76% of the total), iii) automated backups (68% of the total), and iv) network security (VPN, NAC, ISE, IDS/IPS, Web filtering, secure e-mail, etc.) (54%). It is highlighted that 100% of large financial entities and institutions implement measures such as firewalls, automated antivirus and system updates, network security, robust authentication mechanisms, penetration tests/audits and encryption controls.

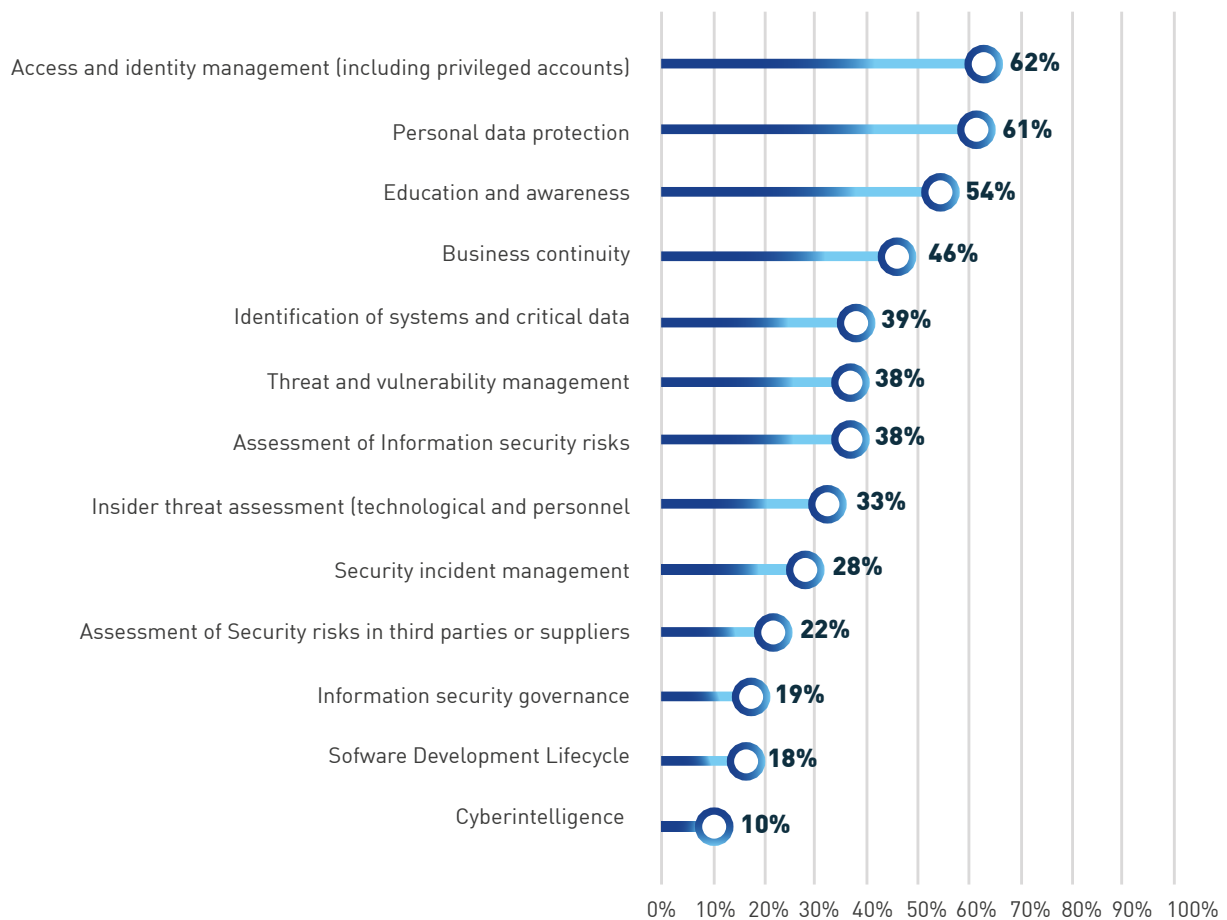
Figure 13. Information Security (Including Cybersecurity) Actions and Technical Measures to protect Critical Information Systems



Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Additionally, the most common processes/programs associated with digital security implemented in the financial entities and institutions in the country are: i) *Identity and access management (including privileged accounts)* (62%), ii) *personal data protection* (61%), iii) *education and awareness* (54%), and iv) *business continuity* (46%). It is highlighted that in the Mexican banking sector (commercial or multiple banking and development banking), 100% of large banks implement: information security governance, identification of critical systems and data, *information security risk assessment, education and awareness, threat and vulnerability management and personal data protection.*

Figure 14. Digital Security Processes/Programs Currently Implemented by Financial Entities and Institutions

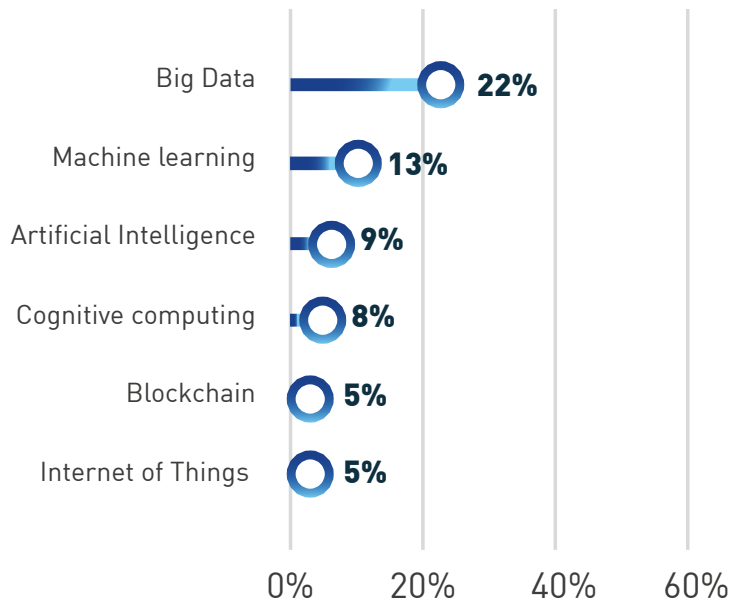


Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

The use of emerging digital technologies applied to tools, controls or digital security processes in Mexican financial entities and institutions is still lagging behind. Only 22% of the total financial entities and institutions implement data analytics in tools, controls or processes, 13% of the total financial entities and institutions implement machine learning and 9% of the total financial entities and institutions implement artificial intelligence.

A fact to highlight is that in the Mexican banking sector (commercial or multiple banking and development banking), the use of Big Data Analytics registers an average of 45%,⁹ which significantly exceeds the average of the financial sector and the average of the banking sector in the Latin America and the Caribbean region (29% of the total) (Organization of American States, 2018).

Figure 15. Emerging Digital Technologies Applied to Digital Security Tools, Controls or Processes In The Financial Entity/Institution



Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

On the other hand, information security risks considered to deserve more attention from Mexican financial entities and institutions, regardless of organization size, are i) *loss/theft of classified information assets (confidential or sensitive)*, ii) *ransomware*, and iii) *compromise of privileged user credentials*. On the part of the banking entities in the Latin America and the Caribbean region, regardless of organization size, these are i) *critical database theft*, ii) *compromise of privileged user credentials*, and iii) *data loss* (Organization of American States, 2018).

⁹ Figure 39 of Annex 2 presents the comparison of the result: *Emerging digital technologies applied to digital security tools, controls or processes in the financial entity/institution* between the different sectors analyzed in the Mexican Financial System.

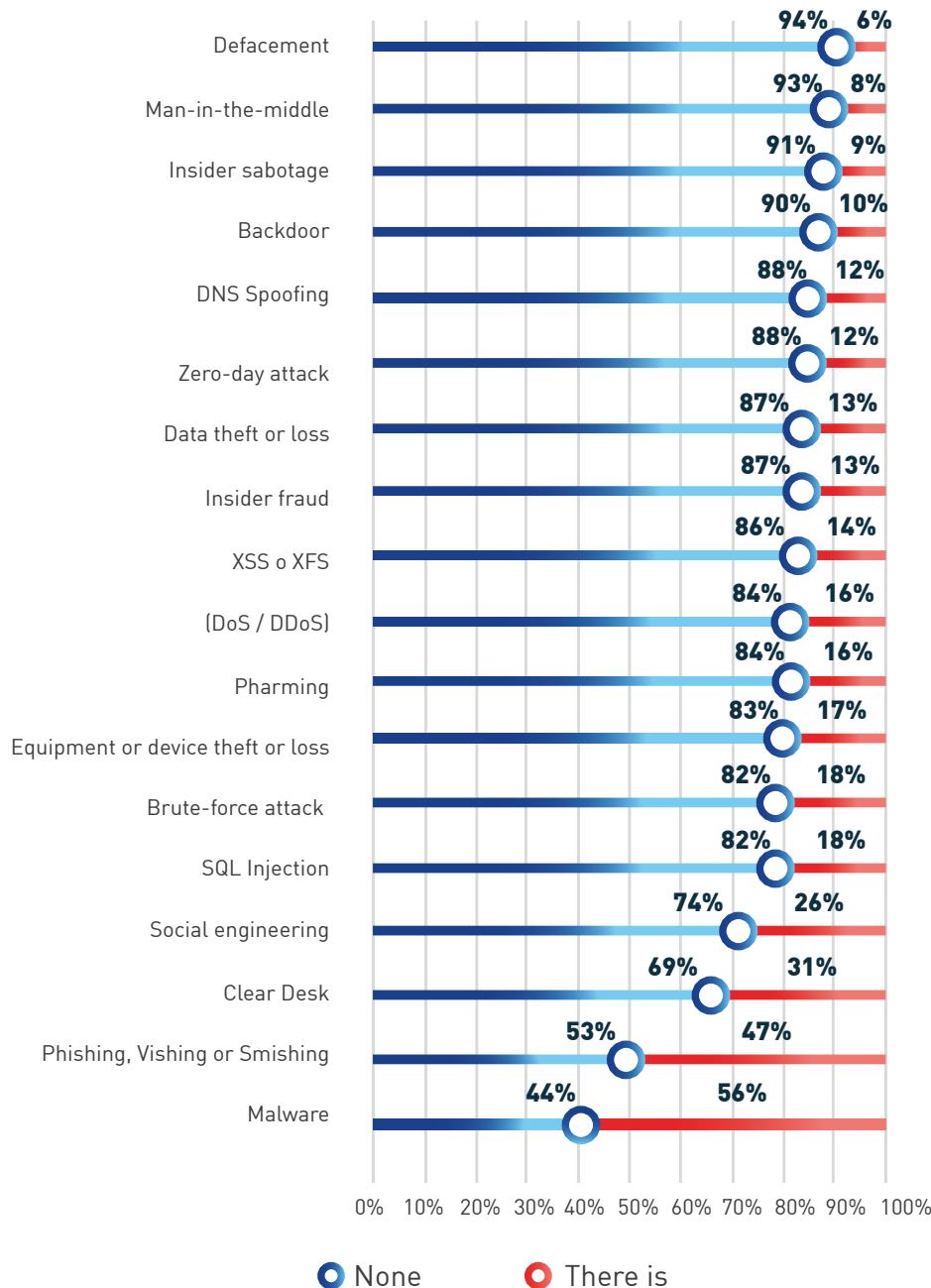
Table 6. Cyber Risks that Deserve More Attention from the Financial Entity/Institution

	Large	Medium	Small	Total
Classified Information Assets Loss/Theft (Confidential or Sensitive)	1.71	2.35	2.64	2.55
Ransomware	4.71	3.18	2.75	2.91
Compromise of Privileged User Credentials	2.29	3.08	3.24	3.17
Insider Sabotage or Fraud	2.43	3.04	3.35	3.25
Denial of Service	4.57	3.80	3.88	3.88
Defacement	5.29	5.00	4.66	4.76

Note: 240 records and interviewees prioritized risks from 1 to 7, where 1 is the highest risk and 7 the lowest risk.
Source: GS/OAS based on information collected from Mexican financial entities and institutions

Additionally, the digital security events most commonly identified by Mexican financial entities and institutions during 2018 were: i) *malware* (56% of all entities), ii) *phishing targeting access to entity systems* (47% of the total number of entities), and iii) *violation of clear desk policies* (31% of the total number of entities). In contrast, the financial entities and institutions in the country mention that the least common security events are: i) *defacement* (only 6% of the total entities), ii) *man-in-the-middle* (only 8% of total entities), and iii) *insider sabotage* (only 9% of the total number of entities). It is important to consider the similarity with the digital security events most commonly identified by the banking entities of the Latin America and the Caribbean region in 2017, which were: i) *malware* (80% of the total of Banks), ii) *violation of clear desk policies* (63% of total banks), and iii) *phishing targeting access to the bank systems* (57% of total banks) (Organization of American States, 2018).

Figure 16. Events (Successful Attacks And Unsuccessful Attacks) in Information Security (Including Cybersecurity) against Financial Entities and Institutions That Have Been Identified During the Last Twelve Months

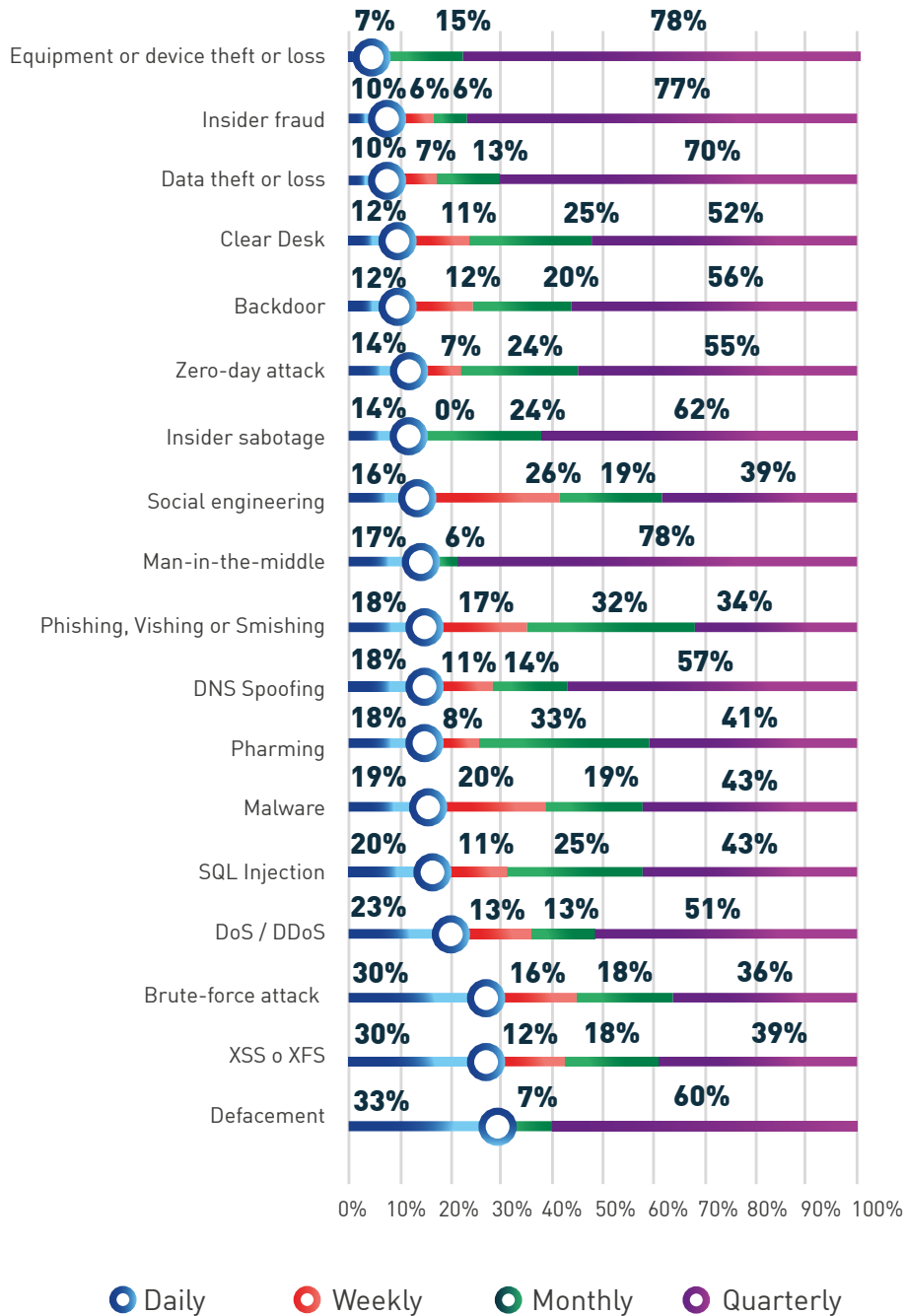


Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions


When analyzing the results regarding the approximate frequency of occurrence of events identified by the Mexican financial entities and institutions in 2018, a particular dynamic can be seen by type of event that also depends on organization size. For example, when reviewing the frequency with which events related to *malware* occur for the total number of financial entities and institutions in the country, the following can be seen: i) 19% of the entities identify the occurrence of *malware* events on a daily basis, ii) 20% of the total identify it weekly, iii) 19% of the total identify it monthly, and

iv) 43% of the total identify it quarterly. Regarding *phishing, vishing or smishing*, the following can be seen: i) 18% of the entities identify occurrence of this type of events daily, ii) 17% of the total identify it weekly, iii) 32% of the total identify it monthly, and iv) 34% of the total identify it quarterly.

Figure 17. Frequency of Occurrence of Information Security (Including Cybersecurity) Events against Financial Entities and Institutions



Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions



Analysis of the frequency of occurrence of information security (including cybersecurity) events (successful attacks and unsuccessful attacks) in the Mexican Financial System allows us to observe an average occurrence. However, when reviewing the results by financial entity/institution size, particular dynamics occur.

For example, it is noted that the large entities of the Mexican Financial System are subject to attacks of all kinds of digital security events, where almost all are identified by the majority of said entities in the country. The digital security events (successful attacks and unsuccessful attacks) most commonly identified by large entities in Mexico in 2018 are: i) *malware* (100% of all large entities), ii) *violation of clear desk policies* (100% of all large entities), and iii) *phishing, vishing or smishing* (100% of all large entities).

When reviewing the frequency with which events related to *malware* occur for the total of large entities in Mexico, the following can be seen: i) 43% of large entities detect *malware* events daily and ii) 57% of the total say they identify it weekly. Lastly, there is a dynamic of identification of the occurrence of a variety of digital security events that are daily, weekly, monthly and quarterly by the large entities in the country.

Table 7. Digital Security Events against Large Financial Entities and Institutions that Have Been Identified During the Last Twelve Months

	None	There is	Total	Daily	Weekly	Monthly	Quarterly	Total
Social engineering	14%	86%	100%	0%	50%	17%	33%	100%
Malware	0%	100%	100%	43%	57%	0%	0%	100%
Phishing, Vishing or Smishing	0%	100%	100%	14%	43%	14%	29%	100%
Pharming	29%	71%	100%	0%	40%	20%	40%	100%
Data theft or loss	71%	29%	100%	0%	0%	0%	100%	100%
Equipment or device theft or loss	43%	57%	100%	0%	0%	25%	75%	100%
Zero-day attack	100%	0%	100%	0%	0%	0%	0%	0%
(DoS / DDoS)	29%	71%	100%	0%	20%	0%	80%	100%
DNS Spoofing	71%	29%	100%	0%	0%	0%	100%	100%
Clear Desk	0%	100%	100%	14%	14%	14%	57%	100%
Insider sabotage	86%	14%	100%	0%	0%	0%	100%	100%
Insider fraud	57%	43%	100%	0%	0%	33%	67%	100%
Defacement	86%	14%	100%	0%	0%	0%	100%	100%
Backdoor	100%	0%	100%	0%	0%	0%	0%	0%
SQL Injection	29%	71%	100%	20%	40%	0%	40%	100%
XSS or XFS	29%	71%	100%	20%	40%	0%	40%	100%
Brute-force attack	29%	71%	100%	20%	40%	20%	20%	100%
Man-in-the-middle	86%	14%	100%	0%	0%	0%	100%	100%

Note: 7 records Source: GS/OAS based on information collected from Mexican financial entities and institutions




In relation to the medium-sized entities of the Mexican Financial System, it is highlighted that they are also subject to attacks of all kinds of digital security events, showcasing the identification of some by most of these entities in the country. The digital security events (successful attacks and unsuccessful attacks) most commonly identified by medium-sized entities during 2018 are: i) *malware* (69% of all medium-sized entities), ii) *phishing, vishing or smishing* (62% of the total of medium-sized entities), and iii) *violation of clear desk policies* (40% of the total of medium-sized entities).

When reviewing the frequency of occurrence of events related to *malware* for the total of medium-sized entities in the country, the following can be seen: i) 24% of medium-sized entities identify the occurrence of *malware* events on a daily basis, ii) 24% of the total identify it weekly, iii) 13% of the total identify it monthly, and iv) 39% of the total identify it quarterly. Lastly, there is a dynamic of identification of the occurrence of some digital security events on a daily basis and of the rest of the events, a monthly and quarterly occurrence on the part of medium-sized entities in Mexico.

Table 8. Digital Security Events against Medium-Sized Financial Entities and Institutions that Have Been Identified During the Last Twelve Months

	None	There is	Total	Daily	Weekly	Monthly	Quarterly	Total
Social engineering	55%	45%	100%	24%	16%	28%	32%	100%
Malware	31%	69%	100%	24%	24%	13%	39%	100%
Phishing, Vishing or Smishing	38%	62%	100%	21%	18%	29%	32%	100%
Pharming	73%	27%	100%	20%	7%	40%	33%	100%
Data theft or loss	82%	18%	100%	10%	10%	40%	40%	100%
Equipment or device theft or loss	71%	29%	100%	6%	0%	25%	69%	100%
Zero-day attack	75%	25%	100%	14%	0%	29%	57%	100%
(DoS / DDoS)	76%	24%	100%	23%	23%	15%	38%	100%
DNS Spoofing	76%	24%	100%	8%	15%	15%	62%	100%
Clear Desk	60%	40%	100%	14%	9%	32%	45%	100%
Insider sabotage	87%	13%	100%	14%	0%	43%	43%	100%
Insider fraud	76%	24%	100%	8%	15%	8%	69%	100%
Defacement	85%	15%	100%	25%	0%	13%	63%	100%
Backdoor	84%	16%	100%	11%	11%	22%	56%	100%
SQL Injection	65%	35%	100%	16%	0%	26%	58%	100%
XSS or XFS	76%	24%	100%	23%	0%	23%	54%	100%
Brute-force attack	64%	36%	100%	25%	5%	30%	40%	100%
Man-in-the-middle	85%	15%	100%	13%	0%	13%	75%	100%

Note: 53 records Source: GS/OAS based on information collected from Mexican financial entities and institutions



Lastly, in relation to the small entities of the Mexican Financial System, it is highlighted that they are subject to attacks of some types of digital security events, noting the identification of a few by most of said entities in the country. The digital security events (successful attacks and unsuccessful attacks) most commonly identified by the small entities during 2018 are: i) *malware* (68% of the total of medium-sized entities), ii) *the violation of clear desk policies* (45% of the total of medium-sized entities) and iii) *phishing targeting access to entity systems* (42% of the total of medium-sized entities).

When reviewing the frequency of occurrence of events related to *malware* for the total of small entities in Mexico, the following can be seen: i) 14% of the small entities identify the occurrence of *malware* events on a daily basis, ii) 16% of the total identify it weekly, iii) 22% of the total identify it monthly, and iv) 48% of the total identify it quarterly. Lastly, there is a dynamic of identification of the occurrence of some digital security events on a daily basis, and of the rest of the events as a weekly, monthly and quarterly occurrence by the small entities of the country.

Table 9. Digital Security Events against Small Financial Entities and Institutions that Have Been Identified During the last Twelve Months

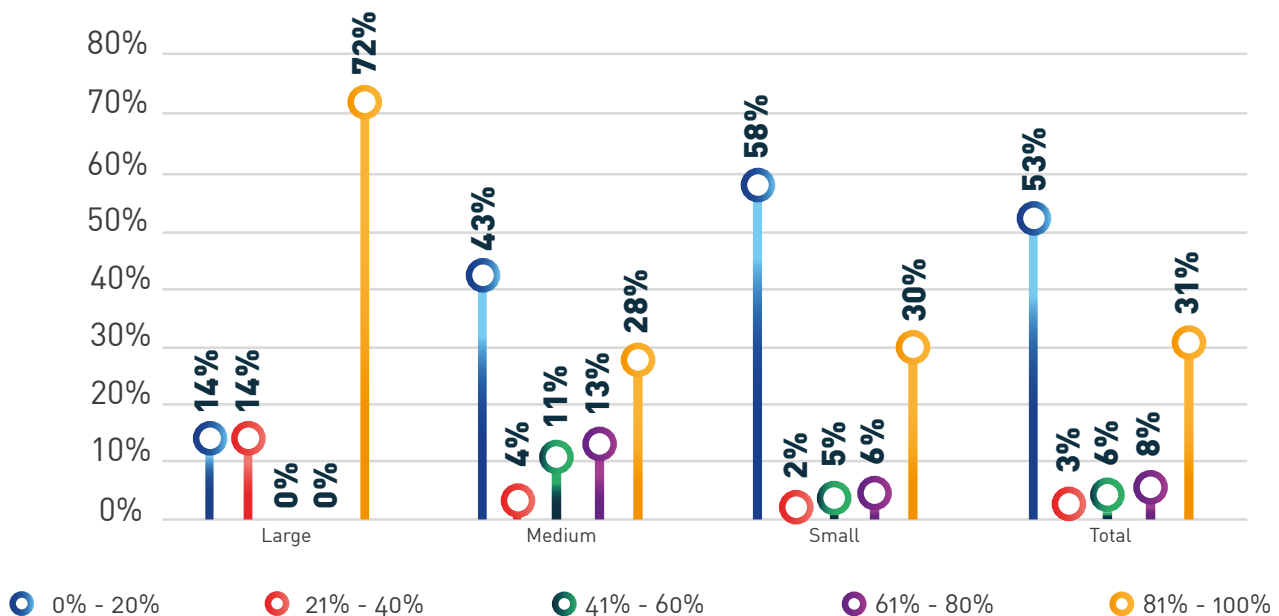
	None	There is	Total	Daily	Weekly	Monthly	Quarterly	Total
Social engineering	83%	17%	100%	13%	29%	13%	45%	100%
Malware	49%	51%	100%	14%	16%	22%	48%	100%
Phishing, Vishing or Smishing	60%	40%	100%	17%	14%	35%	35%	100%
Pharming	89%	11%	100%	21%	0%	32%	47%	100%
Data theft or loss	90%	10%	100%	11%	6%	0%	83%	100%
Equipment or device theft or loss	88%	12%	100%	10%	0%	5%	86%	100%
Zero-day attack	92%	8%	100%	13%	13%	20%	53%	0%
(DoS / DDoS)	88%	12%	100%	29%	5%	14%	52%	100%
DNS Spoofing	93%	7%	100%	31%	8%	15%	46%	100%
Clear Desk	74%	26%	100%	11%	11%	24%	54%	100%
Insider sabotage	93%	7%	100%	15%	0%	15%	69%	100%
Insider fraud	92%	8%	100%	13%	0%	0%	87%	100%
Defacement	97%	3%	100%	50%	0%	0%	50%	100%
Backdoor	91%	9%	100%	13%	13%	19%	56%	0%
SQL Injection	89%	11%	100%	25%	15%	30%	30%	100%
XSS or XFS	92%	8%	100%	40%	13%	20%	27%	100%
Brute-force attack	89%	11%	100%	37%	21%	5%	37%	100%
Man-in-the-middle	95%	5%	100%	22%	0%	0%	78%	100%

Note: 180 records Source: GS/OAS based on information collected from Mexican financial entities and institutions

When analyzing the type of digital security events (successful attacks and unsuccessful attacks) used by cybercriminals against financial service clients (partners, associates or users), the Mexican financial entities and institutions mention that the events of i) phishing, ii) spyware (malware or Trojans), and iii) social engineering are the most frequent in the country, similar to that registered by the banking sector in the Latin America and the Caribbean region in 2017 (Organization of American States, 2018). On the other hand, less common digital security events against clients (partners, associates or users) are: i) *insider fraud* (carried out by corporate clients), ii) *RFID identity theft* (credit cards/mobile phones), and iii) *false software that poses as the real entity software*.

Lastly, in matters of detection and analysis of digital security events, it is highlighted that, on average, 53% of the financial entities and institutions in the country detect, using their own systems (and not of third parties), 0% - 20% of events (successful attacks and unsuccessful attacks) in information security (including cybersecurity); 3% of entities detect 21% - 40% of events with their own systems, 6% of entities detect 41% - 60% of events with proprietary systems, 8% of entities detect 61% - 80% of events with their own systems and 31% of entities detect 81% - 100% of events with own systems. It is highlighted that in sectors such as securities and FINTECH, more than 75% of the financial entities and institutions in these sectors detect, through their own systems (and not third parties) 81% - 100% of information security events.¹⁰

Figure 18. Percentage of Digital Security Events that Are Detected by the Detection Systems of the Financial Entity/Institution (and not Third-Party Systems)



Note: 237 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

¹⁰ Figure 40 of Annex 2 presents the comparison of the result: *Percentage of digital security events that are detected by the detection systems of the financial entity/institution (and not third-party systems)* between the different sectors analyzed in the Mexican Financial System.

When analyzing by entity size, most of the large entities (71%) detect 81% - 100% of events with their own systems, most of the medium-sized entities (43%) detect 0% - 20% of events with their own systems and most of the small entities (58%) detect 0% - 20% of events with their own systems. The case of the Mexican banking sector (commercial or multiple banking and development banking) is highlighted, where 83% of large banks detect between 81% and 100% of events with their own systems, while on average 30% of banks of the Latin America and the Caribbean region detect events in that range (Organization of American States, 2018).

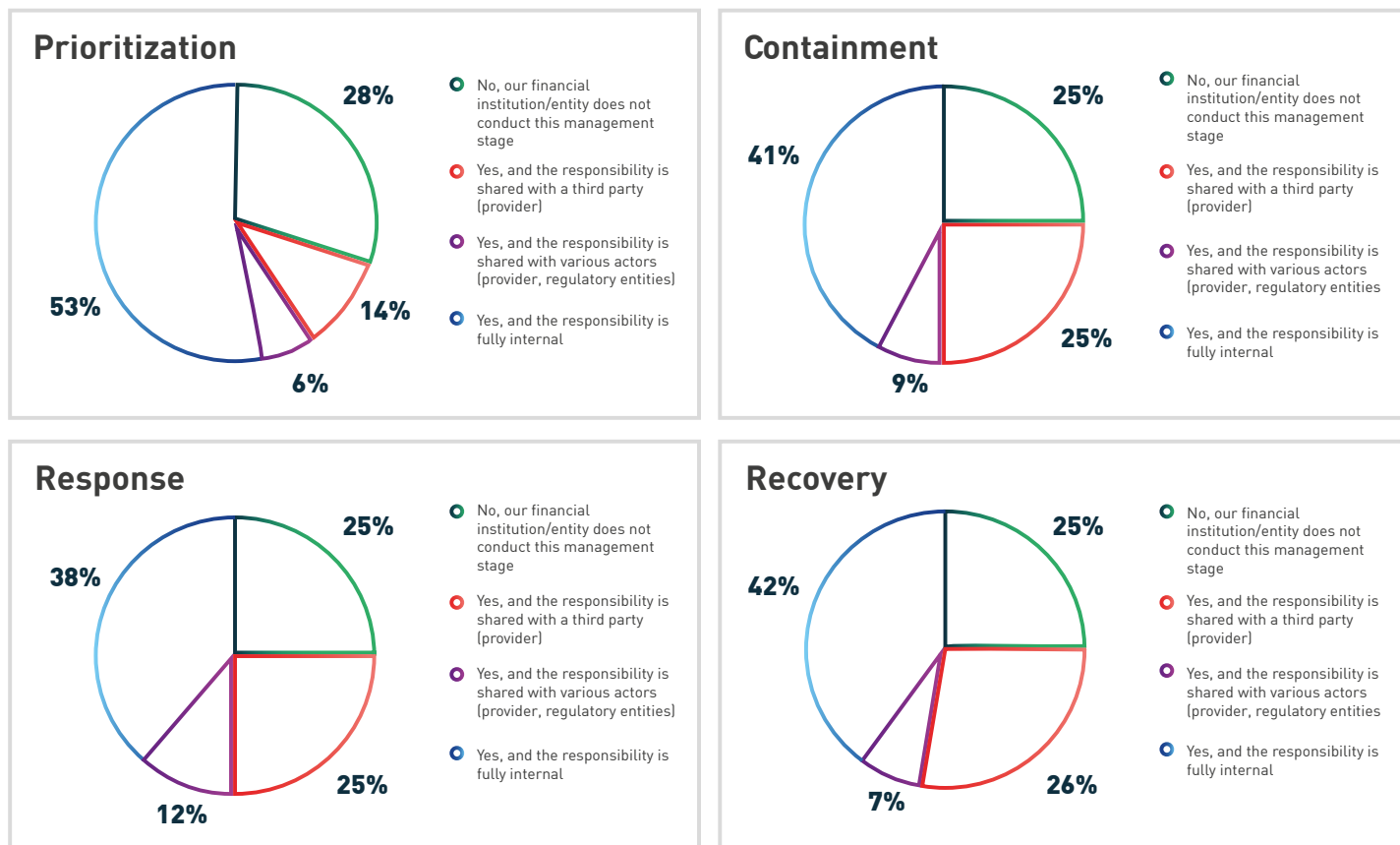
3.2.3. Digital Security Incident Management, Response and Recovery

Taking into account the distinction expressed in the information collection instrument—that was sent to financial entities and institutions—between information security (including cybersecurity) event (the sum of successful attacks and unsuccessful attacks against the financial entity/institution during a certain period of time) and information security (including cybersecurity) incident (the total of successful attacks against the financial entity and institution during the same period of time), the results are analyzed below, emphasizing the latter concept: the management, response and recovery of digital security incidents.

When analyzing the management stages regarding incidents (successful attacks) in information security (including cybersecurity), it is highlighted that: i) 53% of the entities in the country have and execute an incident *prioritization strategy* under the internal responsibility of the organization, ii) 41% of the country's entities have and execute an incident *containment strategy* under the internal responsibility of the organization, iii) 38% of the country's entities have and execute an incident *response strategy* under the internal responsibility of the organization, and iv) 42% of the entities in the country have and execute an incident *recovery strategy* under the internal responsibility of the organization. In other words, at least one third of the country's entities have digital security incident management, response and recovery strategies.

When analyzing the Mexican Financial System by sectors, it is observed that the banking sectors (commercial or multiple banking and development banking), securities, and FINTECH report percentages higher than 74% when executing an incident *prioritization strategy* under the internal responsibility of the organization, which is slightly higher than the average of 70% of the banks in the Latin America and the Caribbean region (Organization of American States, 2018), while the sectors of popular savings and credit institutions (SOCAP and SOFIPO) and of non-financial intermediaries report averages less than 44% over that same stage.

Figure 19. Strategies against Digital Security Incidents (Successful Attacks)

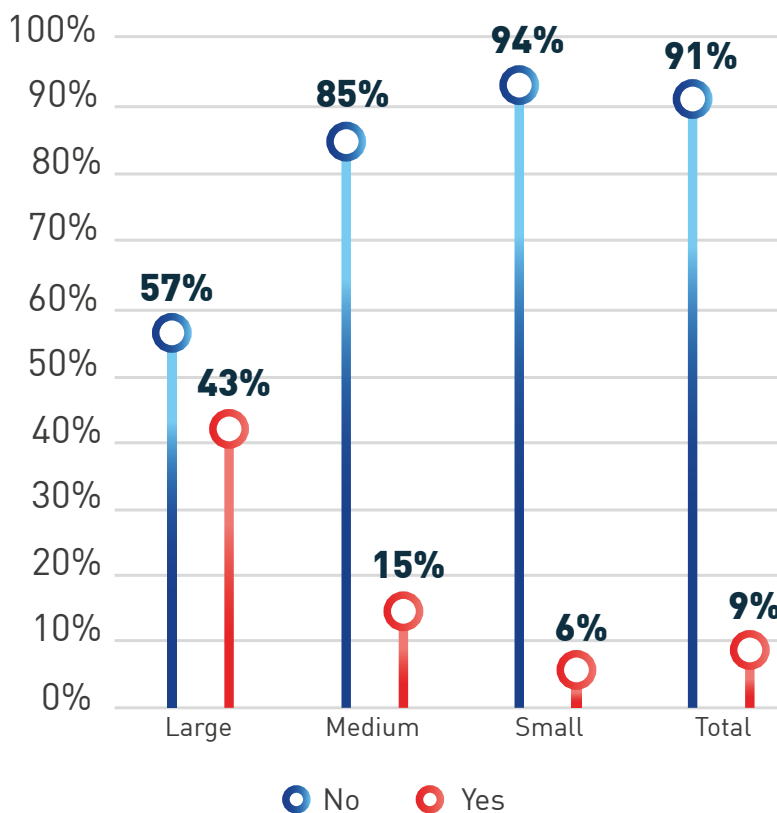


Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

In relation to the materialization of incidents (successful attacks) in information security (including cybersecurity) in financial entities and institutions in the country during 2018, it is highlighted that 43% of large entities state that they were victims of successful attacks, while among medium-sized entities, the percentage is 15%, and among small entities, it is 6%. Highlighted is the fact that in the Mexican banking sector (commercial or multiple banking and development banking), the average is higher with respect to other sectors of the Mexican Financial System, reporting the materialization of incidents (successful attacks) in 50% of large entities, 22% of medium-sized entities and 11% of small entities.¹¹ However, it is lower than in the banking sector of the Latin America and the Caribbean region, where 65% of large banks, 43% of medium-size companies, and 19% of small ones report having been victims of successful information security (including cybersecurity) attacks.

¹¹ Figure 41 of Annex 2 presents the comparison of the result: *Was the financial entity/institution to which you belong (in the country where you are located), as an organization, the victim of incidents (successful attacks) in information security (including cybersecurity) during the last twelve months?* between the different sectors analyzed in the Mexican Financial System.

Figure 20. Was the Financial Entity/Institution to Which You Belong (in the Country Where You Are Located), as an Organization, a Victim of Incidents (Successful Attacks) in Information Security (Including Cybersecurity) During the Last Twelve Months?



Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Specifically, and based on the financial entities and institutions that are victims of incidents (successful attacks) in information security (including cybersecurity) (22 entities), it is highlighted that the vast majority (86% on average) investigate the source that originated such incidents. At the sectoral level, all the entities in the banking sector (commercial or multiple banking and development banking) and securities investigate the source.¹²

In addition, and as a result of the investigations, said financial entities and institutions in the country identify and prioritize the main motivations of said incidents (successful attacks) in information security (including cybersecurity) during 2018, these being: i) *economic reasons* (74% of victim entities), ii) *political reasons/hacktivism* (32% of victim entities), and iii) *personal information theft* (26% of victim entities).

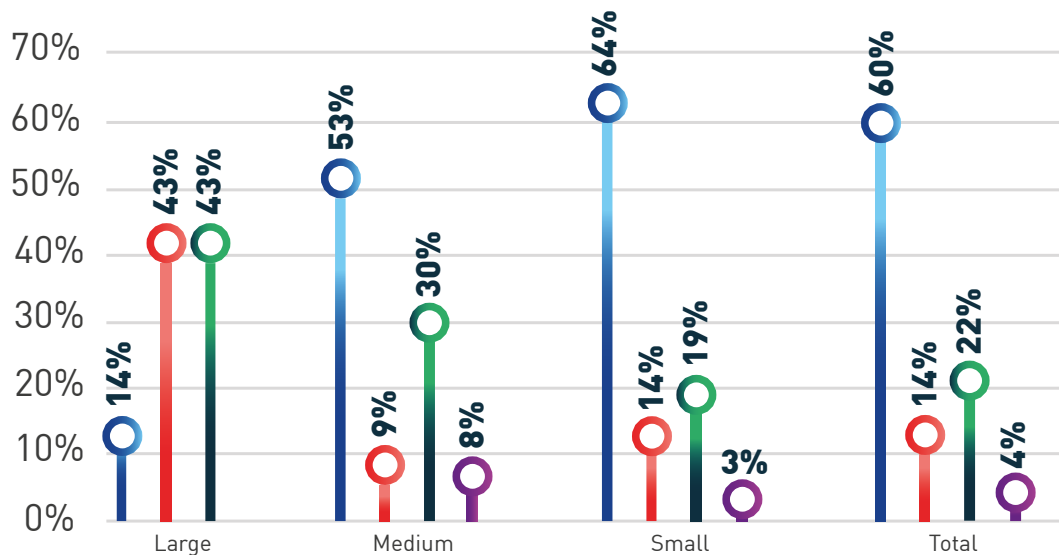
With regard to the banking sector (commercial or multiple banking and development banking), the main motivations are the same, but with higher percentages of occurrence (89% of banks victims for *economic reasons*, 56% of banks victims for *political motives/hacktivism* and 33% of the banks victims for *personal information theft*). It is worth noting that, in the banking sector of the Latin American and Caribbean region, the section of *political motives/hacktivism* is not considered one of the main causes behind computer attacks (Organization of American States, 2018).

When asking whether financial entities and institutions fully complete a maturity assessment under an information security (including cybersecurity) methodology or conducting all the derivative actions, differences

¹². Figure 42 of Annex 2 presents the comparison of the result: *Did the financial entity/institution to which you belong investigate the source that originated such incidents (successful attacks) in information security (including cybersecurity)?* between the different sectors analyzed in the Mexican Financial System.

are found according to organization size. While 43% of large entities in Mexico carry out this evaluation and the corresponding actions, only 30% of medium-sized entities and 19% of small entities reflect this situation. In contrast, it is worrying that 53% of medium-sized entities and 64% of small entities do not assess the maturity of digital security. At a sectoral level, it is also concerning that more than 70% of the financial entities and institutions of the popular savings and credit (SOCAP and SOFIPO) and non-banking financial intermediary sectors of Mexico indicate that they have not been evaluated.¹³

Figure 21. Has the Financial Entity/Institution to Which You Belong Been Externally Evaluated in the Last Two (2) Years under Any Information Security (Including Cybersecurity) Methodology to Determine Level of Maturity?



- No, our entity has not been evaluated
- Yes, the evaluation was made and the corresponding actions were made to satisfaction
- Yes, the evaluation was made and the corresponding actions are being carried out
- Yes, the evaluation was made but it hasn't been possible to carry out the corresponding actions

Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

¹³ Figure 43 of Annex 2 presents the comparison of the result: *Has the financial entity/institution to which you belong been externally evaluated in the last two (2) years under any information security (including cybersecurity) methodology to determine its level of maturity?* between the different sectors analyzed in the Mexican Financial System.

The financial entities and institutions of the Mexican Financial System that stated that they do not fully complete a cybersecurity maturity assessment or do not execute the derivative actions, attribute it mainly to: i) insufficient specialized personnel (39% of entities without evaluation), ii) lack of budget allocation (28% of entities without evaluation), and iii) little knowledge of the impact of threats (27% of entities without evaluation).

The main causes reported by banks in the Mexican banking sector (commercial or multiple banking and development banking) as to why, on average, they do not fully complete a digital security maturity assessment or do not perform their derivative actions coincide with the main causes reported by the banking sector in the Latin America and the Caribbean region: i) *Insufficient specialized staff* (36% in Mexico versus 46% in the region), ii) *Lack of budget allocation* (24% in Mexico versus 45% in the region), iii) *Lack of specific regulation that mandates implementation* (21% in Mexico versus 34% in the region) (Organization of American States, 2018).

3.2.4. Reports of Digital Security Incidents

From the analysis of results regarding the information security (including cybersecurity) incident report (total of successful attacks against the financial entity/institution during the same period of time) it is important to check whether the organizations have internal mechanisms or plans, as well as specific regulations, on the matter.

In general terms, it can be seen that more than half of the Mexican financial entities and institutions—large (86%), medium-sized (57%) and small (53%)—offer a mechanism for their collaborators (employees and contractors) to report digital security incidents (successful attacks), and in sectors such as the Mexican banking sector (commercial or multiple banking and development banking) this reaches 93%¹⁴, surpassing even the average of the Latin America and the Caribbean region (68% of the banks in the region) (Organization of American States, 2018).

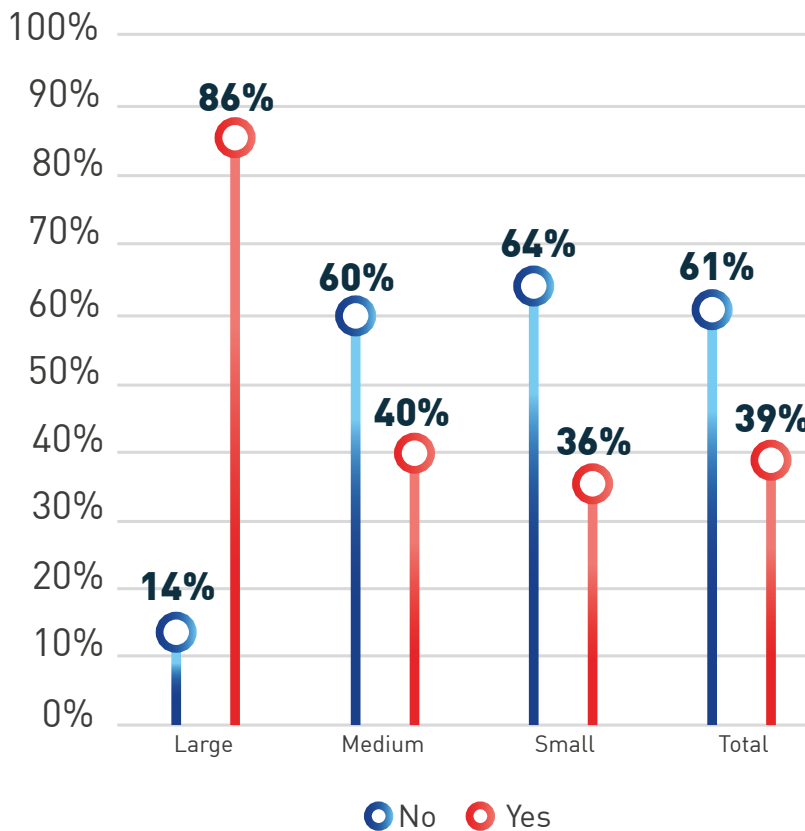
In contrast to the above, the existence of mechanisms for the financial service clients (partners, associates or users) to report digital security incidents (successful attacks) to the entity varies according to entity size. It is appreciated that 86% of large entities offer a mechanism for their financial services clients to report digital security incidents (successful attacks) to the entity, in contrast to 40% of medium-sized entities and 36% of small entities in the country.

In this case, 67% of banks in the Mexican banking sector (commercial or multiple banking and development banking) offer their clients this type of mechanism¹⁵, which is equal to the average of banks in the Latin American and Caribbean region (68% of the total) (Organization of American States, 2018).

¹⁴. Figure 44 of Annex 2 presents the comparison of the result: *Does the financial entity/institution to which you belong offer a mechanism for its collaborators (employees and contractors) to report information security (including cybersecurity and fraud using digital means) incidents (successful attacks)?* between the different sectors analyzed in the Mexican Financial System.

¹⁵. Figure 45 of Annex 2 presents the comparison of the result: *Does the financial entity/institution to which you belong offer a mechanism for its financial services clients (partners, associates or users) to report information security (including cybersecurity and fraud using digital means) incidents (successful attacks)?* between the different sectors analyzed in the Mexican Financial System.

Figure 22. Does the Financial Entity/Institution to Which You Belong Offer a Mechanism for your Financial Service Clients (Partners, Associates or Users) to Report Information Security Incidents (Successful Attacks) (Including Cybersecurity and Fraud Using Digital means)?



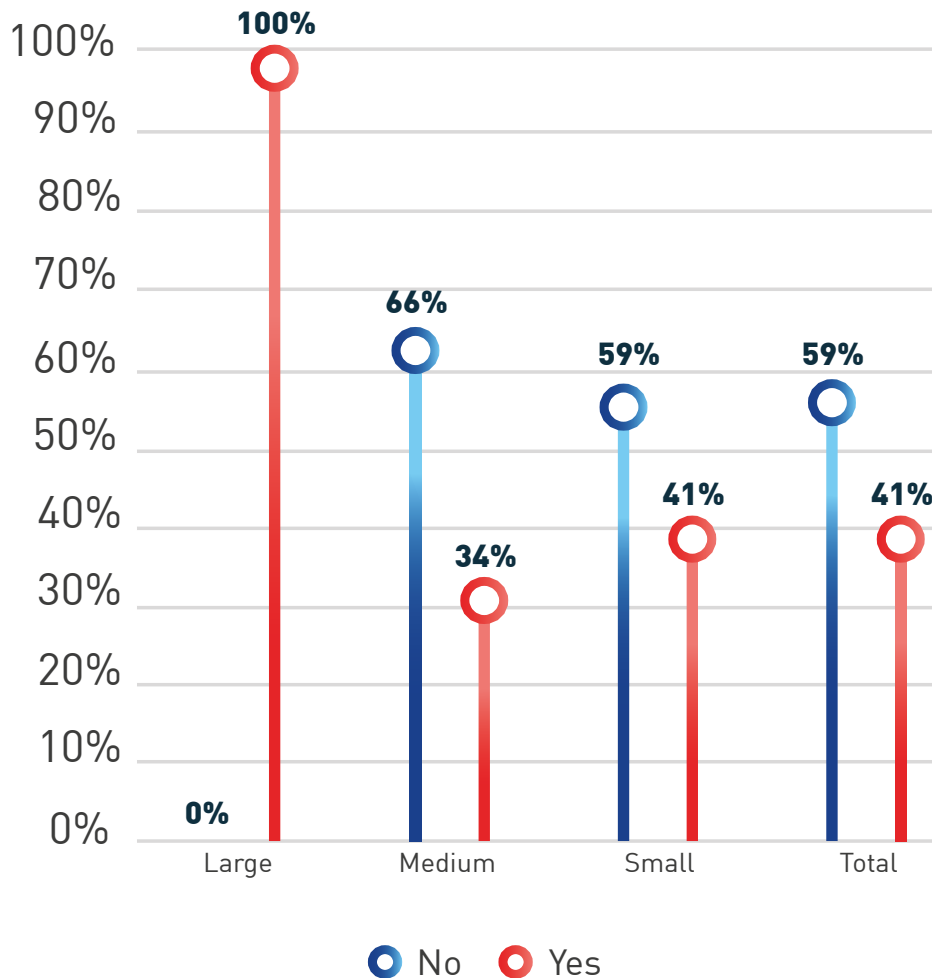
Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Likewise, the existence of a communications plan that allows financial services clients (partners, associates or users) to be informed when their personal information has been compromised varies according to the size of the entity. It is appreciated that in all large entities there is a communication plan to inform their financial services clients when their personal information has been compromised, in contrast with a third of the medium-sized entities (34%) in the country and a little more than one third of small entities (41%).

When conducting a sectoral analysis within the Mexican Financial System, contrasts emerge, like the one between the Mexican banking sector (commercial or multiple banking and development banking), where 81% of the total number of banks have the aforementioned communications plan, and the popular savings and credit sector (SOCAP and SOFIPO) where only 23% of entities report having it.¹⁶

¹⁶ Figure 46 of Annex 2 presents the comparison of the result: *Does the financial entity/institution to which you belong have a communications plan that allows informing financial service clients (partners, associates or users) when their personal information has been compromised?* between the different sectors analyzed in the Mexican Financial System.

Figure 23. Does the Financial Entity/Institution to Which You Belong Have a Communications Plan that Allows Informing Financial Service Clients (Partners, Associates or Users) When Their Personal Information has been Compromised?

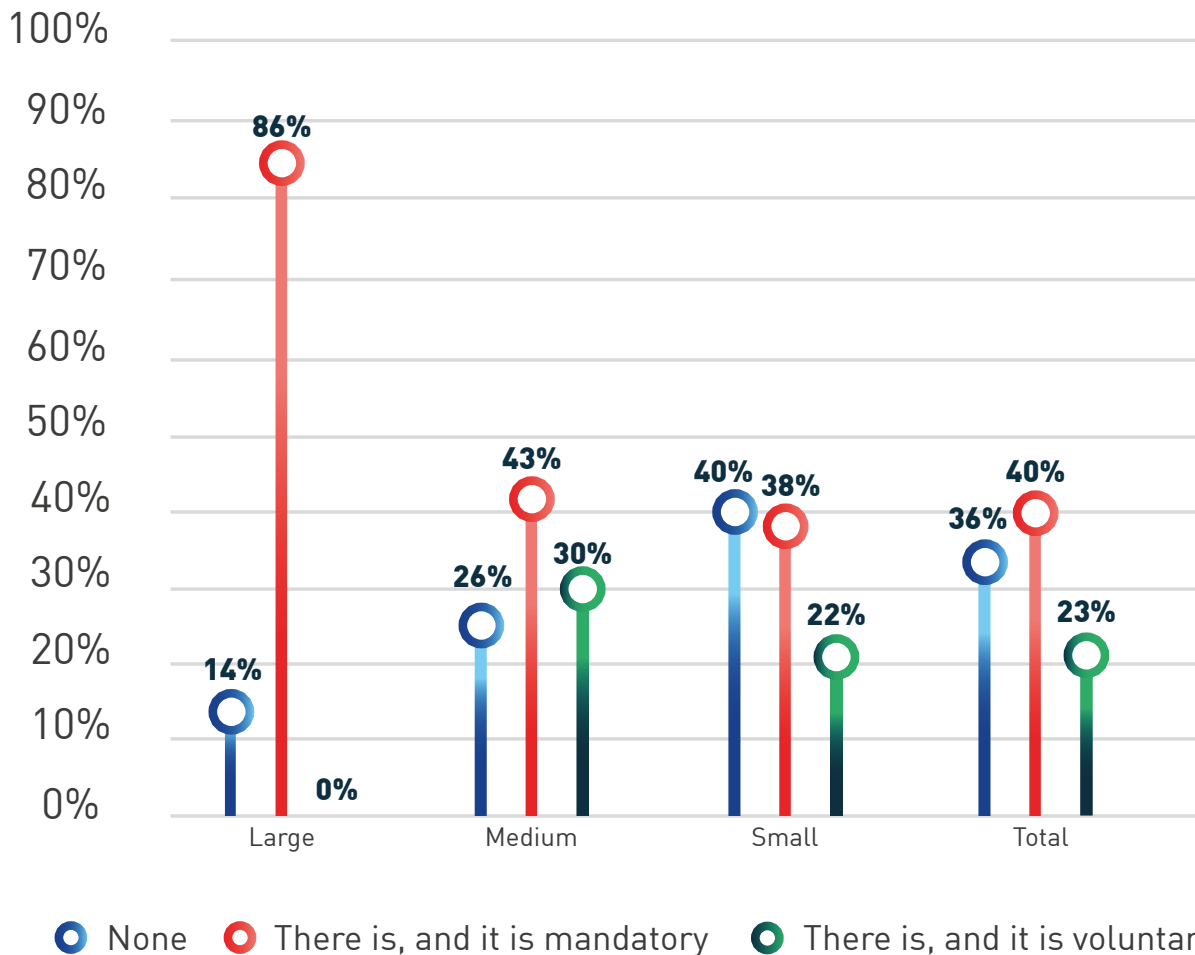


Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

In relation to the reporting of incidents (successful attacks) in information security (including cybersecurity and fraud using digital means) by financial entities and institutions to a regulatory authority in Mexico, differences between large versus medium-sized and small entities are also appreciated. 86% of large entities versus 43% of medium-sized entities and 38% of small entities state that they know of some mechanism to report incidents and it is mandatory due to provisions established by some regulatory authority. On the other hand, it is noteworthy that only 14% of large entities in the country, in contrast to 40% of small entities, state that there is no mechanism to report incidents to a regulatory authority.¹⁷

¹⁷ Figure 47 of Annex 2 presents the comparison of the result: Do you know any mechanism to report information security (including cybersecurity and fraud using digital means) incidents (successful attacks) against the financial entity/institution to which you belong, to a regulatory authority in Mexico? between the different sectors analyzed in the Mexican Financial System.

Figure 24. Do you Know Any Mechanism to Report Incidents (Successful Attacks) in Information Security (Including Cybersecurity and Fraud Using Digital means) against the Financial Institution/Entity to Which You Belong, to a Regulatory Authority in Mexico?

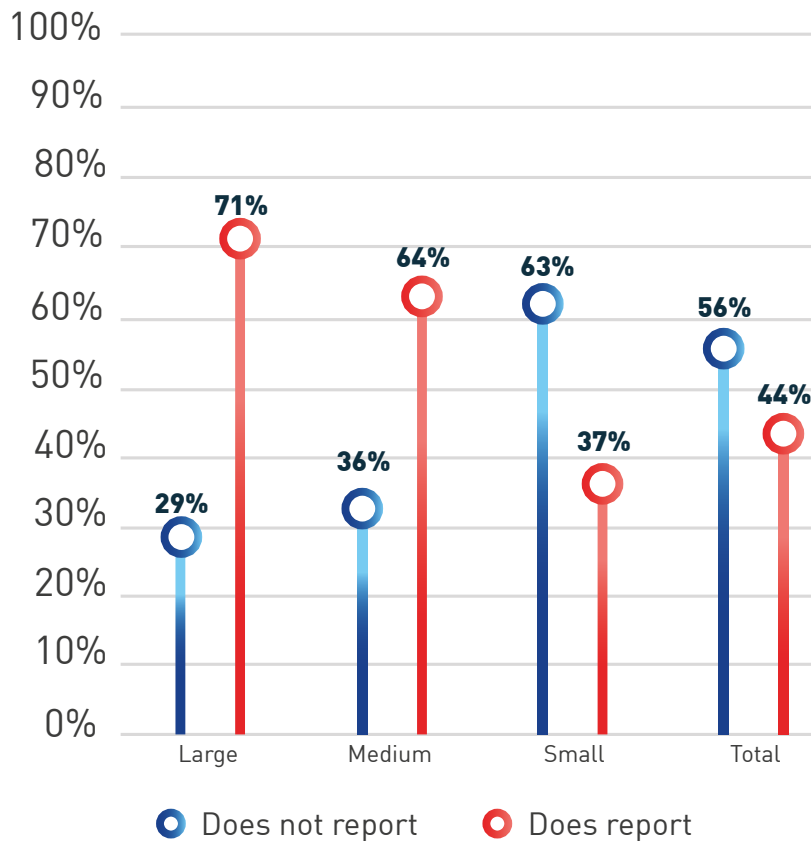


Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Additionally, it is appreciated that as the size of the financial entity/institution grows, the reporting of incidents (successful attacks) in information security (including cybersecurity and fraud using digital means) to a Mexican law enforcement authority increases. 71% of the large entities, 64% of the medium-sized entities and 37% of the small entities report incidents before this authority in the country. This situation is contrasted with the fact that in sectors such as the popular savings and credit sector (SOCAP and SOFIPO), the securities sector, the non-banking financial intermediaries' sector and the FINTECH sector, less than 40% of the total number of entities in these sectors report incidents to authorities.¹⁸

¹⁸ Figure 48 of Annex 2 presents the comparison of the result: Does the financial entity/institution to which you belong report the information security (including cybersecurity and fraud using digital means) incidents (successful attacks) to a law enforcement authority in Mexico? between the different sectors analyzed in the Mexican Financial System.

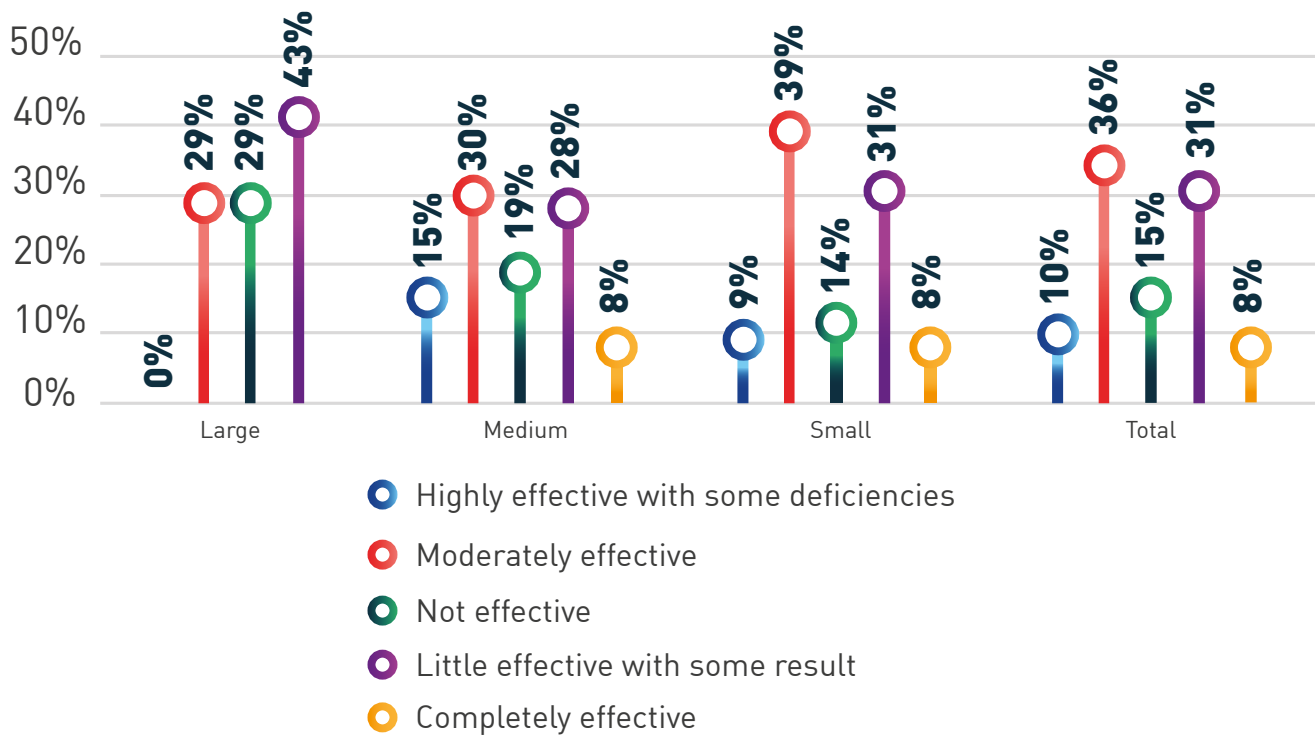
Figure 25. Does the Financial Entity/Institution to Which You Belong Report the Incidents (Successful Attacks) in Information Security (Including Cybersecurity and Fraud Using digital means) to a Law Enforcement Authority in Mexico?



Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Lastly, regardless of the size of the financial entity/institution, 36% of entities in Mexico consider the role of law enforcement authorities to be *moderately effective* with respect to the investigation and prosecution of cybercriminals, while 31% consider it to be *quite ineffective with some results*.

Figure 26. How Do You Consider the Effectiveness of Law Enforcement Authorities in Mexico Regarding the Investigation and Prosecution of Cybercriminals?



Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

When analyzing the results for the Mexican banking sector versus the results for the banking sector of the Latin America and the Caribbean region, it is concluded that there are coincidences regarding the consideration of effectiveness of the aforementioned authorities: i) moderately effective (36% of Mexican banks versus 31% of the banks in the region), and ii) little effective with some results (31% of Mexican banks versus 37% of banks in the region) (Organization of American States, 2018).

3.2.5. Training and Awareness

Lastly, the systematic management of digital security risks must include training and awareness actions within organizations. In particular and regardless of size of the financial entity/institution, more than half (57%) of the Mexican financial entities and institutions have awareness and training plans in matters of information security (including cybersecurity) and fraud prevention using digital means for their collaborators. It is highlighted that 100% of the large entities of the Mexican Financial System and 100% of the securities sector entities have such plans in the country.¹⁹

The foundation of Mexican financial entities and institutions includes preparedness, response and training

¹⁹ Figure 49 of Annex 2 presents the comparison of the result: Does the financial entity/institution to which you belong have awareness and training plans on matters of information security (including cybersecurity and fraud prevention using digital means) for its collaborators? between the different sectors analyzed in the Mexican Financial System.

plans in digital security matters for their collaborators, so it is highlighted that 61% of them are conducted annually, 24% are conducted every six months and the 15% are conducted quarterly.²⁰

On the other hand, 67% of the financial entities and institutions in the country put the capacity of the entity's collaborators to the test to adequately respond to events (successful and unsuccessful attacks) in information security (including cybersecurity) and threats such as phishing and social engineering on an annual basis, 20% every six months and 13% on a quarterly basis.²¹

Lastly, in relation to training and awareness-raising issues, financial entities and institutions identify that the most effective mechanisms for the entity to be more aware of digital security risks are: i) Training and means of internal communication, ii) actions for compliance with legal and/or regulatory requirements, and iii) free publications in magazines, websites and mailing lists. These three (3) mechanisms were also prioritized by the banking sectors (commercial or multiple banking and development banking) and popular savings and loans (SOCAP and SOFIPO) of Mexico.

Table 10. Most Effective Mechanism to Generate Greater Awareness in the Financial Entity/Institution Regarding Digital Security Risks

	Large	Medium	Small	Total
Training and internal communication means	1.29	2.05	2.28	2.19
Legal and/or regulatory requirements	2.17	2.67	2.68	2.66
Free publications in magazines, websites and mailing lists	4.75	3.65	4.14	4.05
Documentation from specialized agencies in the field	4.40	4.48	4.27	4.32
Social networks	4.00	5.12	4.29	4.46
Presentations and debates at conferences	4.33	4.74	4.66	4.66
Specialized subscription services	5.75	5.41	5.36	5.39
Professional associations	7.25	5.91	5.23	5.43
Other	7.50	6.80	7.18	7.10

Note: : 236 records and all mechanisms are prioritized with a number from 1 to 9, where 1 is the most effective mechanism and 9 the least effective mechanism.
Source: GS/OAS based on information collected from Mexican financial entities and institutions

²⁰. Figure 50 of Annex 2 presents the comparison of the result: *How often are such awareness and training plans conducted?* between the different sectors analyzed in the Mexican Financial System.

²¹. Figure 51 of Annex 2 presents the comparison of the result: *How often is the capacity of employees of the financial institution to which you belong put to the test to adequately respond to digital security incidents (successful attacks) (including security aspects of information security, cybersecurity and fraud prevention using digital means) and phishing and social engineering schemes?* between the different sectors analyzed in the Mexican Financial System.

3.3. Impact of Digital Security Incidents

Once the financial entities and institutions that participated in this study had been characterized and once the results had been prepared on the management of digital security risks by the Mexican Financial System, the analysis of the impact of digital security incidents in Mexican financial entities and institutions in 2018 began.

As mentioned, the assets of the sample of financial entities and institutions, which are the basis of the results presented, amount to US\$682.4 billion with net profits of US\$7.1 billion as of December 31, 2018, which makes it possible to affirm that said sample represents the different levels of the country's assets and equity. It is highlighted that the assets reported by banks in the commercial or multiple banking sector contributed US\$429.4 billion which correspond to almost 63% of the total sample.

Table 11. Distribution of the Estimated Asset Value by Sector of the Mexican Financial System (millions of US dollars)

	Large	Medium	Small	Total
Commercial or Multiple Banking	150,503	217,664	61,201	429,368
Development Banking		68,538	27,876	96,414
Securities Sector			17,998	17,998
Popular Savings and Credit Sector (SOCAP)		2,780	2,558	5,338
Popular Savings and Credit Sector (SOFIPO)	3	213	14	230
Non-Banking Financial Intermediaries' Sector		18	2,903	2,921
FINTECH Sector			130,130	130,130
MEXICAN FINANCIAL SYSTEM	150,506	289,213	242,679	682,398

Note: 235 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

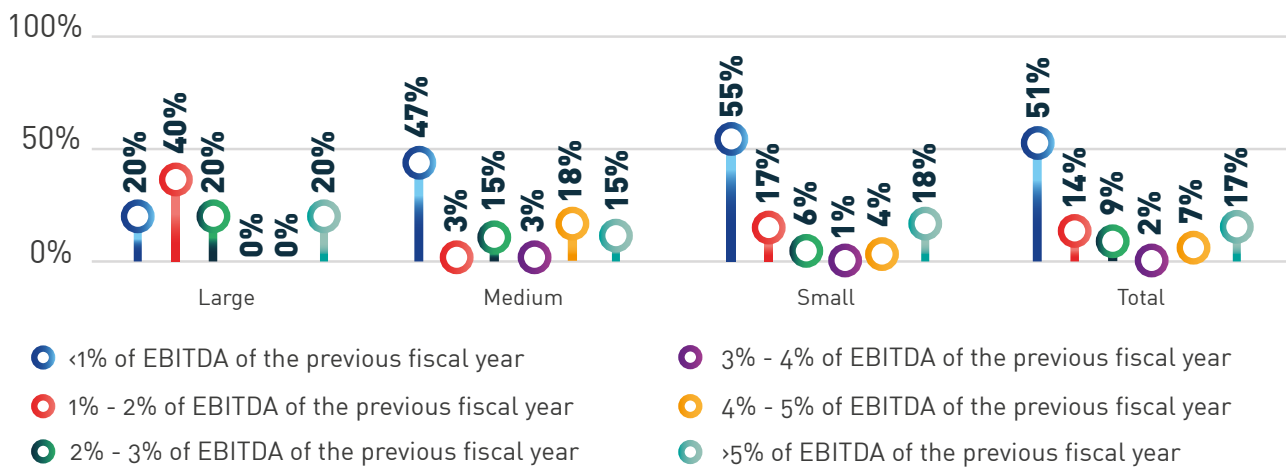
Table 12. Distribution of the Estimated Value of EBITDA by Sector of the Mexican Financial System (millions of US dollars)

	Large	Medium	Small	Total
Commercial or Multiple Banking	1,650	636	564	2,850
Development Banking		1,490	738	2,228
Securities Sector			58	58
Popular Savings and Credit Sector (SOCAP)		47	165	211
Popular Savings and Credit Sector (SOFIPO)	0,005	18	1	19
Non-Banking Financial Intermediaries' Sector		0,05	793	794
FINTECH Sector			991	991
MEXICAN FINANCIAL SYSTEM	1,650	2,190	3,310	7,150

Note: 235 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Studying the financial entities and institutions that responded, it is highlighted that 51% of the entities in the region state that the digital security budget (including aspects of information security, cybersecurity and fraud prevention using digital means) equals, on average, less than 1% of EBITDA of the previous fiscal year, 14% of the entities state that the value of said budget is between 1% and 2% of EBITDA of the previous fiscal year, 9% of the entities report that the value of said budget is between 2% and 3% of EBITDA of the previous fiscal year, 2% of the entities state that the value of said budget is between 3% and 4% of EBITDA of the previous fiscal year, 7% of the entities state that the value of said budget is between 4% and 5% of EBITDA of the previous fiscal year and 17% state that the value of said budget is equivalent to a value greater than 5% of the EBITDA of the previous fiscal year.

Figure 27. Budget of Information Security (including cybersecurity) as a % of EBITDA of the Previous Year



Note: 235 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

The differences between the estimates of this budget in the Mexican banking sector (commercial or multiple banking and development banking) and in the average of the banking sector in the Latin America and the Caribbean region are of note,²² where it can be seen that 43% of banks in Mexico versus 61% of banks in the region state that this budget is on average less than 1% of EBITDA of the previous fiscal year, 37% of banks in Mexico versus 34% of banks in the region state that the value of said budget is between 1% and 5% of EBITDA of the previous fiscal year and 20% of banks in Mexico versus 5% of banks in the region state that the value of said budget equals a value greater than 5% of EBITDA of the previous fiscal year (Organization of American States, 2018).

From the analysis of the sample results, it can be inferred that the value of the budget for information security (including cybersecurity) and fraud prevention using digital means as a percentage of EBITDA of the previous fiscal year is equivalent to 2.18%. It is also estimated that this budget for large entities is equivalent to 2.30% of EBITDA of the previous fiscal year, for medium-sized entities it is equivalent to 2.51% of EBITDA of the previous fiscal year and for small entities it is equivalent to 2.04% of EBITDA of the previous fiscal year.

²² Figure 52 of Annex 2 presents the comparison of the Dynamic of the digital security budget in the last year between the different sectors analyzed in the Mexican Financial System.

Table 13. Digital Security Budget as a % of EBITDA of the Previous Year by Sector of the Mexican Financial System

	Large	Medium	Small	Total
Commercial or Multiple Banking	2.30%	3.05%	1.88%	2.38%
Development Banking		1.63%	2.50%	2.00%
Securities Sector			2.57%	2.57%
Popular Savings and Credit Sector (SOCAP)		2.26%	1.65%	1.90%
Popular Savings and Credit Sector (SOFIPO)		3.33%	5.00%	4.00%
Non-Banking Financial Intermediaries' Sector			1.82%	1.82%
FINTECH Sector			2.65%	2.65%
MEXICAN FINANCIAL SYSTEM	2.30%	2.51%	2.04%	2.18%

Note: 235 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

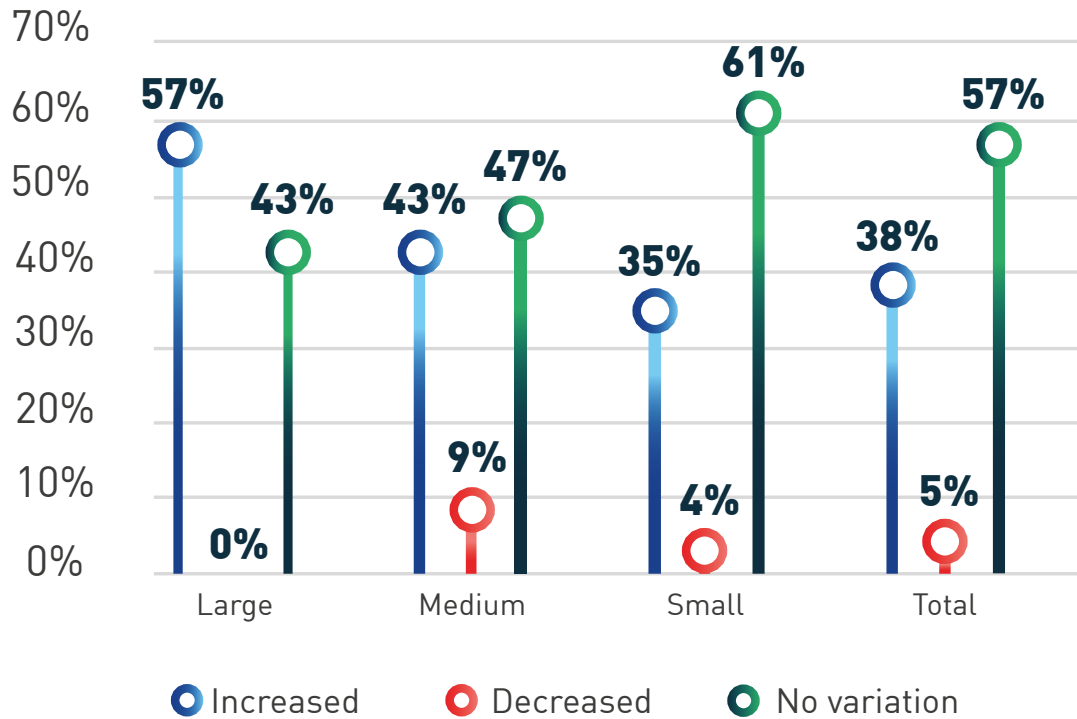
When analyzing the Mexican Financial System by sector, it is seen for example that the budget for information security (including cybersecurity) and fraud prevention using digital means for the commercial or multiple banking sector is equivalent to 2.38% of EBITDA of the previous fiscal year, while said budget for the non-banking financial intermediaries' sector is equivalent to 1.82% of EBITDA of the previous fiscal year.

In addition, compared to the immediately previous fiscal year, 57% of the financial entities and institutions in the country state that the budget for information security (including cybersecurity) and fraud prevention using digital means remained unchanged; 38% said it had increased and only 5% said it had decreased. However, the specific results for the Mexican banking sector (commercial or multiple banking and development banking) are different: 31% of the banks in the country state that said budget remained unchanged, 64% state that it increased and only 5% say that it decreased.

When analyzing the results in detail, differences were observed for each size of financial entity and institution in the Mexican Financial System. It is highlighted that for 57% of large entities, 43% of medium-sized entities and 35% of small entities, the digital security budget increased compared to the immediately previous fiscal year. On the other hand, for 43% of large entities, 47% of medium-sized entities and 61% of small entities, the digital security budget remained the same as that of the immediately preceding fiscal year.²³

²³Figure 53 of Annex 2 presents the comparison of the result: *Growth of the information security budget (including cybersecurity) and fraud prevention using digital means of the financial entity/institution between the different sectors analyzed in the Mexican Financial System.*

Figure 28. Dynamics of the Budget for Information Security (Including Cybersecurity) and Fraud Prevention Using digital means in the Last Year

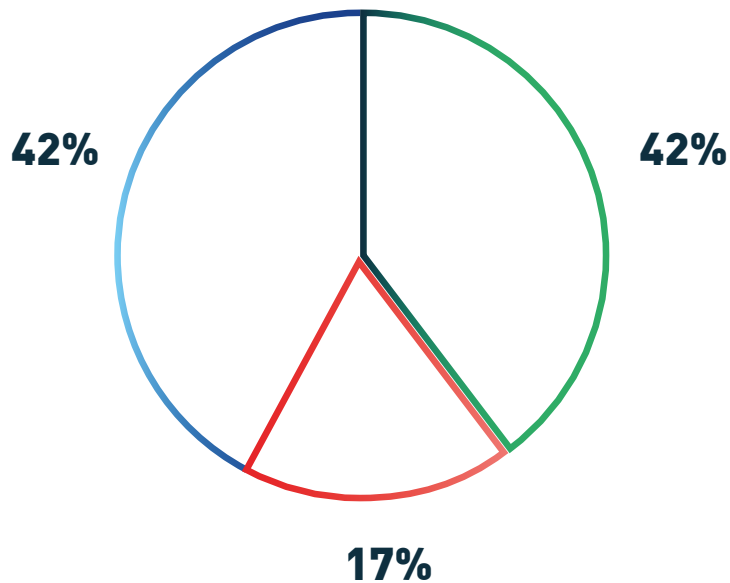


Note: 235 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Of the total of financial entities and institutions that state that the digital security budget increased compared to the immediately previous fiscal year, 76% indicated that said increase was due to *Regulatory Compliance*, 54% said it is due to *Compliance with new internal policies*, and 38% to *Business Continuity/Disaster Recovery*. In relation to the banking sector, it can be seen that, on average, Mexican banks and banks in the Latin American and Caribbean region agree that the increase is mainly due to *Regulatory Compliance* (70% of banks in Mexico versus 62% of banks in the region) and *New cybersecurity threats due to the use of NICT* (48% of banks in Mexico versus 54% of banks in the region) (Organization of American States, 2018).

On the other hand, of the total of financial entities and institutions that state that the digital security budget decreased compared to the immediately previous fiscal year, 42% indicated that it is due to a *Decrease in the financial entity/institution profits*, the 42% a *Budget adjustment due to high costs associated with information security* and 17% a *Change and transformation of the business with an impact on risk appetite*.

Figure 29. Reasons for the Decrease in the Budget for Information Security (Including Cybersecurity) and Fraud Prevention Using Digital means

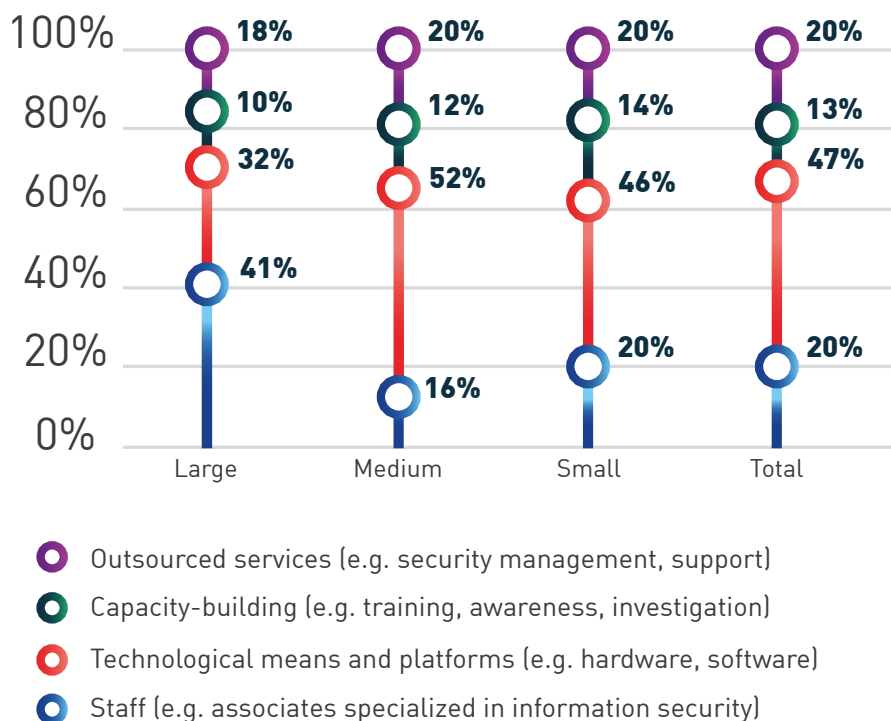


- Budget adjustment due to high costs associated to information security
- Business change or transformation with impact on risk appetite
- Decrease of financial entity/institution profit

Note: 12 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

From the budget allocated by an average financial entity/institution of the Mexican Financial System for information security (including cybersecurity) and fraud prevention using digital means, the following distribution can be seen: 47% in *Platforms and technological means* (e.g. hardware, software), 20% in *Staff* (e.g. collaborators specialized in Information Security), 20% in *outsourced services* (e.g. security management, outsourcing, support) and the 13% in *capacity building* (e.g. training, awareness, research).

Figure 30. Distribution of the Budget for Information Security (Including Cybersecurity) and Fraud Prevention Using Digital means of the Financial Entity/Institution



Note: 196 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

When comparing the distribution of the above-mentioned budget between the Mexican banking sector (commercial or multiple banking and development banking) and the average of the banking sector of the Latin America and the Caribbean region,²⁴ the following can be seen: i) 35% in Mexico versus 43% in the region for *Platforms and technological means (e.g. hardware, software)*, ii) 23% in Mexico versus 22% in the region for *Staff (e.g. collaborators specialized in Information Security)*, iii) 31% in Mexico versus 22% in the region for *outsourced services (e.g. security management, outsourcing, support)*, and, iv) 11% in Mexico versus 13% in the region for *capacity building (e.g. training, awareness, research)* (Organization of American States, 2018).

Based on the estimate of the budget for information security (including cybersecurity) and fraud prevention using digital means as a percentage of EBITDA of the immediately preceding year of the country's financial entities and institutions, by organization size, and the estimate of the percentage of the budget allocated to staff, it follows that: i) the budget assigned to an average member of the digital security team by a large entity in the country in 2018 was approximately US\$67,674 per year, ii) the budget assigned to an average member of the digital security team by a medium-sized entity in the country in 2018 was approximately US\$49,453 per year, and iii) the budget assigned to an average member of the digital security team by a small entity in the country in 2018 was approximately US\$12,488 per year.

The average value for the Mexican Financial System, regardless of size, was approximately US\$25,557

²⁴ Figure 54 of Annex 2 presents the comparison of the result: *Distribution of the information security budget (including cybersecurity) and fraud prevention using digital means of the financial entity/institution* between the different sectors analyzed in the Mexican Financial System.

per year versus a budget assigned to an average member of the digital security team by a bank in the Latin America and the Caribbean region which was approximately US\$19,437 per year (Organization of American States, 2018).

On the other hand, from the information collected from the sample of financial entities and institutions, it is estimated that the return on investment (ROI) in information security (including cybersecurity) and fraud prevention using digital means was approximately 10.94%. When analyzing by entity size, we obtain: i) 15% for a large entity in the country (represented by commercial or multiple banking), ii) 9.58% for a medium-sized entity in the country, and iii) 10.36% for a small entity of the Mexican Financial System.

Table 14. Return on Investment (ROI) in Information Security (Including Cybersecurity) and Fraud Prevention Using digital means

	Large	Medium	Small	Total
Commercial or Multiple Banking	15.00%	7.50%	17.50%	11.56%
Development Banking				
Securities Sector			2.50%	2.50%
Popular Savings and Credit Sector (SOCAP)		13.75%	5.00%	9.38%
Popular Savings and Credit Sector (SOFIPO)				
Non-Banking Financial Intermediaries' Sector			17.50%	17.50%
FINTECH Sector			12.50%	12.50%
MEXICAN FINANCIAL SYSTEM	15.00%	9.58%	10.36%	10.94%

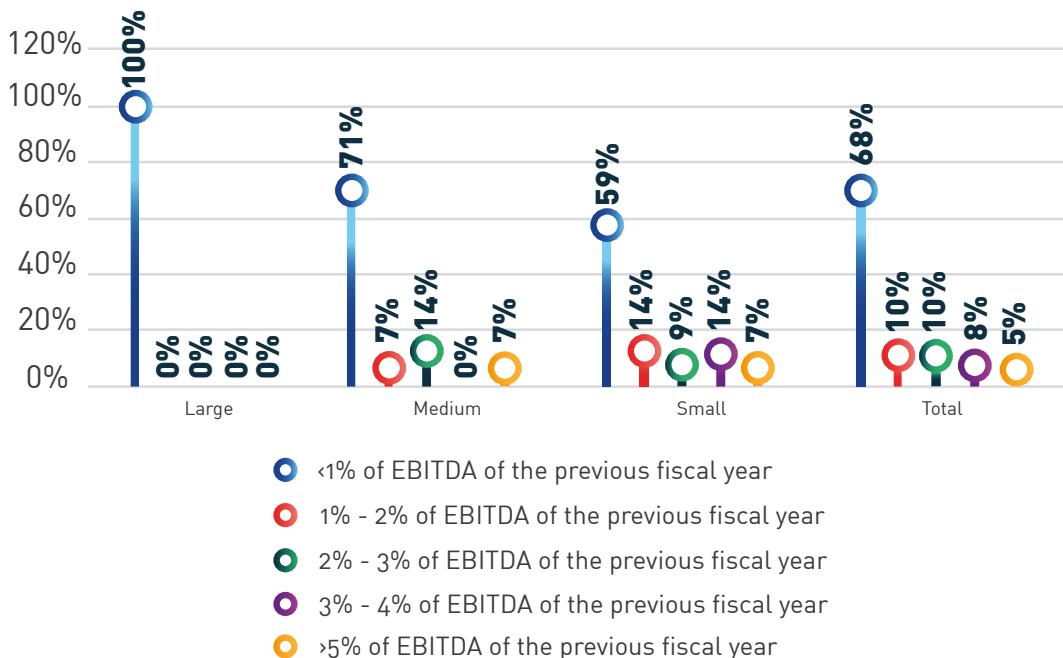
Note: 19 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Regarding the estimates of the return on the investment in digital security: i) 33% of the medium-sized entities and 20% of the small entities consider that they are low returns, ii) 20% of the small entities consider that they are average returns, iii) 100% of large entities, 33% of medium-sized entities and 40% of small entities consider them high returns, and iv) 33% of medium-sized entities and 20% of small entities consider them to be very high returns.

The financial entities and institutions that provided information²⁵ show that 68% of the entities in the country state that the cost of responding and recovering from incidents (successful attacks) in information security (including cybersecurity) is equivalent on average to less than 1% of EBITDA of the previous fiscal year, 10% of the entities state that the value of said cost is between 1% and 2% of EBITDA of the previous fiscal year, 10% of the entities state that the value of said cost is between 2% and 3% of EBITDA of the previous fiscal year, 8% of the entities state that the value of said cost is between 3% and 4% of EBITDA of the previous fiscal year and 5% state that the value of said cost equals a value greater than 5% of EBITDA of the previous fiscal year.

The analysis also allows inferring that as the size of the financial entity and institution increases, the total cost of response and recovery from digital security incidents decreases as a % of EBITDA of the immediately preceding year. For example, 100% of large entities state that the value of said cost is less than 1% of EBITDA of the previous fiscal year, while 71% of medium-sized entities and 59% of small entities state that said cost is in that range.

Figure 31. Cost of Response and Recovery from Incidents (Successful Attacks) in Information Security (Including Cybersecurity) as a % of EBITDA of the Previous Year



Note: 40 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

²⁵ Figure 55 of Annex 2 presents the comparison of the result: Did the financial entity/institution to which you belong estimate the total cost of response and recovery from incidents (successful attacks) in information security (including cybersecurity) for the last fiscal year? between the different sectors analyzed in the Mexican Financial System.

The similarity between the estimates of said cost is highlighted between the Mexican banking sector (commercial or multiple banking and development banking) with the average of the banking sector in the Latin America and the Caribbean region²⁶ where it is observed that 76% of banks in Mexico versus 73% of banks in the region state that said cost is equivalent on average to less than 1% of EBITDA of the previous fiscal year and 24% of banks in Mexico versus 27% of banks in the region state that the value of said budget is between 1% and 5% of EBITDA of the previous fiscal year (Organization of American States, 2018).

From the analysis of the sample results, it can be inferred that the value of the cost of response and recovery from incidents (successful attacks) in information security (including cybersecurity) as a % of EBITDA of the previous year is equivalent to 1.59%. It is also estimated that this budget for large entities is equivalent to 1% of EBITDA of the previous fiscal year, for medium-sized entities it is equivalent to 1.54% of EBITDA of the previous fiscal year and for small entities it is equivalent to 1.73% of EBITDA of the previous fiscal year.

Table 15. Cost of Response and Recovery from Incidents (Successful Attacks) in Information Security (Including Cybersecurity) by Sector of the Mexican Financial System

	Large	Medium	Small	Total
Commercial or Multiple Banking	1.00%	1.39%	1.80%	1.42%
Development Banking		1.00%	1.00%	1.00%
Securities Sector			2.50%	2.50%
Popular Savings and Credit Sector (SOCAP)		2.00%	1.13%	1.56%
Popular Savings and Credit Sector (SOFIPO)			1.00%	1.00%
Non-Banking Financial Intermediaries' Sector			1.70%	1.70%
FINTECH Sector			2.63%	2.63%
MEXICAN FINANCIAL SYSTEM	1.00%	1.54%	1.73%	1.59%

Note: 40 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

²⁶ Figure 56 of Annex 2 presents the comparison of the result: *Cost of response and recovery from incidents (successful attacks) in information security (including cybersecurity) as a % of EBITDA of the immediately preceding year* between the different sectors analyzed in the Mexican Financial System.

When analyzing the Mexican Financial System by sector, it can be seen, for example, that the cost of responding to and recovering from incidents (successful attacks) in information security (including cybersecurity), as well as the commercial or multiple banking sector, is equivalent to 1.42% of EBITDA of the previous fiscal year, while for securities sector it is equivalent to 2.50% of EBITDA of the previous fiscal year.

Based on the information collected from the Mexican financial entities and institutions that participated in the development of this study, it was possible to analyze some average indicators for the country and by organization size that allow estimating the impact of digital security incidents during 2018, for example: i) the annual total budget and cost related to digital security as a % of EBITDA of the immediately previous year, ii) the total annual cost of response and recovery from digital security incidents per financial entities/institutions of the Mexican Financial System, and iii) the total annual cost of response and recovery from digital security incidents of financial entities and institutions of the Mexican Financial System.

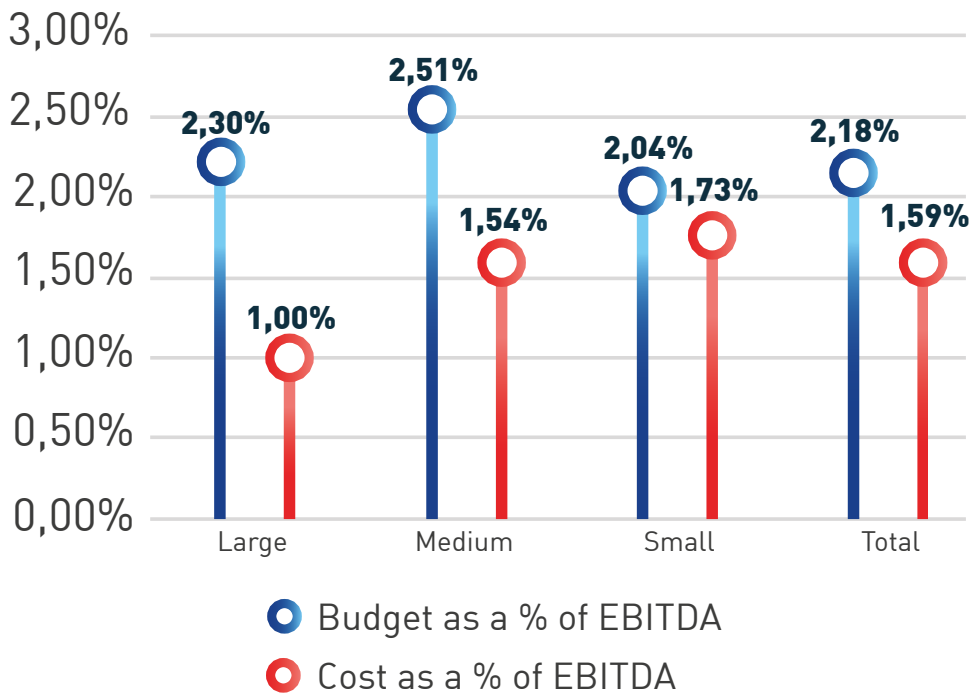
Table 16. Estimate of the Budget and Total Annual Cost Related to Digital Security of the Immediately Preceding Year (millions of US dollars)

	Budget by sector				Cost by sector			
	Large	Medium	Small	Total	Large	Medium	Small	Total
Multiple or Commercial Banking	38	19	11	68	17	9	10	35
Development Bank		24	18	43		15	7	22
Securities Sector			1	1			1	1
Savings and Loan Cooperatives (SOCAP)		1	3	4		1	2	3
Popular Finance Corporations (SOFIPO)		1	0	1		0	0	0
Non-Banking Finance Intermediary Sector (Credit Unions)			14	14			13	13
FINTECH Sector			26	26			26	26
MEXICAN FINANCIAL SYSTEM	38	45	74	157	17	34	57	107

Source: GS/OAS based on information collected from Mexican financial entities and institutions

From the previous analysis and from the sample of financial institutions and entities of the Mexican Financial System that reported information, on average, it is concluded that: i) the budget destined to digital security by an average financial entity and institution in the region is equivalent to approximately 2.18% of EBITDA of the immediately preceding year (versus 2.09% for the banking sector in the Latin America and the Caribbean region), and ii) the total cost of response and recovery from digital security incidents for an average financial entity/institution in the region is equivalent to approximately 1.59% of EBITDA of the immediately preceding year (versus 1.52% for the banking sector in the Latin America and the Caribbean region).

Figure 32. Budget and Cost of Response and Recovery from Incidents (Successful Attacks) in Information Security (Including Cybersecurity) as a % of EBITDA of the Previous Year



Source: GS/OAS based on information collected from Mexican financial entities and institutions

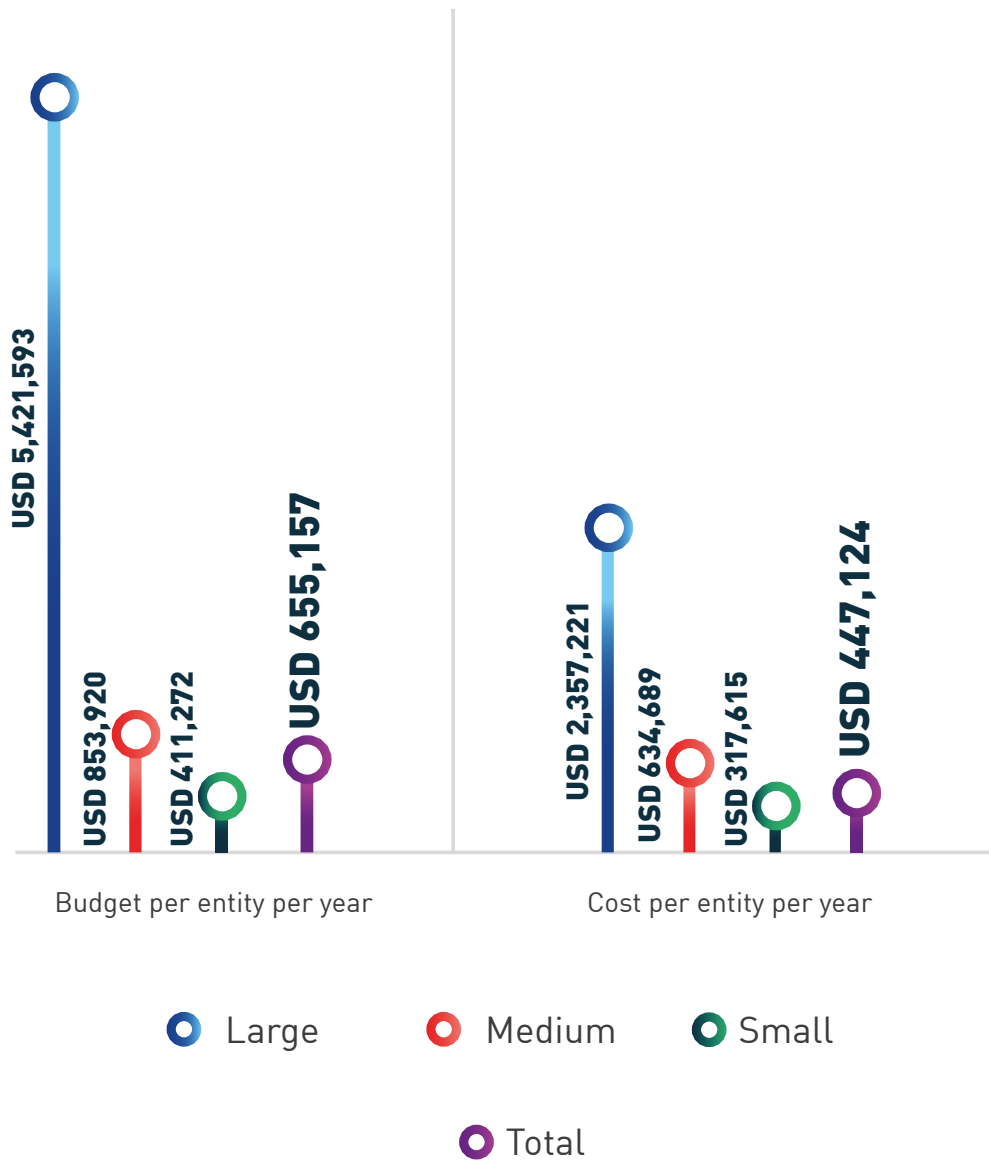
Table 17. Budget and Cost of Response and Recovery from Incidents (Successful Attacks) in Information Security (Including Cybersecurity) as a % of EBITDA of the Previous Year by Sector

	Budget as a % of EBITDA for each sector				Cost as a % of EBITDA for each sector			
	Large	Medium	Small	Total	Large	Medium	Small	Total
Multiple or Commercial Banking	2.30%	3.05%	1.88%	2.38%	1.00%	1.39%	1.80%	1.42%
Development Bank		1.63%	2.50%	2.00%		1.00%	1.00%	1.00%
Securities Sector			2.57%	2.57%			2.50%	2.50%
Savings and Loan Cooperatives (SOCAP)		2.26%	1.65%	1.90%		2.00%	1.13%	1.56%
Popular Finance Corporations (SOFIPO)		3.33%	5.00%	4.00%			1.00%	1.00%
Non-Banking Finance Intermediary Sector (Credit Unions)			1.82%	1.82%			1.70%	1.70%
FINTECH Sector			2.65%	2.65%			2.63%	2.63%
MEXICAN FINANCIAL SYSTEM	2.30%	2.51%	2.04%	2.18%	1.00%	1.54%	1.73%	1.59%

Source: GS/OAS based on information collected from Mexican financial entities and institutions

When analyzing the results in absolute terms, it is estimated that the total cost of response and recovery from digital security incidents for an average large entity is approximately US\$2,357,221 per year, for an average medium-sized entity it is approximately US\$634,689 per year and for an average small entity it is equivalent to approximately US\$317,615 per year.

Figure 33. Budget and Cost of Response and Recovery from Incidents (Successful Attacks) in Information Security (Including Cybersecurity)



Source: GS/OAS based on information collected from Mexican financial entities and institutions

Table 18. Budget and Cost of Response and Recovery from Incidents (Successful Attacks) in Information Security (Including Cybersecurity) by Sector (thousands of US dollars)

	Budget per financial entity/institution				Cost per financial entity/institution			
	Large	Medium	Small	Total	Large	Medium	Small	Total
Multiple or Commercial Banking	6,325	1,492	759	2,060	2,750	680	725	1,075
Development Bank		4,843	4,613	4,740		2,980	1,845	2,476
Securities Sector			167	167			162	162
Savings and Loan Cooperatives (SOCAP)		39	38	38		35	26	28
Popular Finance Corporations (SOFIPO)		84	7	43		0	1	1
Non-Banking Finance Intermediary Sector (Credit Unions)			249	245			233	229
FINTECH Sector			1,544	1,544			1,530	1,530
MEXICAN FINANCIAL SYSTEM	5,422	854	411	655	2,357	635	318	447

Source: GS/OAS based on information collected from Mexican financial entities and institutions



CYBERSECURITY RECOMMENDATIONS FOR THE MEXICAN FINANCIAL SYSTEM

Based on the findings, a set of cybersecurity recommendations was prepared for the Mexican Financial System. For this purpose, two (2) target groups were established as recipients of the recommendations: i) the Mexican financial entities and institutions, and ii) the financial system authorities and regulatory bodies and the law enforcement authorities of the Government of Mexico.

4.1. For the Financial Entities and Institutions of the Mexican Financial System

It is important to note that these suggestions are generally formulated and they may be obvious for some organizations, but they are included taking into account the heterogeneity of financial entities and institutions in the country and their different levels of development and maturity in digital security aspects. The recommendations are grouped using the same thematic structure adopted in the information collection instrument used.

4.1.1. In Aspects of Preparedness and Governance

- As far as possible, have one single responsible body or corporate governance body to lead information security (including cybersecurity) and fraud prevention using digital means, mainly in the banking sectors (commercial or multiple banking and development banking) and popular savings and loans (SOCAP and SOFIPO).
- Although as the size of the banking entity increases, the aim is to specialize various areas of the organization in information security (including cybersecurity) and fraud prevention using digital means, it must be guaranteed that these areas work coordinately and effectively.
- Properly size the work teams dedicated to information security matters, carry out safety evaluations of the collaborators, adequately segregate roles and functions, guarantee knowledge management processes that break up “one person” divisions, and establish mechanisms to elevate employee loyalty and retention,

relying on the development of human talent and considering incentive plans.

- Have formal mechanisms for the selection of outsourced service providers, considering that they could require access to sensitive information, with adequate selection criteria and with clear contractual conditions that guarantee the protection of personal data, confidentiality, service-level agreements and other requirements that would “shield” the outsourced activities.
- Establish clear mechanisms to ensure knowledge of information security (including cybersecurity) risk management by the decision-making bodies in the organizations (Director’s Office or General Management or Presidency) and to periodically conduct awareness processes with the active participation of its members, in order to raise the priority and support for these issues, mainly in medium-sized and small entities of the sectors of popular savings and credit (SOCAP and SOFIPO), of non-banking financial intermediaries and FINTECH.

- Carry out a regular review of best practices in government frameworks, security and/or international standards, as well as the local and international regulatory framework applicable to the various sectors and financial entities and institutions, mapping and prioritizing them for application.
- It is of the utmost importance to carry out the processes of adoption and application of regulatory frameworks (local and international), best practices and/or international standards, aimed at going beyond reviewing “checklists” in order for them to really become processes of positive transformation, guided by continuous improvement and strengthening of the culture of security.

4.1.2. In aspects of Detection and Analysis of Digital Security Events

- Ensure that the prioritization of digital security actions, processes and programs to protect the critical information systems of the financial entity/institution correspond to a plan derived from the needs of adoption and application of regulatory frameworks (local and international), better practices and/or international standards. It is vital for this plan to have, as one of its targets, the elevation of cyber resilience.
- There should be mechanisms to verify the proper detection and analysis capabilities of security events, preferably through collaboration with public or private incident response teams, mainly in the financial entities and institutions of the popular savings and credit sectors (SOCAP

and SOFIPO) and of non-banking financial intermediaries. This means validating whether the developed capacities are being able to predict or detect threats with the same degree of effectiveness as other response teams.

- Prioritize the development of capacities using emerging digital technologies, such as Big Data, Artificial Intelligence and related (such as Cognitive Computing and Machine Learning), which have an important potential in the optimization of detection and prevention resources, especially in the financial entities and institutions of the popular savings and credit sectors (SOCAP and SOFIPO) and of non-banking financial intermediaries.

- Extend detection and prevention to the sphere of interaction by users, for example, by incorporating detection or prevention solutions that users can install on their devices, on a voluntary basis, which also increases user perception of trust in the service.

4.1.3. In Aspects of Digital Security Incident Management, Response, Recovery and Reporting

- Guarantee the design and implementation of a prioritization, containment, response and recovery strategy from events (successful attacks and unsuccessful attacks) in information security (including cybersecurity) against financial entities and institutions, especially in the sectors of popular savings and loans (SOCAP and SOFIPO) and non-banking financial intermediaries. It must articulate the participation of third parties, as appropriate to the different stages, processes or associated protocols, specifically defining the responsibilities and moments of intervention by suppliers, escalation or intervention of external response teams (for example, incident response teams in the sector or in the country, if applicable).
- Investigate the source that creates incidents (successful attacks) in information security (including cybersecurity), mainly in the financial entities and institutions of the popular savings and credit sector (SOCAP and SOFIPO).
- Support investigations and follow the protocols required by law enforcement authorities and the best practices applicable to the digital evidence chain of custody (for example, that facilitate national cooperation) that are relevant to the investigation processes.
- Actively participate in partnerships to share the conclusions and lessons learned on the management of events (successful attacks and unsuccessful attacks), which facilitate crime identification and

prevention, as well as the development of holistic solutions to manage cyber risk.

- Train and specialize staff allocating adequate budgets to perform maturity assessment processes using an information security (including cybersecurity) methodology on a regular basis, by suitable external agents, to establish opportunities for improvement, prioritization and the updating of the related plans and strategies, especially in medium-sized and small financial entities and institutions of the securities, popular savings and credit sectors (SOCAP and SOFIPO) and non-banking financial intermediaries.
- Take reasonable and appropriate technological measures to protect information against loss, misuse and destruction, constantly complying with the fundamental security principles (confidentiality, integrity, availability and traceability).
- Establish, from the point of view of technology and its processes, the actions necessary to guarantee that the information is protected throughout the information life cycle, including as a minimum: i) periodic vulnerability assessments of applications and infrastructure, ii) timely remediation of the problems found in those assessments, iii) adoption of safe development methodologies to minimize the risk of introducing new vulnerabilities in the production of business solutions, iv) adopt controls to restrict the use of solutions without manufacturer support (due to product life cycle conditions)

and/or illegal software, and, v) adopt processes to perform the installation of security updates systematically, among others.

- Guarantee adequate communication to clients of the reporting mechanisms the financial entity/

institution has available, in the event that they are victims of incidents (successful attacks) in information security (including cybersecurity).

4.1.4. In aspects of Training and Awareness

- Instill cybersecurity concepts and good practices, especially targeting the areas most related to innovation and digital transformation processes, especially in medium-sized/small financial entities and institutions in the sectors of securities, popular savings and credit (SOCAP and SOFIPO) and of non-banking financial intermediaries.
- Actively participate in discussion spaces (forums, workshops, conventions, etc.).
- Carry out event prevention campaigns for i) phishing, ii) spyware (malware or Trojans), iii) social engineering, and iv) theft of financial service clients credentials (partners, associates or users).
- Assimilate design criteria for digitally-based products and services under premises of “security from the start”.
- Increase the banking entity’s percentage of investment for workforce capacity building (e.g. training, awareness, research), especially in its early development to close the gap in the trained cyber staff, and to increase or maintain the available work force on digital security issues in order to develop and strengthen an agile cyber resilience workforce, which may require greater education capacity and incentives.
- Provide training plans with specific target audiences (internal employees, insourcing, suppliers, customers, etc.) aimed at raising the digital safety culture, capacity and awareness building (as the case may be), guaranteeing their implementation periodically and establishing evaluations to determine impact. Training must include the development of early cyber skills in order to close the gap in terms of trained personnel.
- Increase and maintain the specialized digital security workforce, through specialized training and incentives, in order to count on an agile and robust team that supports the organization’s cyber resilience.

4.1.5. In Aspects Related to the Impact of Digital Security Incidents

- Invest in information security (including cybersecurity) and fraud prevention using digital means, mainly in the securities, popular savings and credit (SOCAP and SOFIPO) and non-banking financial intermediaries' sectors.
- Establish responsibilities within the financial entity/institution to concentrate or centralize the digital security incident registry and determine the quantification methods of the economic impact on the organization.
- Have cost centers or other methods for determining the classification of digital security investments and recurrent expenses, so that its weight can be accurately assessed within the organization's other items and its behavior.
- Establish, as accurately as possible, the rate of return of investments in information security (including cybersecurity) and fraud prevention using digital means. Start from an adequate valuation of the bank's assets, as well as an estimate of the costs associated with the impact derived from possible digital security incidents.
- Communicate strategically to senior management and government bodies that the resources allocated to digital security are not a cost, but actually an investment; and that protection against digital incidents should be an integral part of the business strategy, given their likely high impact and repercussions to the organization.

4.2. For the Financial System Authorities and Regulatory Bodies and Law Enforcement Authorities of the Government of Mexico

- Carry out the review of the catalog of critical infrastructures and see the dependency levels that the financial institutions / entities of the Mexican Financial System have, in order to assess their current status, the prioritization of the management of their associated risks and, in particular, the impact and the affectation that attacks to other infrastructures (for example, telecommunications or energy) could have on the mentioned financial system.
- Coordinate efforts with associations or associations related to the Mexican Financial System aimed at the development of digital security capabilities, preferably regulated through an agenda with expected results, milestones, resources and responsible parties.
- Strengthen knowledge management networks based on the capacities of the different response teams of entities and institutions of the Mexican Financial System, other sector teams and the national focal point, incorporating the voluntary participation of other government agencies, the private sector, academia, technical and professional communities and non-governmental organizations, according to their degree of participation in the financial system.
- Evaluate the relevance of developing cyber-exercises that generate challenging spaces to promote digital security capacity building in the Mexican Financial System.
- Continue with the reinforcement of the capacities of the law enforcement authorities, regarding support for the response, investigation and prosecution of cybercriminals which will contribute to the application of effective sanctions to those who attack the actors in the Mexican Financial System.
- Socialize protocols for the management of digital evidence and promote appropriate chain of custody practices, as required by competent authority provisions.
- Issue guidelines, recommendations and instructions, as the case may be, derived from the periodic review of digital security best practices and/or applicable

international standards, as well as the international regulatory framework applicable to the Mexican Financial System, and, if necessary, issue the necessary legal instruments for application.

- At the moment of creating or updating regulations related to cybersecurity, continue with the adoption of regulations in accordance with frameworks already established by the issuers of international standards, reducing regulatory fragmentation, taking advantage of the lessons learned and providing stability throughout the Mexican Financial System.

- Establish a strategy for securing the chain that makes up the stability of the Mexican Financial System in key services such as the Interbank Electronic Payment System (SPEI) and develop a legal framework to facilitate the transnational persecution of cybercriminals.

- Verify that regulations are based on principles and are balanced against the risks they address, in order to maximize effectiveness, while avoiding unnecessary expenses and burdens of control.

- Be careful about standardizing the technical details of security and business control systems, as this could increase vulnerability rather than decrease it.

- Conduct periodic evaluations of the recent provisions of the National Banking and Securities Commission (CNBV), in particular, compliance with the formulation of secure master plans and the materialization of the position of security officer reporting directly to the general director of financial institutions, in order to measure the degree of implementation and effectiveness of the measures.

- Establish disclosure and socialization mechanisms for the progress of the Incident Response Group (IRG) among authorities of the Mexican Financial System: Banco de México, SHCP, CNBV, CONSAR, CONDUSEF, CNSF and PGR; and to have exercises that put into practice the reaction protocol of the IRG, analyze its performance and guide actions for its permanent improvement.

- Evaluate the effectiveness of the obligation of financial entities and institutions to report the digital security incidents against them, in accordance with the provisions of the Financial System Stability Council (CESF). It must be ensured that the purpose of this report is to be the basis for the inquiries, investigations and associated work required for the understanding of the incident and its scope, as well as the understanding of the context in which it occurred, in order to alert and take complementary measures by other entities and financial institutions.

- Verify, in entities and financial institutions, the provision of reporting mechanisms which their clients can use, in the event of being victims of digital security incidents, and evaluate their effectiveness.

- Implement information exchange mechanisms between the public and private sectors that facilitate the early detection of patterns to allow organizations to protect themselves optimally against cyber-attacks.

- Establish measuring mechanisms that allow for a quantitative evaluation and facilitate the assessment of the progress in implementing the Principles for Strengthening the Security of Information in the Financial System, issued by the CESF. Strong legislation for the exchange of information facilitates that the public and private sectors share information about cyber threats in a timely manner; allows the government to declassify certain threat information so that it can be used by the private sector for its protection; and provides strong protection against the responsibilities of organizations that share appropriate information from cyber threats.

- Establish a unified dashboard that allows to quantify and facilitate the assessment of the progress made in materializing the “Principles for reinforcing the security of information in the financial system”, issued by the CESF.

- Promote knowledge-transfer and capacity-building processes through collaboration, assistance and cooperation, locally and internationally.

BIBLIOGRAPHY

IDB & FELABAN. (2014). PYME y Bancos en América Latina y el Caribe. El “Missing Middle” y los Bancos - Séptima Encuesta 2014. Obtenido de www.felaban.net:
https://www.felaban.net/archivos_publicaciones/archivo20150702202150PM.pdf

OAS. (2018). Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. Obtenido de www.oas.org: <https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf>

SECRETARÍA DE COMUNICACIONES Y TRANSPORTE DE MÉXICO & OAS. (2019). Estudio sobre hábitos de los usuarios en Ciberseguridad en México. Obtenido de:
https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf

WEF. (2019). Informe Global de Riesgos del Foro Económico Mundial 2019. Obtenido de www.weforum.org: <https://www.weforum.org/reports/the-global-risks-report-2019>

ANEXO 1

Information on the Sample of Entities and Institutions of the Mexican Financial System

Table 19. Information of the Mexican Financial System taking into account reports from the National Banking and Securities Commission (CNBV) of Mexico

	Large	Medium	Small	Total	
Multiple or Commercial Banking	6	13	14	33	
Development Bank		5	4	9	
Securities Sector			9	9	
Savings and Loan Cooperatives (SOCAP)		27	71	98	
Popular Finance Corporations (SOFIPO)	1	7	7	15	
Non-Banking Finance Intermediary Sector (Credit Unions)		1	58	59	
FINTECH Sector			17	17	
MEXICAN FINANCIAL SYSTEM	7	53	180	240	entities

ASSETS					
	Large (millions of USD)	Medium (millions of USD)	Small (millions of USD)	Total (millions of USD)	
Multiple or Commercial Banking	USD 150,503	USD 217,664	USD 61,201	USD 429,368	
Development Bank	USD 0	USD 68,538	USD 27,876	USD 96,414	
Securities Sector	USD 0	USD 0	USD 17,998	USD 17,998	
Savings and Loan Cooperatives (SOCAP)	USD 0	USD 2,780	USD 2,558	USD 5,338	
Popular Finance Corporations (SOFIPO)	USD 3	USD 213	USD 14	USD 230	
Non-Banking Finance Intermediary Sector (Credit Unions)	USD 0	USD 18	USD 2,903	USD 2,921	
FINTECH Sector	USD 0	USD 0	USD 130,130	USD 130,130	
MEXICAN FINANCIAL SYSTEM	USD 150,506	USD 289,213	USD 242,679	USD 682,398	millions

CNBV Info					
	CNBV Date of report	Type of exchange	Entities	Assets (millions of Mex pesos)	Assets (millions of USD)
Multiple or Commercial Banking	dic-18	\$19,6566	50	\$9,475,000	USD 482,026
Development Bank	sep-18	\$18,7231	6	\$1,973,600	USD 105,410
Securities Sector	sep-18	\$18,7231	35	\$627,800	USD 33,531
Savings and Loan Cooperatives (SOCAP)	sep-18	\$18,7231	157	\$149,539	USD 7,987
Popular Finance Corporations (SOFIPO)	sep-18	\$18,7231	46	\$32,459	USD 1,734
Non-Banking Finance Intermediary Sector (Credit Unions)	sep-18	\$18,7231	84	\$63,254	USD 3,378
FINTECH Sector					
MEXICAN FINANCIAL SYSTEM			378		87%

of total assets

	% of sample entities of the total in Mexico	% of sample assets the totaofl in Mexico
Multiple or Commercial Banking	66%	89%
Development Bank	150%	91%
Securities Sector	26%	54%
Savings and Loan Cooperatives (SOCAP)	62%	67%
Popular Finance Corporations (SOFIPO)	33%	13%
Non-Banking Finance Intermediary Sector (Credit Unions)	70%	86%

FINTECH Sector

MEXICAN FINANCIAL SYSTEM

63%

of total entities

	EBITDA			
	Large (millions of USD)	Medium (millions of USD)	Small (millions of USD)	Total (millions of USD)
Multiple or Commercial Banking	USD 1,650	USD 636	USD 564	USD 2,850
Development Bank	USD 0	USD 1,490	USD 738	USD 2,228
Securities Sector	USD 0	USD 0	USD 58	USD 58
Savings and Loan Cooperatives (SOCAP)	USD 0	USD 47	USD 165	USD 211
Popular Finance Corporations (SOFIPO)	USD 0	USD 18	USD 1	USD 19
Non-Banking Finance Intermediary Sector (Credit Unions)	USD 0	USD 0	USD 793	USD 794
FINTECH Sector	USD 0	USD 0	USD 991	USD 991
MEXICAN FINANCIAL SYSTEM	USD 1,650	USD 2,190	USD 3,310	USD 7,150

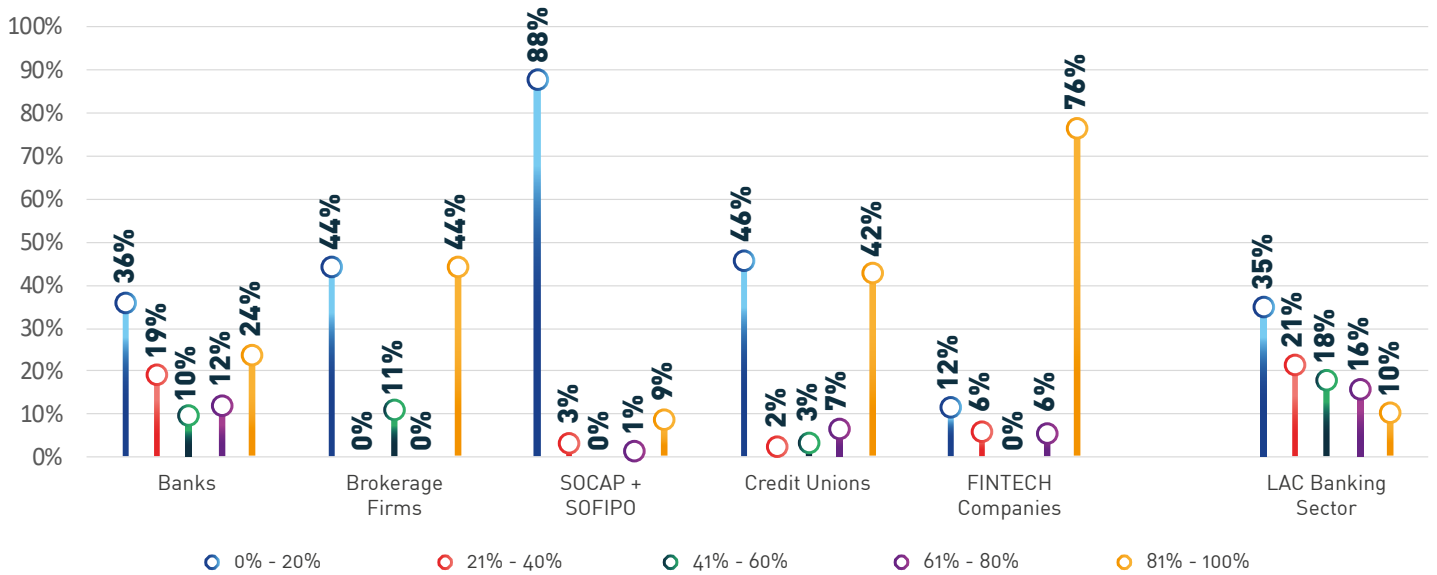
millions

Source: GS/OAS based on information collected from Mexican financial entities and institutions

ANEXO 2

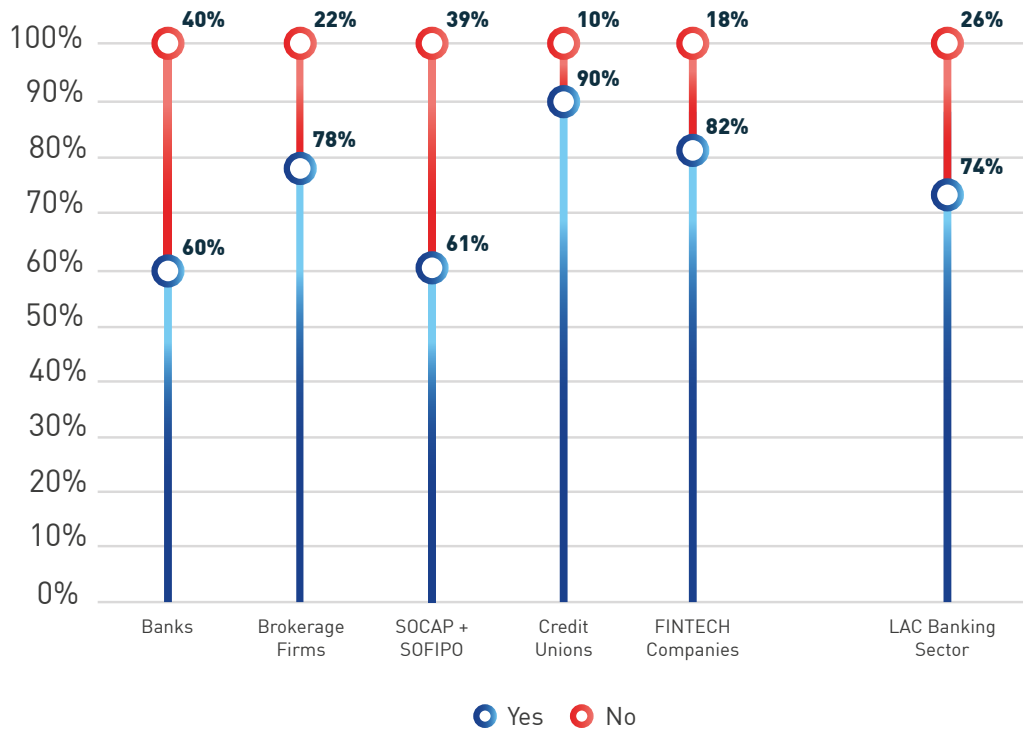
Comparative Analysis Between Sectors of the Mexican Financial System

Figure 34. Percentage of Operations Using Non-Face-To-Face Transactional Channels - Comparison Between Sectors



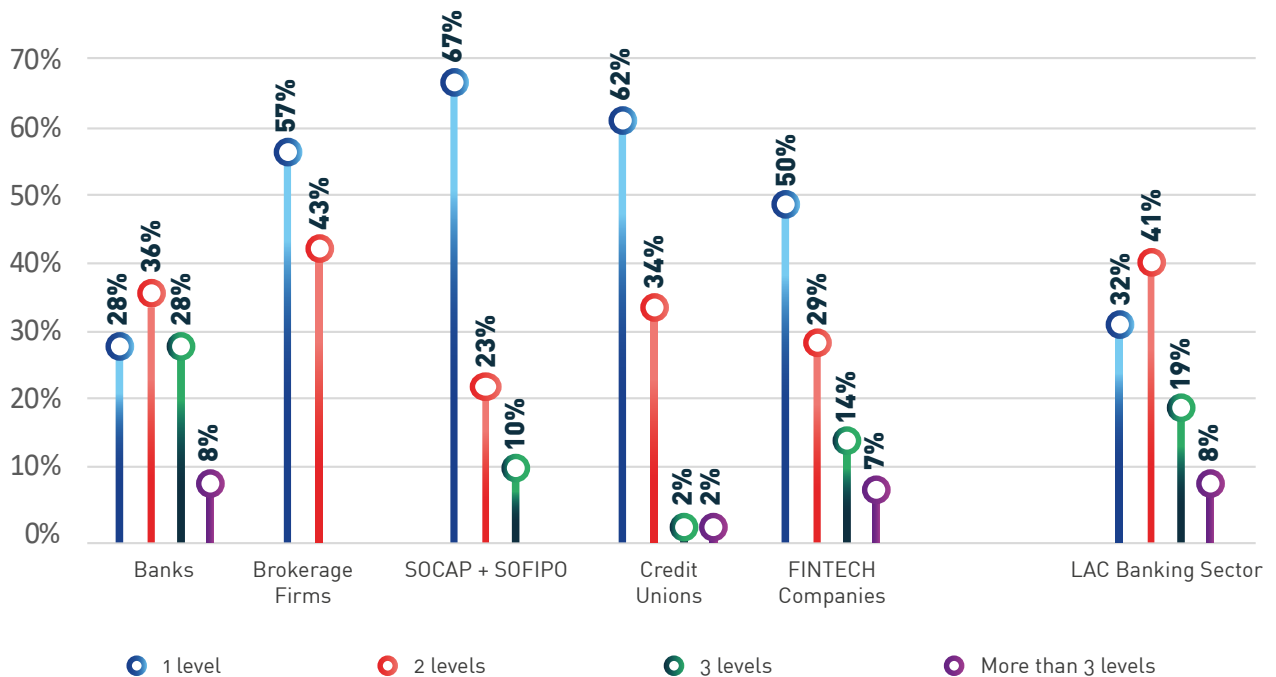
Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 35. Single Area Responsible for Digital Security in the Financial Entity/Institution - Comparison Between Sectors



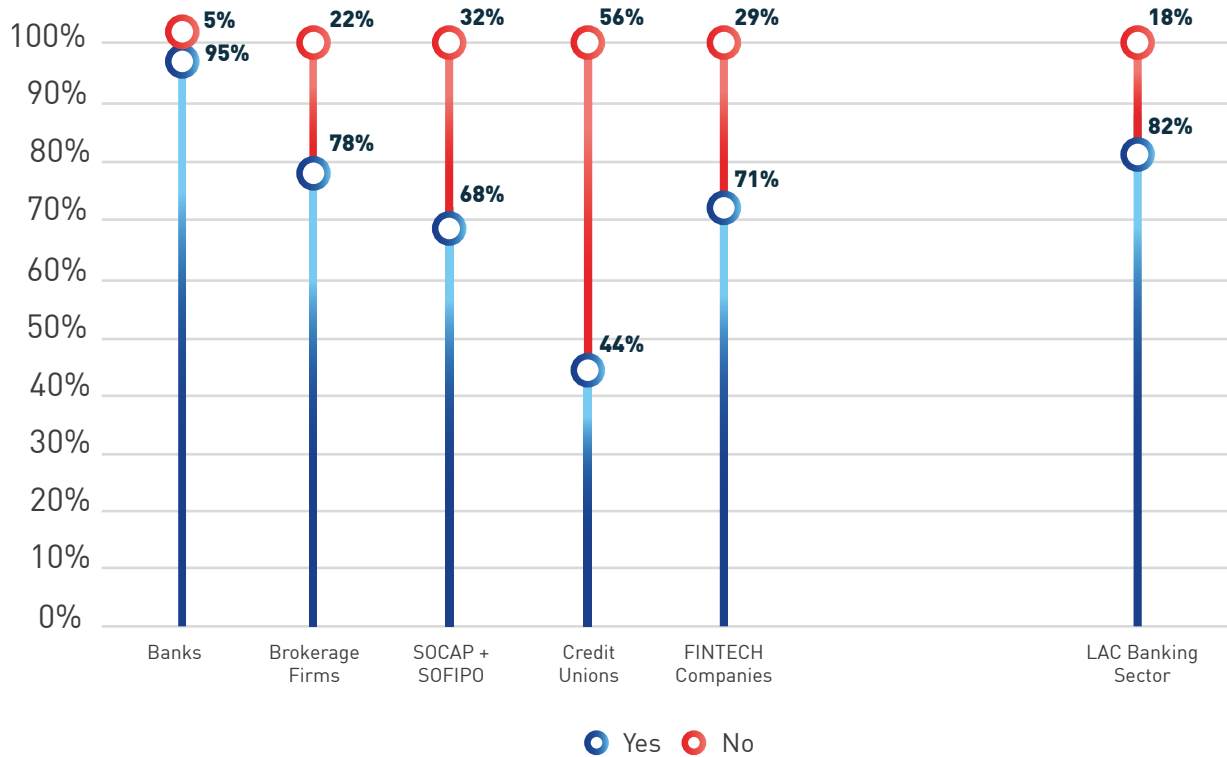
Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 36. Number of Hierarchical Levels Between the CEO and the Head of Digital Security - Comparison Between Sectors



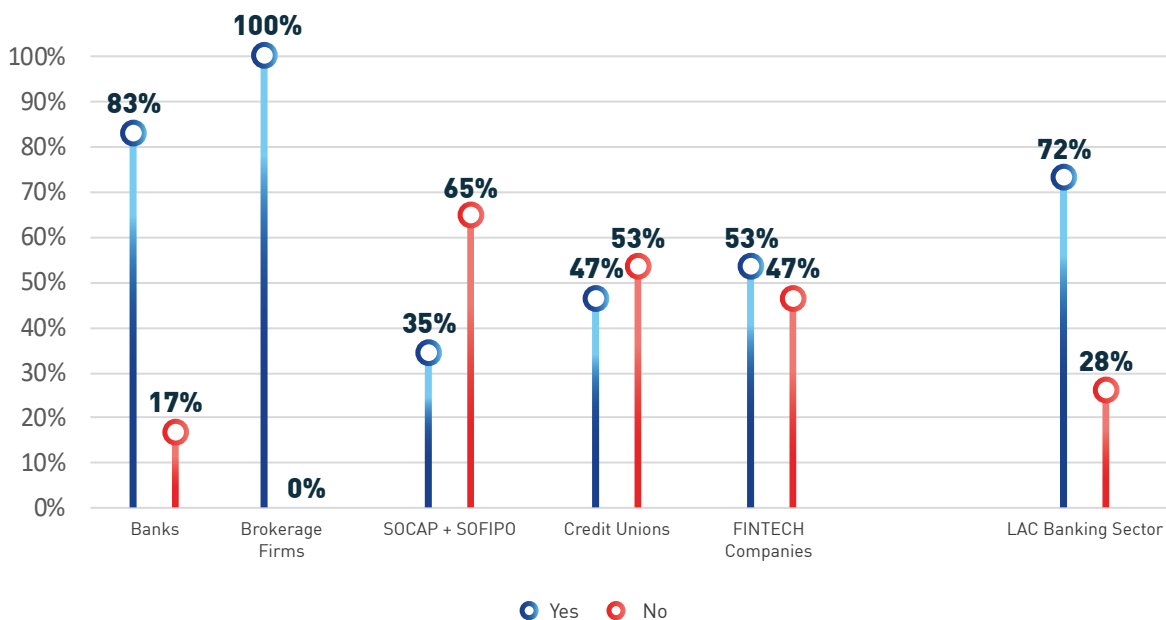
Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 37. Is it Considered Appropriate for This Team to Grow in the Short Term? – Comparison Between Sectors



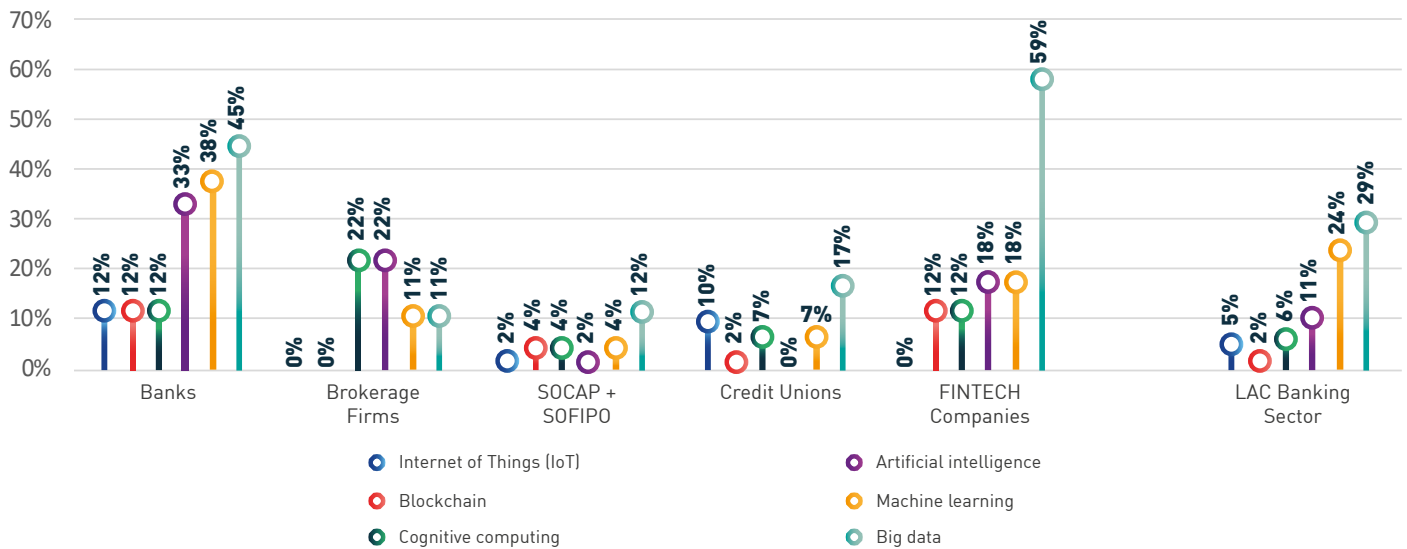
Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 38. Does the Board of Directors, or Similar, Receive Periodic Reports about Information Security Risks? – Comparison Between Sectors



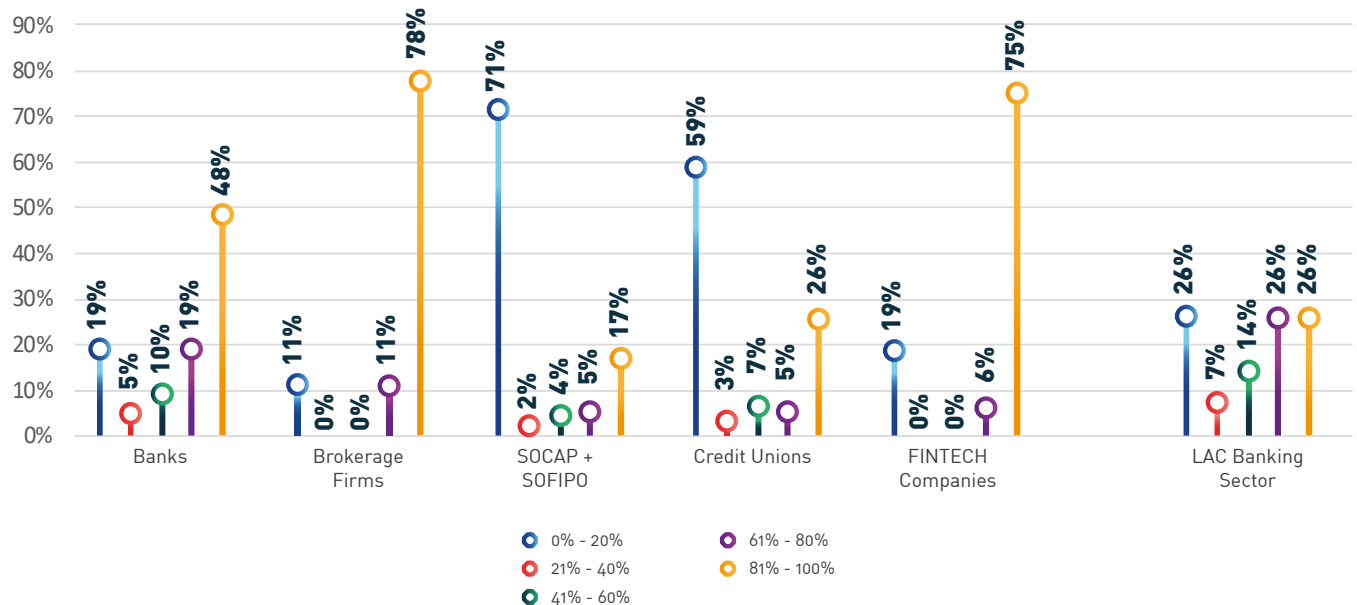
Note: 240 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 39. Emerging Digital Technologies Applied to Digital Security Tools, Controls or Processes in the Financial Entity/Institution – Comparison Between Sectors



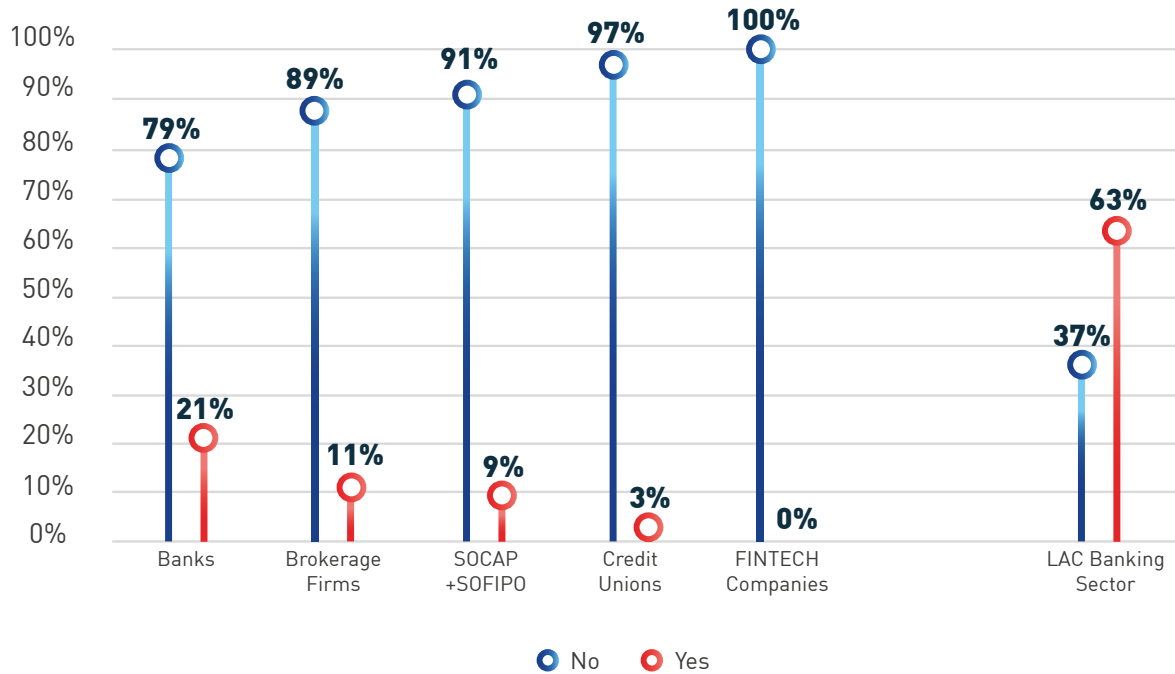
Note: 240 records Source: GS/OAS based on information collected from Mexican financial entities and institutions

Figure 40. Percentage of Digital Security Events that are Detected by the Detection Systems of the Financial Entity/Institution (and not Third-Party Systems) – Comparison Between Sectors



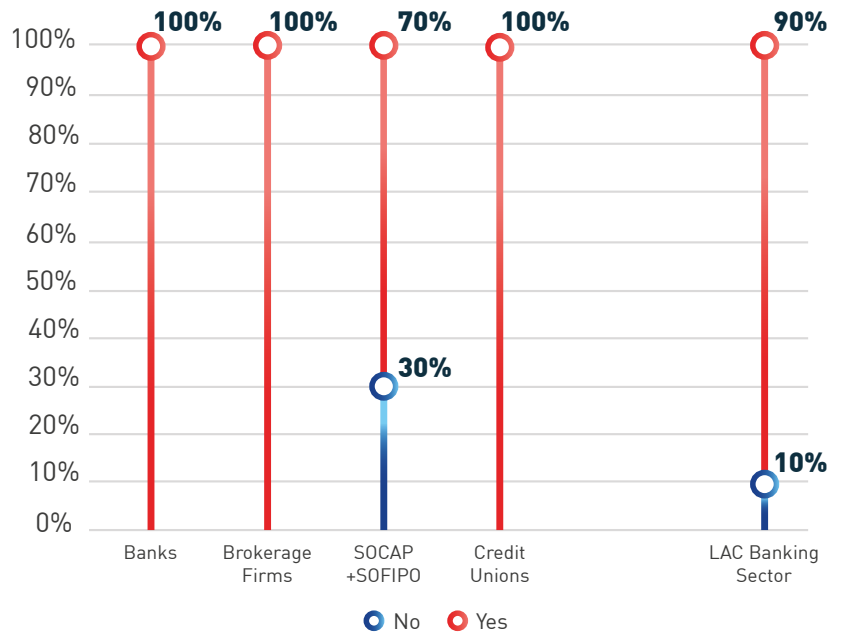
Note: 237 records Source: GS/OAS based on information collected from Mexican financial entities and institutions

Figure 41. Was the financial entity/institution the victim of incidents (successful attacks) in information security (including cybersecurity) during the last twelve months? – Comparison Between Sectors



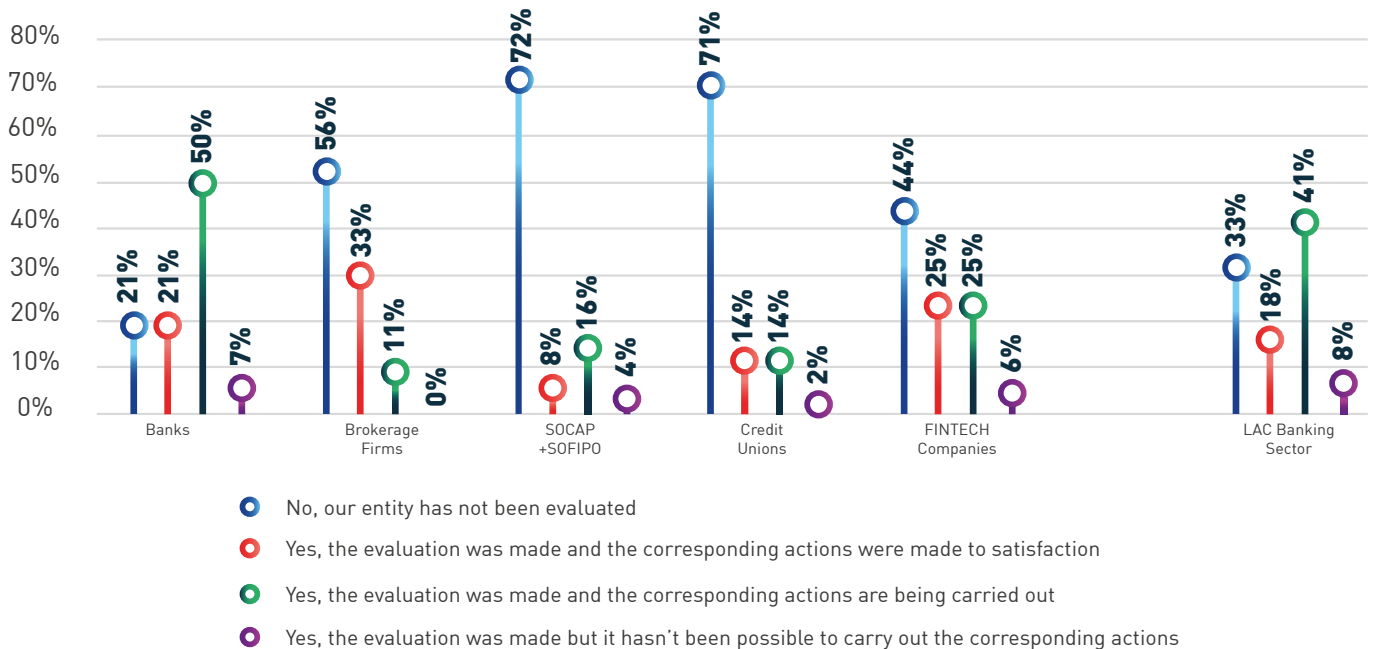
Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 42. Did the Financial Entity/Institution to Which You Belong Investigate the Source That Originated Such Incidents (successful attacks) in information security (including cybersecurity)? – Comparison Between Sectors



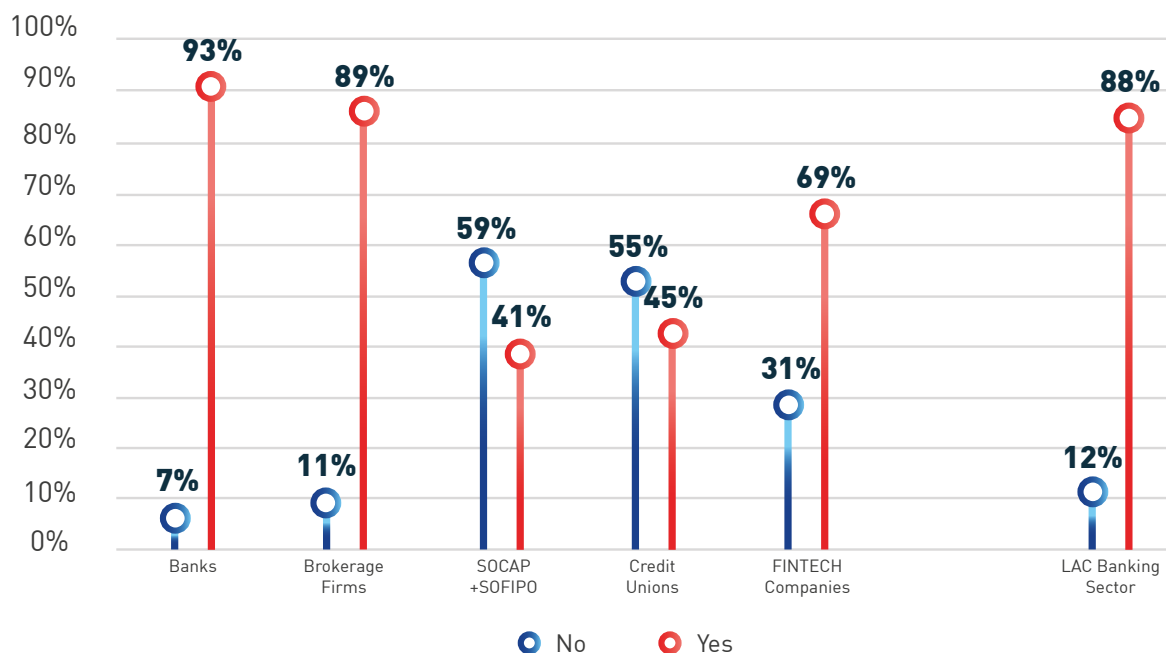
Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 43. Has the Financial Entity/Institution to Which You Belong Been Externally Evaluated in the Last Two (2) Years Under Any Information Security (Including Cybersecurity) Methodology to Determine Level of Maturity? – Comparison Between Sectors



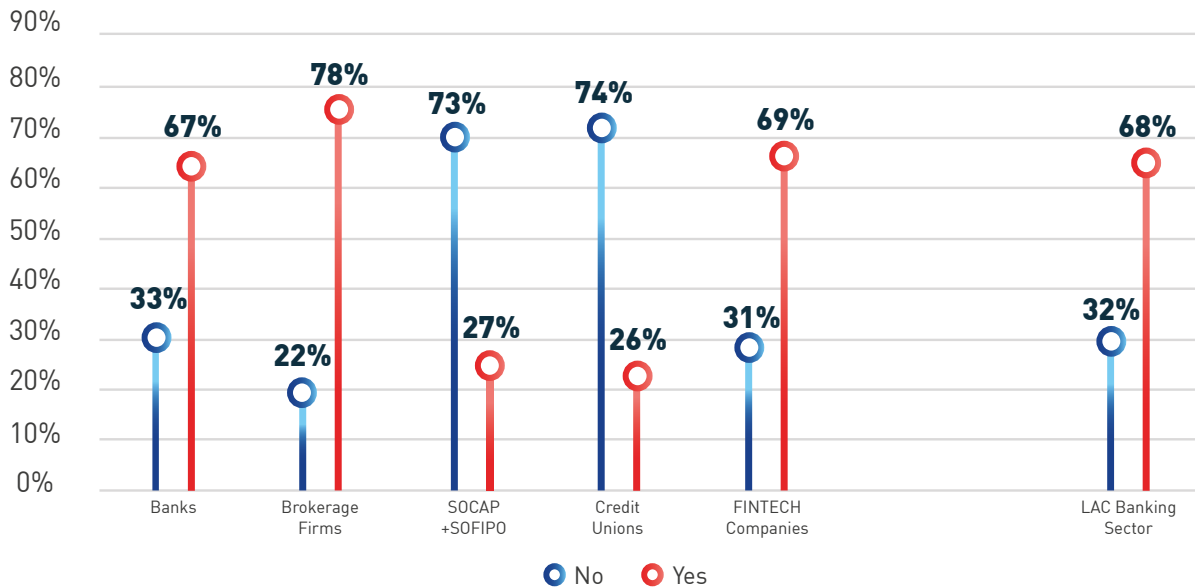
Note: 236 records Source: GS/OAS based on information collected from Mexican financial entities and institutions

Figure 44. Does the Financial Entity/Institution Offer a Mechanism for Its Collaborators (Employees and Contractors) to Report Incidents (Successful Attacks)? – Comparison Between Sectors



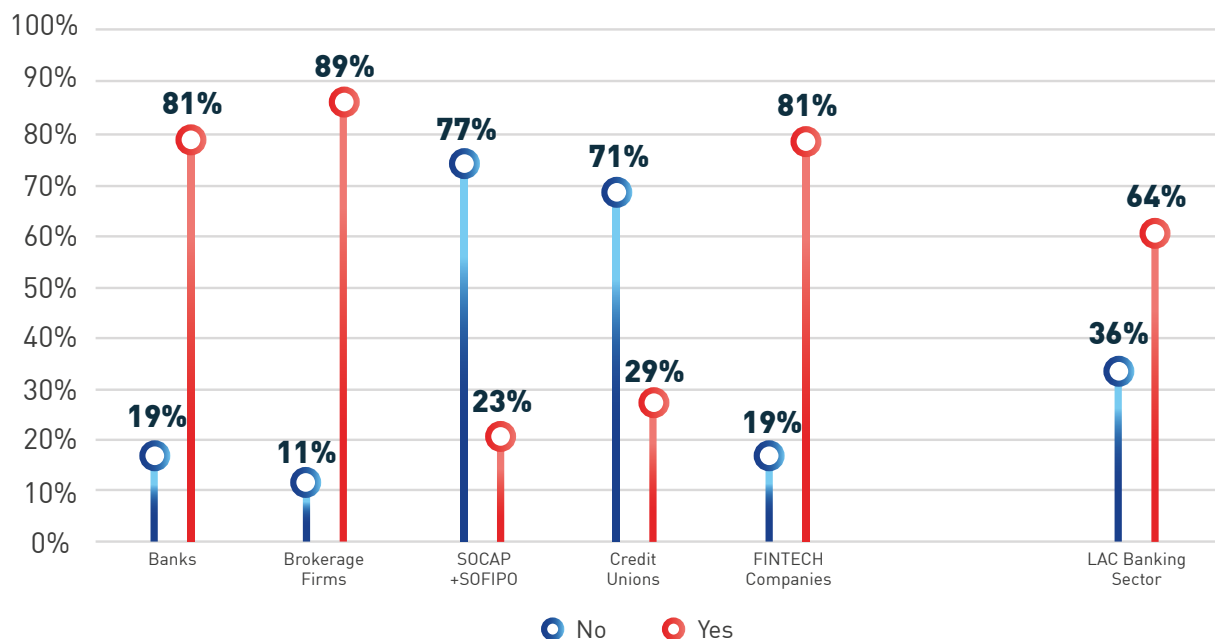
Note: 236 records Source: GS/OAS based on information collected from Mexican financial entities and institutions

Figure 45. Does the financial entity/institution offer a mechanism for its clients (partners, associates or users) to report incidents (successful attacks)? – Comparison Between Sectors



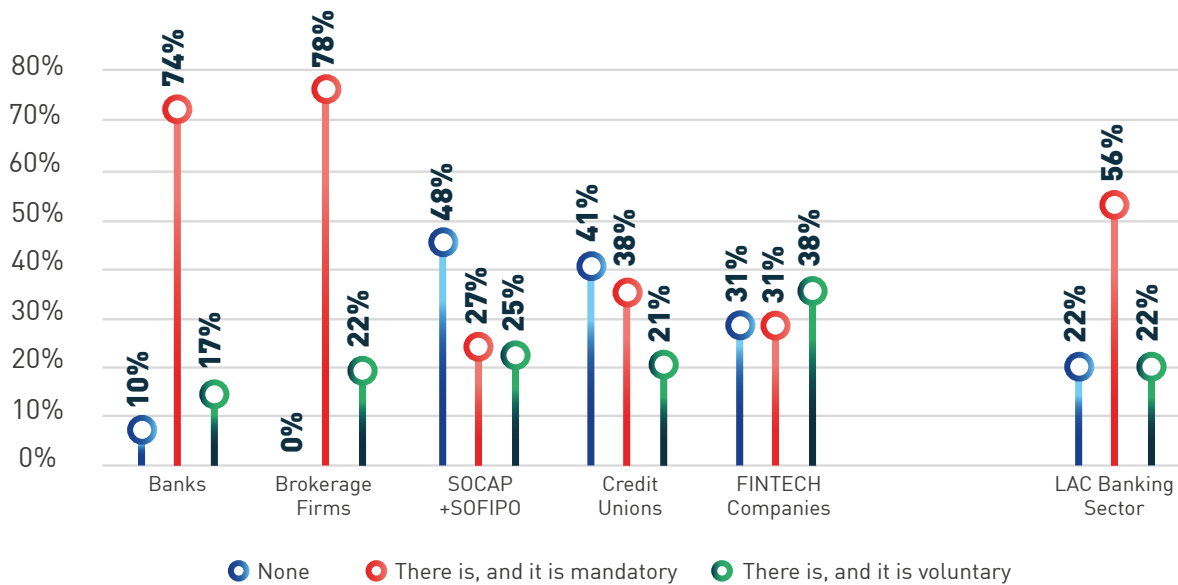
Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 46. Does the Financial Entity/Institution Have a Communications Plan That Allows Informing Clients (Partners, Associates or Users) When Their Personal Information Has Been Compromised? – Comparison Between Sectors



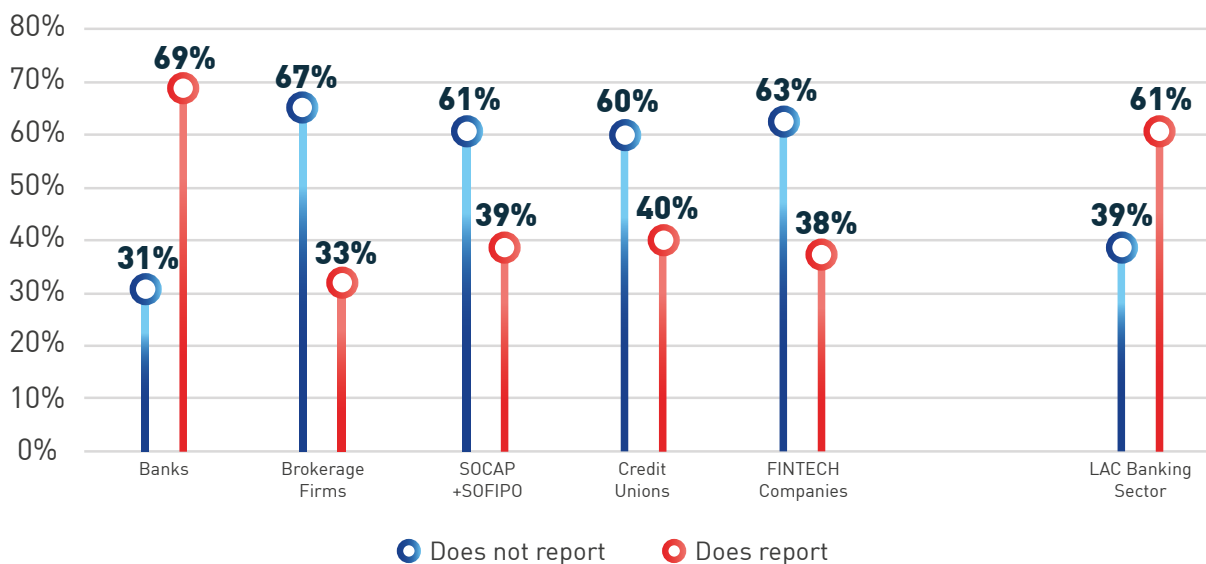
Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 47. Do You Know Any Mechanism to Report Incidents (Successful Attacks) against the Financial Entity/Institution to Which You Belong, to a Regulatory Authority in Mexico? – Comparison Between Sectors



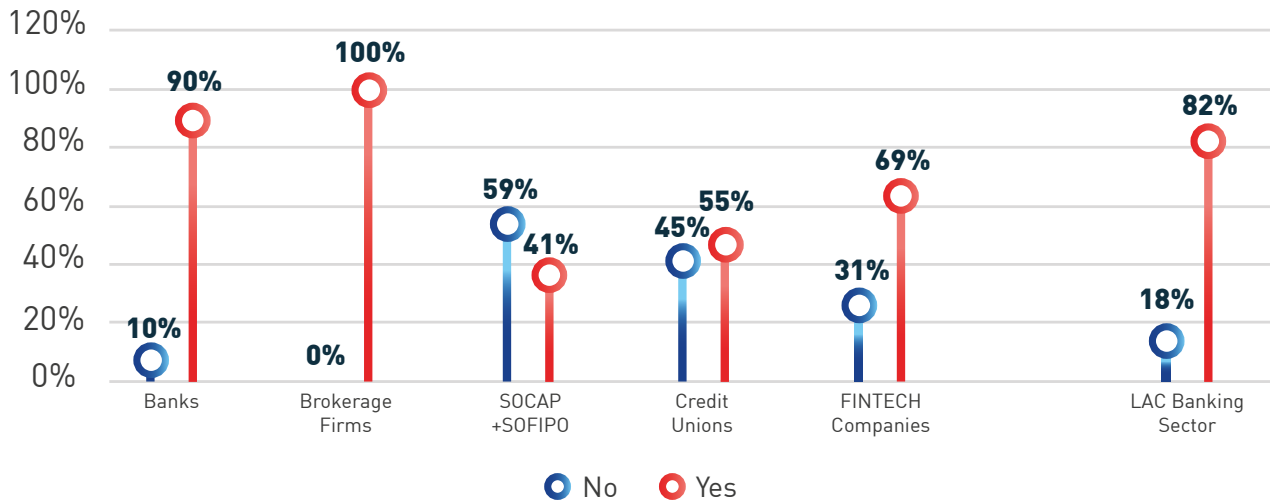
Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 48. Does the Financial Entity/Institution Report the Incidents (Successful Attacks) to a Law Enforcement Authority in Mexico? – Comparison Between Sectors



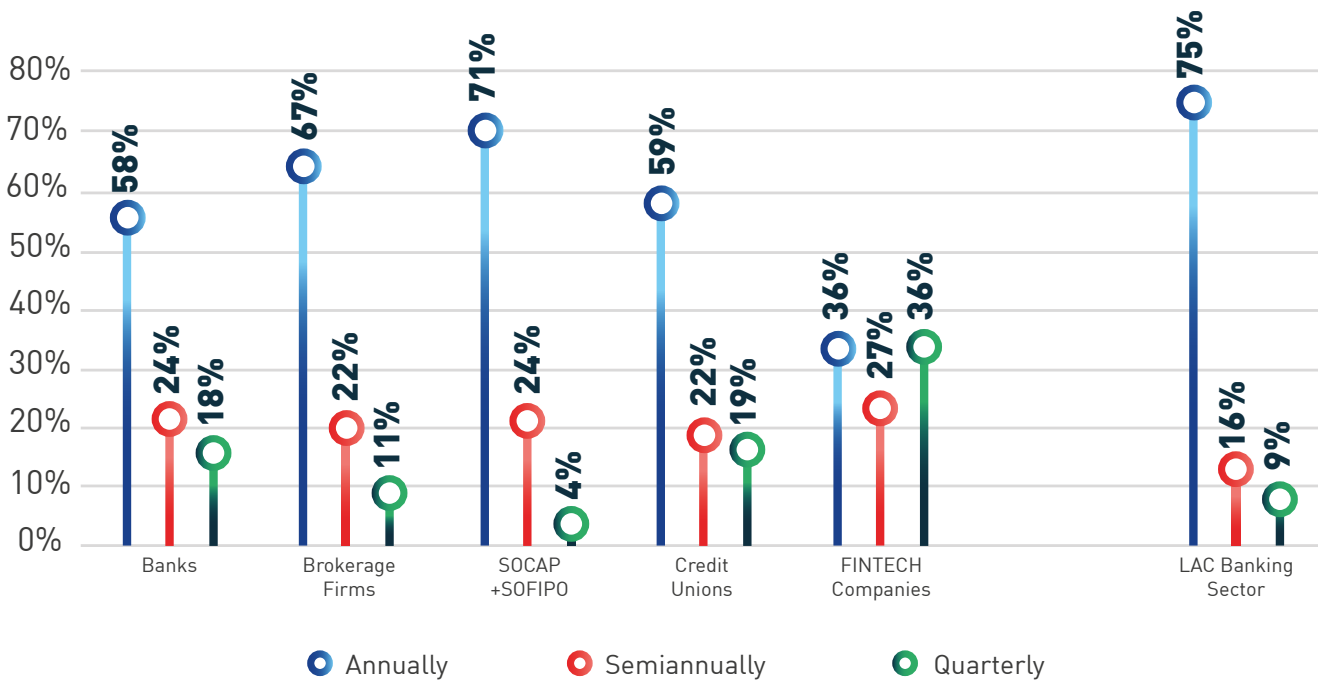
Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 49. Does the Financial Entity/Institution Have Awareness and Training Plans on Matters of Information Security for its Collaborators? – Comparison Between Sectors



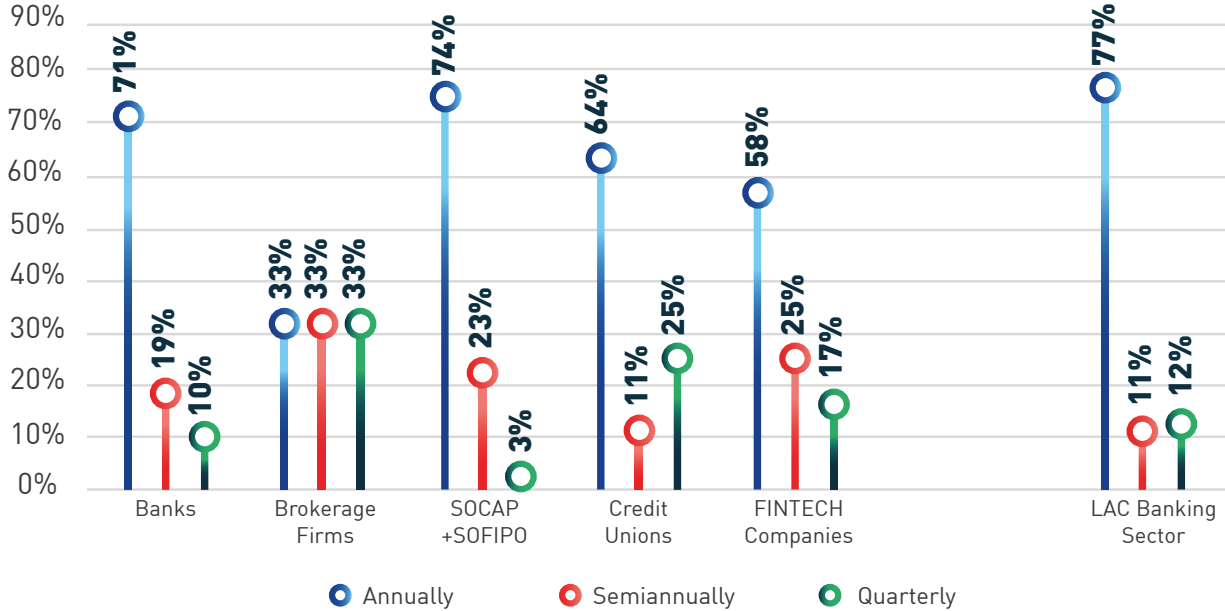
Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 50. How Often are Such Awareness and Training Plans Conducted? – Comparison Between Sectors



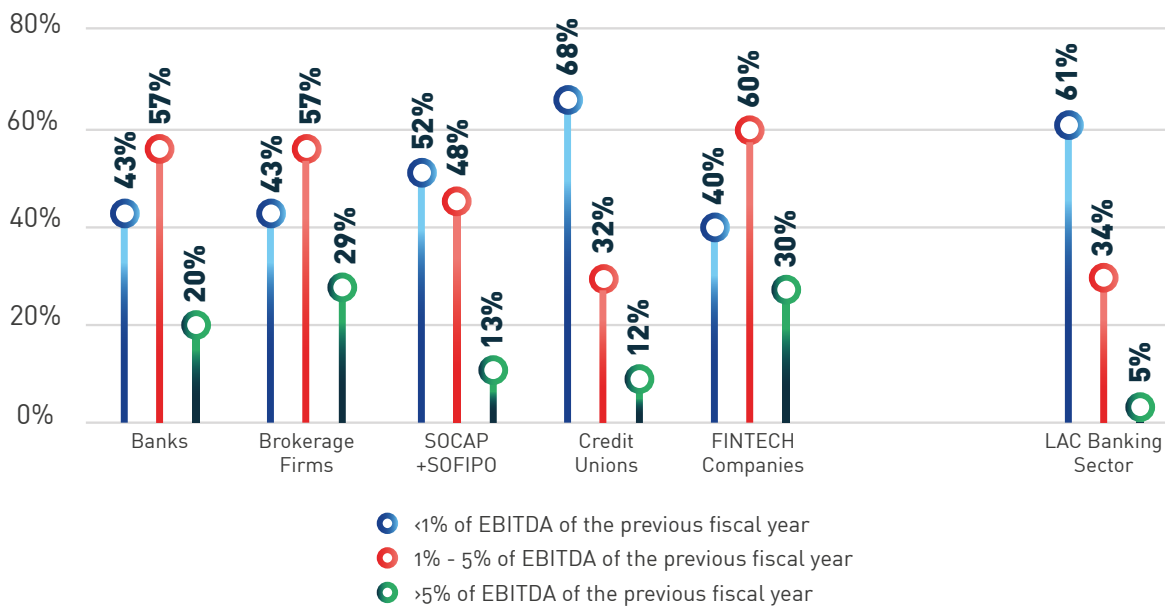
Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 51. How often is the capacity of employees of the financial institution put to the test to adequately respond to incidents (successful attacks) and phishing and social engineering schemes? – Comparison Between Sectors



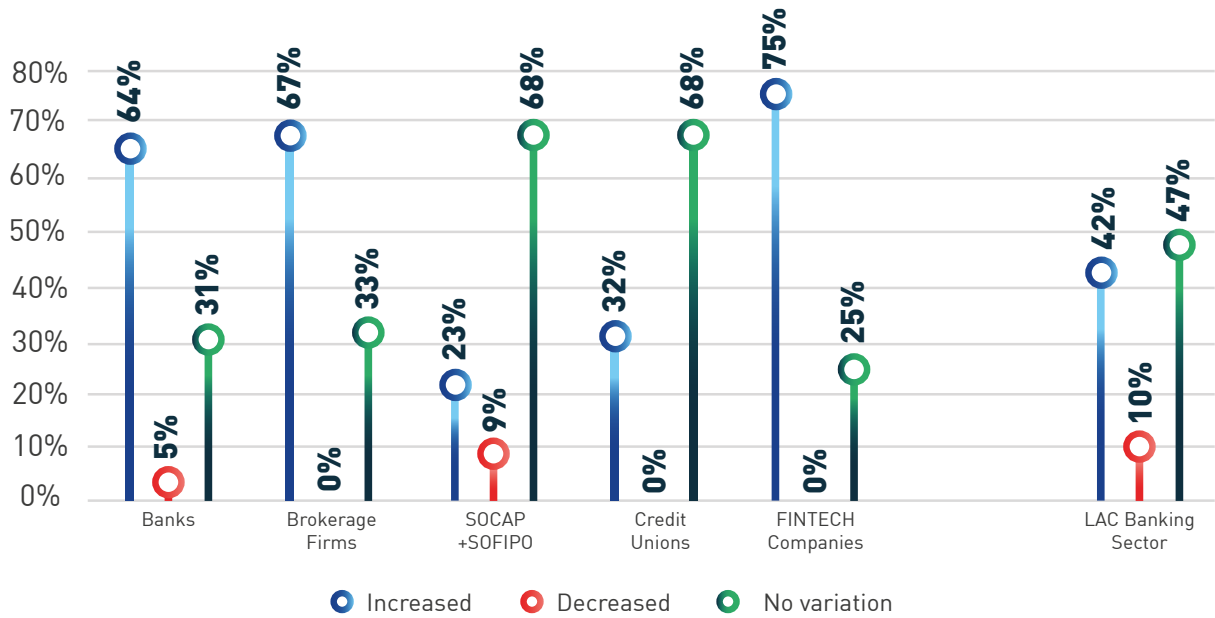
Note: 236 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 52. Dynamic of the Digital Security Budget in the Last Year – Comparison Between Sectors



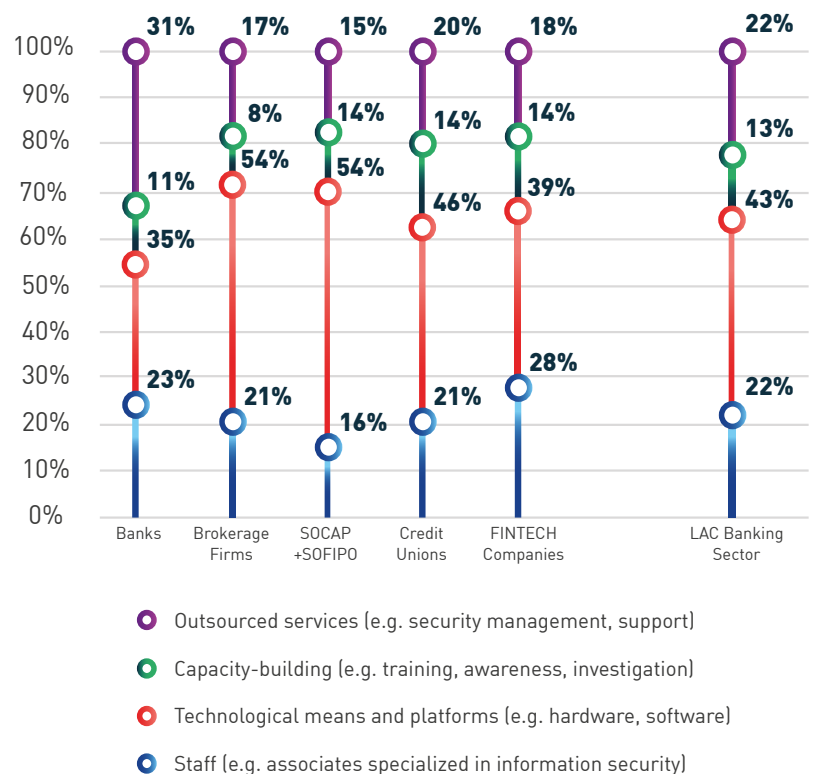
Note: 235 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 53. Growth of the Budget for Information Security (Including Cybersecurity) and Fraud Prevention Using digital means of the Financial Entity/Institution – Comparison Between Sectors



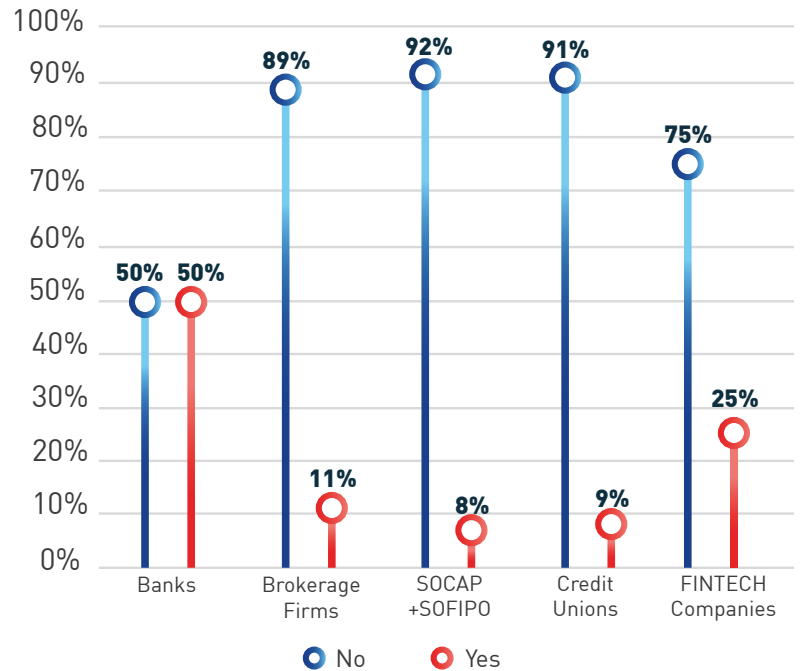
Note: 235 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 54. Distribution of the Budget for Information Security (Including Cybersecurity) and Fraud Prevention Using Digital Means of the Financial Entity/Institution – Comparison Between Sectors



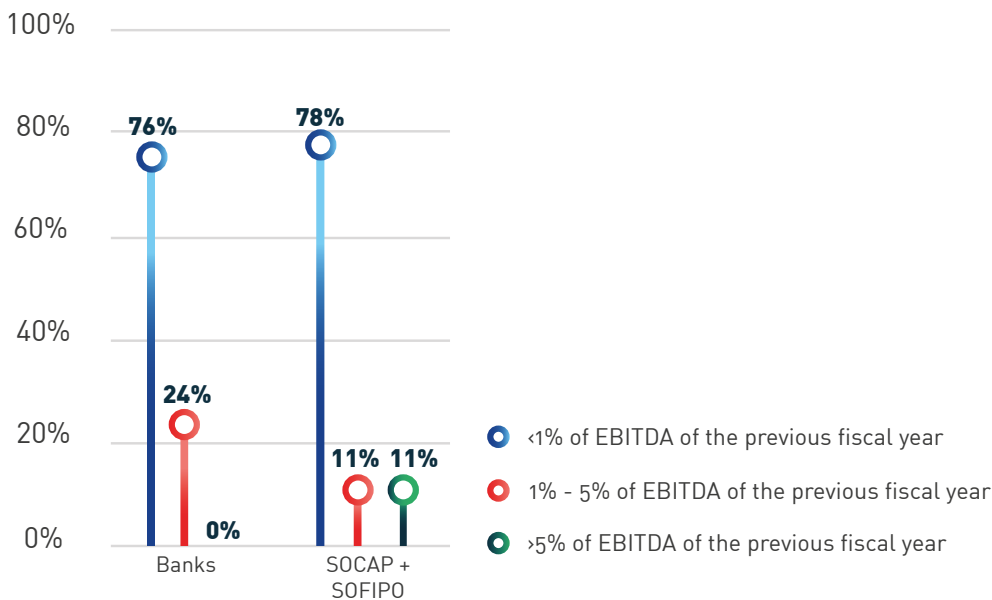
Note: 196 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 55. Did the Financial Entity/Institution to Which You Belong Estimate the Total Cost of Response and Recovery from Incidents (Successful Attacks) in Information Security (Including Cybersecurity) for the Last Fiscal Year? – Comparison Between Sectors



Note: 233 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

Figure 56. Cost of Response and Recovery from Incidents (Successful Attacks) in Information Security (Including Cybersecurity), for the Entity/ Institution to Which You Belong, of the Immediately Preceding Year – Comparison Between Sectors



Note: 40 records **Source:** GS/OAS based on information collected from Mexican financial entities and institutions

THE STATE OF
CYBERSECURITY
IN THE **MEXICAN**
FINANCIAL
SYSTEM



THE STATE OF
CYBERSECURITY
IN THE **MEXICAN**
FINANCIAL
SYSTEM

With the financial
support of



Foreign &
Commonwealth
Office