Datasec

GRUPO RADAR
INTELIGENCIA DE MERCADO

SURVEY

State of Cybersecurity in Uruguayan companies

2020 - 2021

INTRODUCTION

The year 2020 will undoubtedly be remembered as a year of significant challenges for the operational continuity of organizations. In this context, unfortunately cybersecurity has not been an exception, but an aggravating factor in an already complex scenario.

The vertiginous rise in the level of cybersecurity risk is a clear consequence of the rapid digitalization and growth of remote work during the pandemic, which increased exposure by creating more complex and potentially less secure networks.

According to the 'Force Threat Intelligence Index 2021' report, worldwide, ransomware was the most important type of threat, accounting for 23% of all attacks. Vulnerability scanning and exploitation of these was the most important attack vector, overcoming phishing, the main one in 2019.

It is clear that the bewilderment and teleworking have left a very fertile ground for cybercriminals to develop their skills and take advantage of the situation to increase their phishing attacks, double extortion ransomware and vulnerability exploitation. These scenarios have multiplied significantly, leaving organizations in all sectors highly vulnerable and in many cases with serious operational and financial problems.

In this context, and as part of our commitment to raising awareness of information security, we have carried out a new survey to assess how organizations in Uruguay have prepared to face this growing threat, and whether they have been affected by any security incident in the last year.

The vast majority of organizations do not have the necessary controls in place and end up being victims of cyberattacks, which in many cases they are not even able to identify and protect themselves in time.

Information security and cybersecurity is a growing operational risk around the world, so much so that the World Economic Forum report published in 2021 ranks it 4th in the world, well above terrorism and climate change.

CYBERSECURITY

Different reports, carried out worldwide, highlight cybersecurity risks as one of the main operational risks faced by companies globally. This scenario does not elude the Uruguayan reality in which every year more and more companies suffer events and incidents with significant impact on their operations and their customers.

Uruguayan legislation was recently updated incorporating new obligations for the protection of Uruguayans' personal data by companies. Among these obligations, the most important is that the company must take proactive actions to avoid being a victim of an incident. Likewise, companies must report incidents affecting Uruguayans' personal data to AGESIC's incident response center.

In this context, this report seeks to provide information on the business scenario and, at the same time, stimulate companies to implement the minimum necessary practices to ensure their cybersecurity as well as that of their customers, highlighting the privacy and protection of their personal data.

The questions asked throughout this survey seek to determine whether companies were victims of the main cybersecurity incidents that are currently known globally, and at the same time to identify the degree of maturity that these companies present with respect to the most minimal controls necessary to deal with existing risks.

How secure are we in terms of cybersecurity is a question that many companies are not able to answer adequately. In many cases it is subjective based on the perception of their directors or owners: "nothing ever happened to us", "if we had several incidents this year, it is not a clear indicator of reality that the company is facing".

The total or partial absence of indicators, roles and specific responsibilities in this area means that many companies have a clear lack of knowledge about their reality.

TECHNICAL SHEET

A telephone survey was applied to a sample of 600 companies, representative of the universe of all Uruguayan companies.

Quotas were defined according to three criteria:

- **Geographical area:** Montevideo and Interior.
- **Company size:** micro/small and medium/large.
- **Activity Sector:** Industry, Commerce and Services.

The primary sector was excluded from the study because it was too small.

Segments with smaller universes such as industry, and medium and large companies were oversampled.

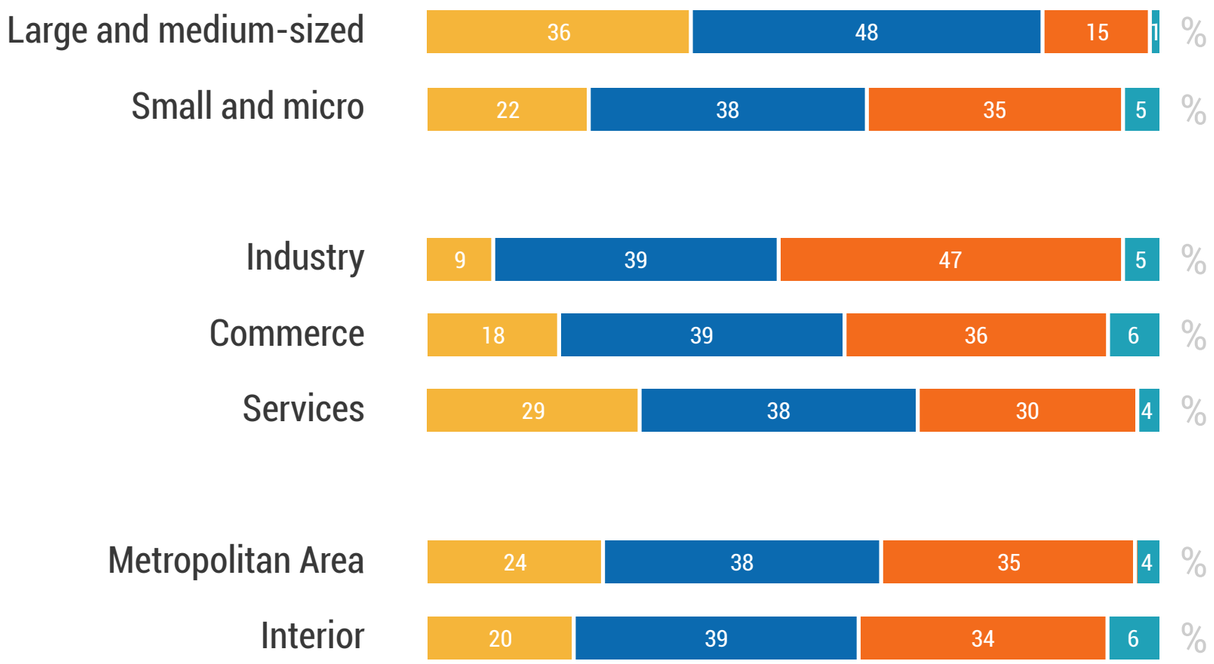
For the purpose of processing the general results, each segment was given its real weight in the universe of companies.

The maximum margin of error for the overall sample is ±4.0, for a 95% confidence level.

	UNIVERSE	SAMPLING
TOTAL	**172133**	**619**
Large and medium-sized	6100	236
Small and micro	166034	383
Industry	25280	107
Commerce	60198	257
Services	86656	255
Metropolitan Area	96963	312
Interior	75170	307

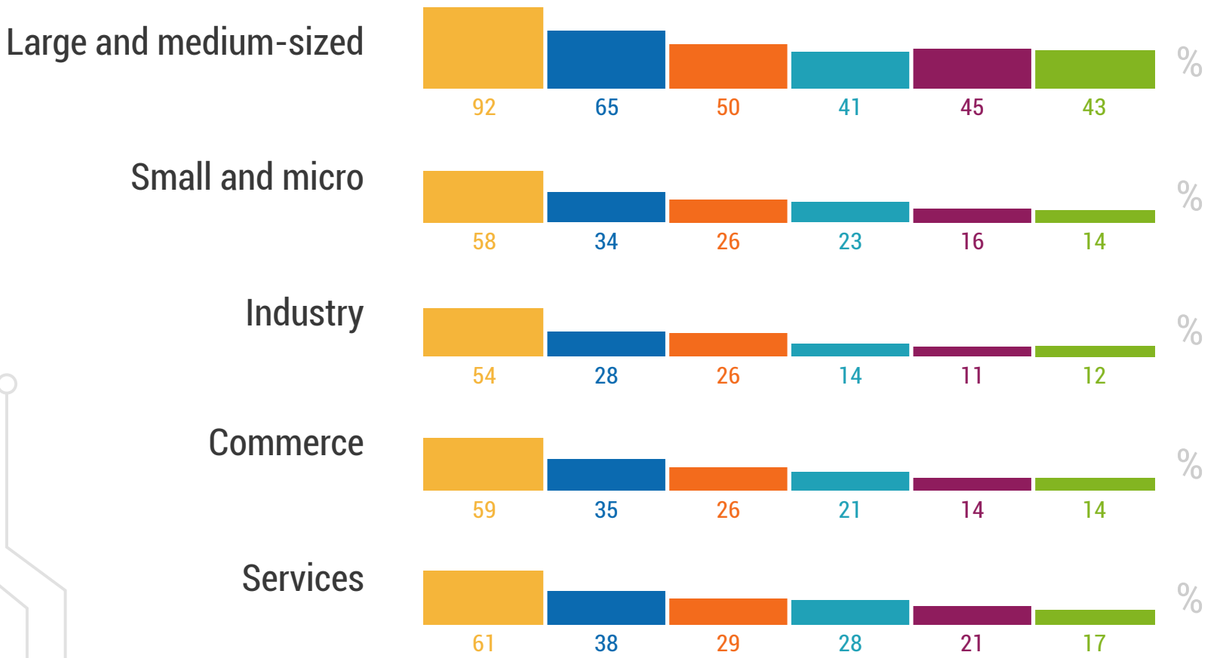
Do you consider that your company is prepared for cybersecurity incidents?

Viruses, hacks, theft or hijacking of information.



	2019
22% Yes, completely	22%
38% Yes, partially	27%
35% No	39%
5% Don't know	12%

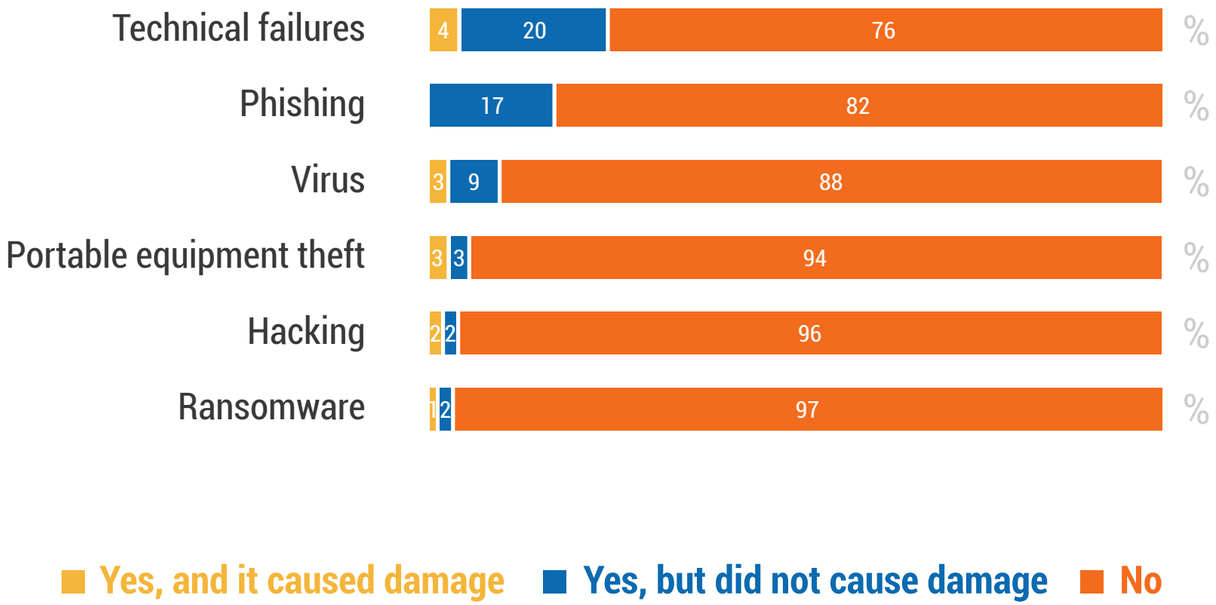
What cybersecurity controls have been implemented?

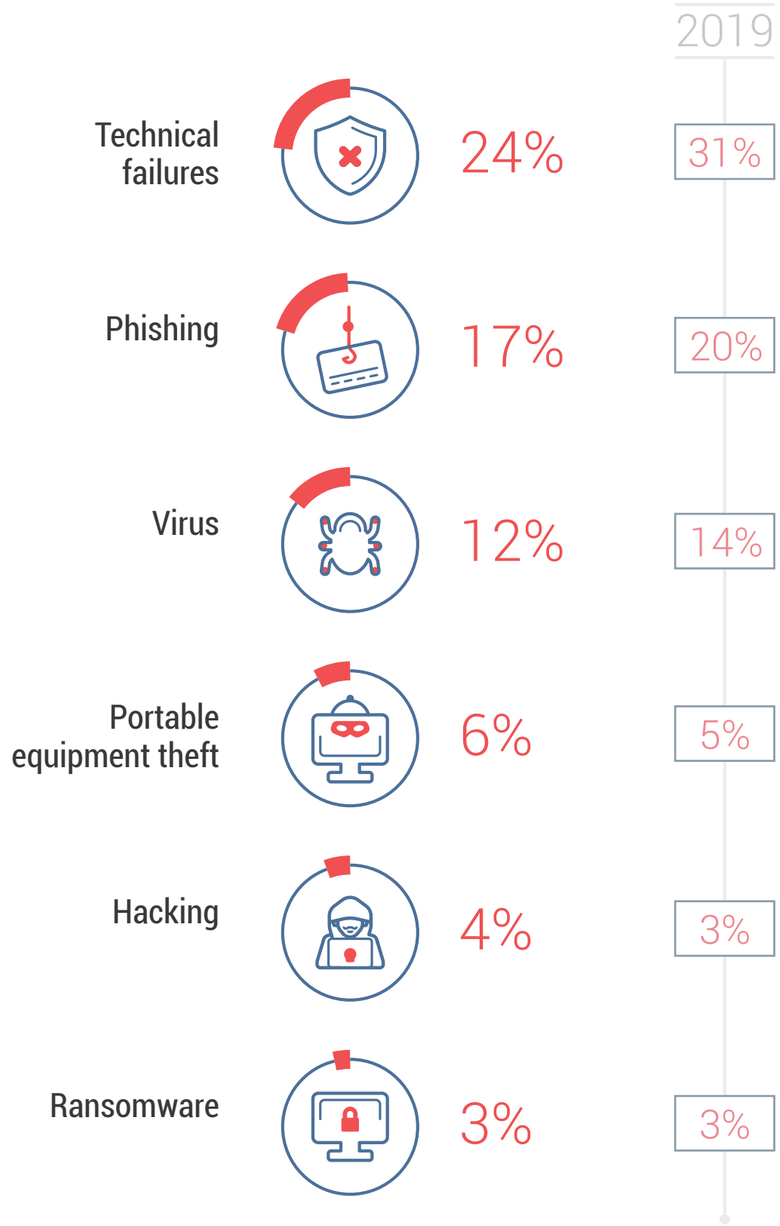


	2019
Count with Antivirus	59%
Back up information on an external site	35%
Raise awareness among employees	27%
They encrypt their portables equipments	23%
They designated a person in charge of cybersecurity	17%
Have cybersecurity policies	15%

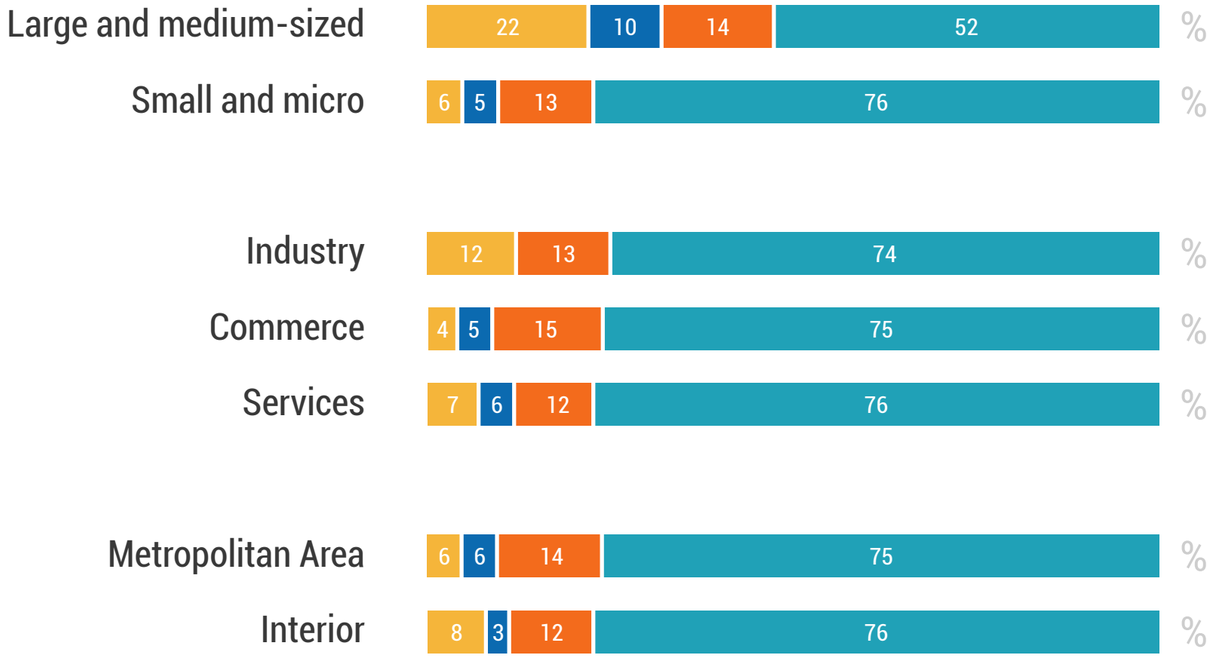
	2019
Count with Antivirus	77%
Back up information on an external site	57%
Raise awareness among employees	42%
They encrypt their portables equipments	20%
They designated a person in charge of cybersecurity	29%
Have cybersecurity policies	22%

What cybersecurity incidents have you had in the last year?





Have you undergone any type of assessment of the state of your cybersecurity?



2019

7%
Yes, regularly
5%

5%
Yes, exceptionally
3%

13%
No, but they would be interested
14%

75%
No, and they do not think it is necessary
77%

Have you undergone an ethical hacking or vulnerability scan to assess your cybersecurity?

11%
Yes, on a regular basis

16%
Yes, exceptionally

49%
No, and they do not think it is necessary

24%
No, but they would be interested

2019

6%

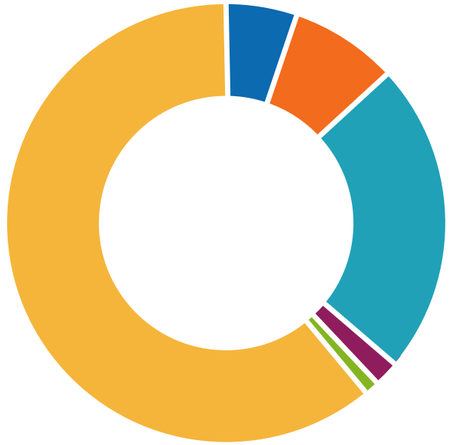
4%

18%

72%

Less than 1/3 of companies that have undergone a security assessment, underwent ethical hacking.

Who is responsible for Cybersecurity?



Large and medium-sized	24	6	26	33	9	1	%
Small and micro	64	4	6	23	3	1	%
Industry	62	1	4	31		1	%
Commerce	58	3	10	16	10	3	%
Services	61	5	7	26			%
Metropolitan Area	62	2	9	25		2	%
Interior	58	8	5	21	6	2	%

60%
Owner or partner

4%
General Manager

7%
IT Manager

24%
Chief Information Security Officer

3%
Contracted company

1%
Other knowledgeable position

2019

42%

7%

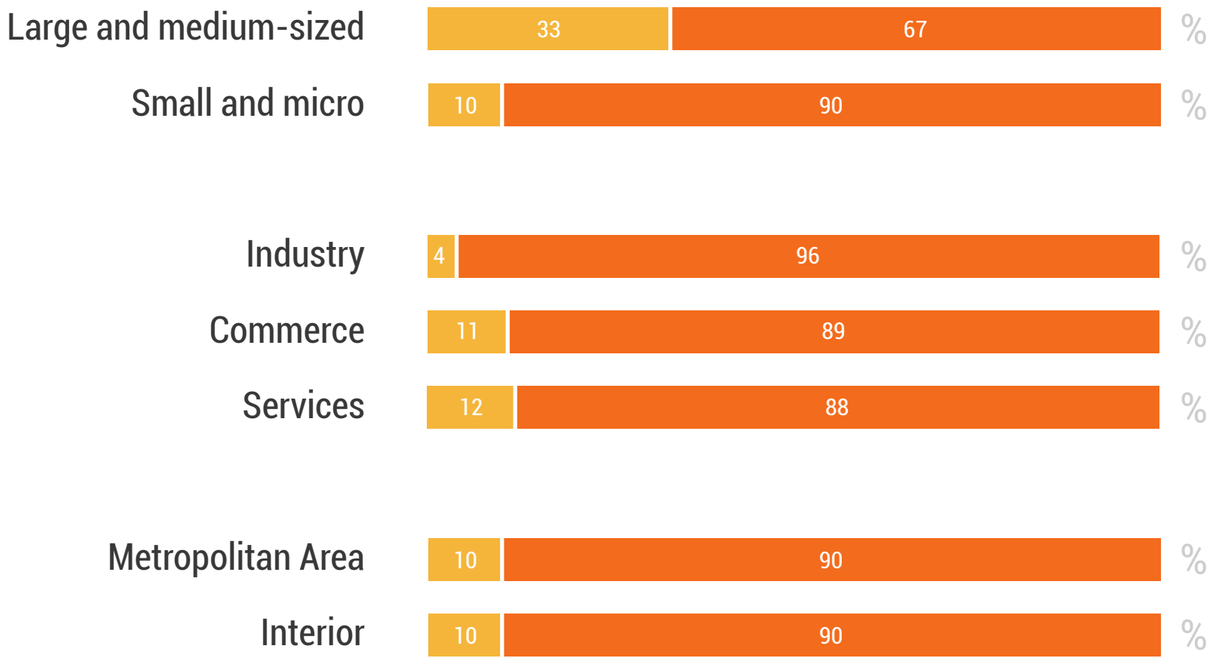
5%

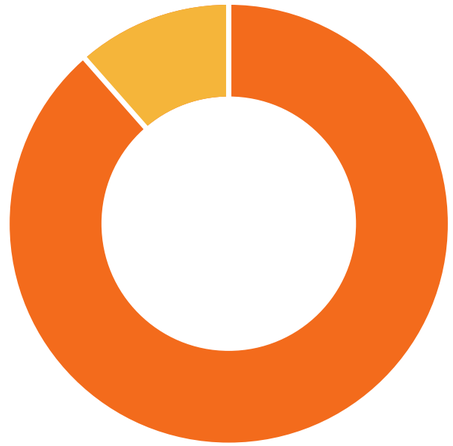
4%

27%

16%

Has anyone been designated to fulfill the role of Data Protection Officer?



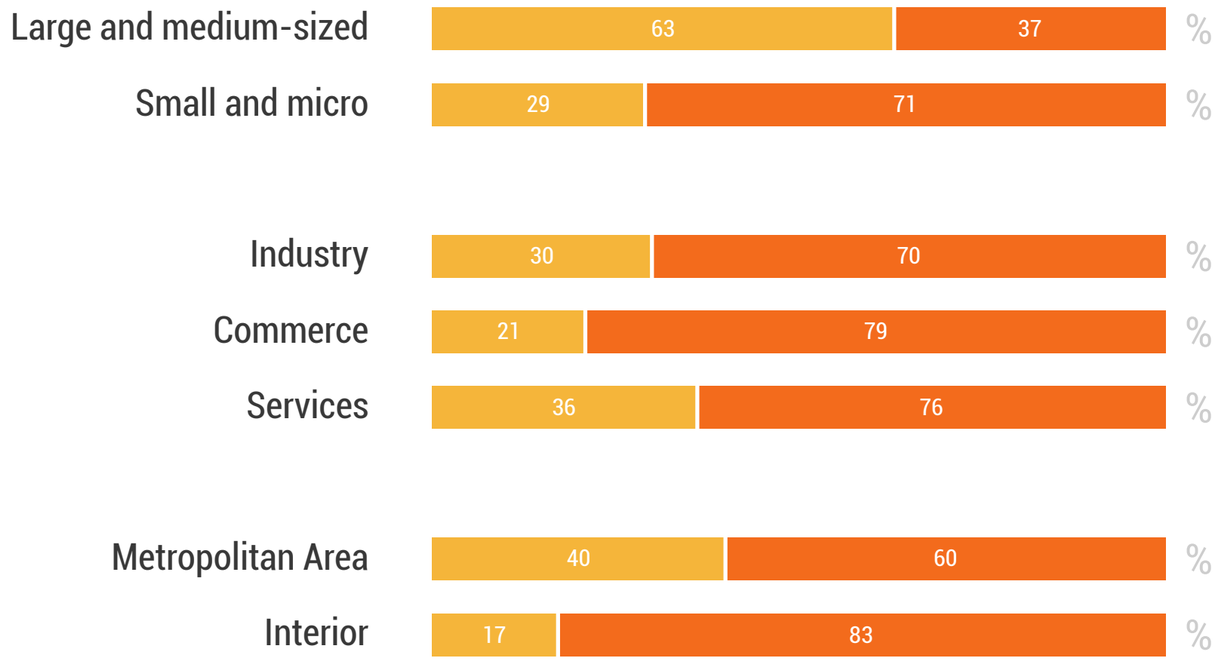


10%
Yes

90%
No

Due to the health emergency

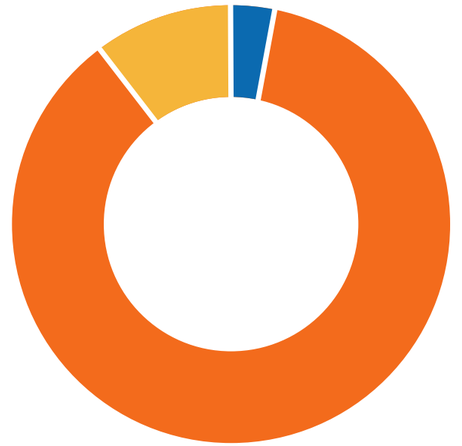
Were there any company personnel who started working remotely?

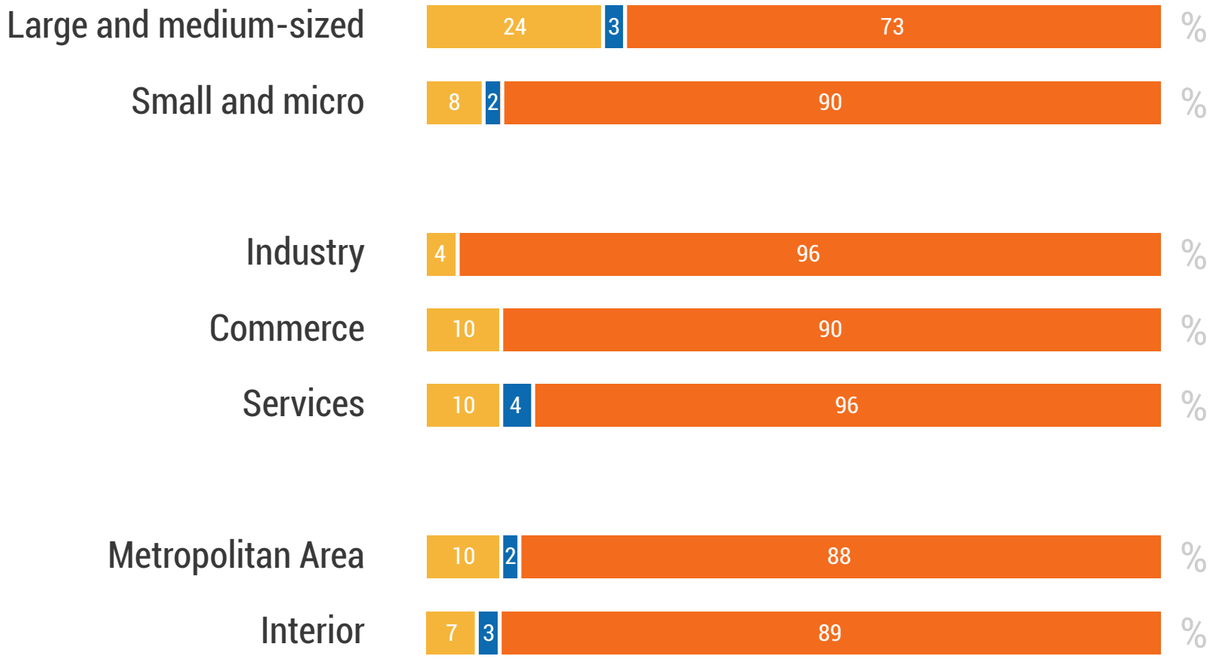


30%
Yes

70%
No

Did Cybersecurity measures change at all for having staff working remotely?





9%
They increased

2%
They became more flexible

89%
They did not change

CONCLUSIONS

We understand that, although awareness of significant cybersecurity threats has increased, there is currently a false perception that the situation is under control.

The truth is that there is no evidence that the low level of reported incidents is due to the implementation of controls and not to a total lack of knowledge of the scenario that is being faced.

Analyzing the numbers we observe that, although 60% of the surveyed organizations indicate that they are prepared for a security incident, when we analyze the implementation of basic controls, 75% of the total do not have them in place.

On the other hand, while specific technical controls such as anti-virus or backups have been deepened, the vast majority of organizations ignore the governance of information security. This is a critical issue when it comes to improving cybersecurity.

Security policies and an adequate risk assessment are the framework for an efficient implementation of controls. In this same context, one of the most important and least costly controls has been neglected by most organizations (75%), which do not carry out any type of personnel awareness-raising actions.
People are the weakest link in this whole chain and the main vector exploited by attackers when an organization is breached.

Information security and cybersecurity is not just a technical issue. It is a matter of governance, commitment and compliance that reaches every type of organization and all its members, penetrating in all spheres and reaching from small actions such as the definition of a policy or a talk, to technical self-assessments as a scan or ethical hacking.

Incidents happen and are already knocking on our neighbors' doors. It is up to each organization to stop pushing fate and start taking effective actions.

Datasec is an Uruguayan company with 30 years of history, a pioneer in risk management and organizational resilience in the region. The objective of this report is to generate local information that will help us to know our reality and at the same time raise awareness about the scenario faced by organizations in terms of Cybersecurity.

We are at your disposal for any query or meeting request in order to evaluate your objectives, risks and requirements in our area of expertise.

Datasec

www.datasec-soft.com