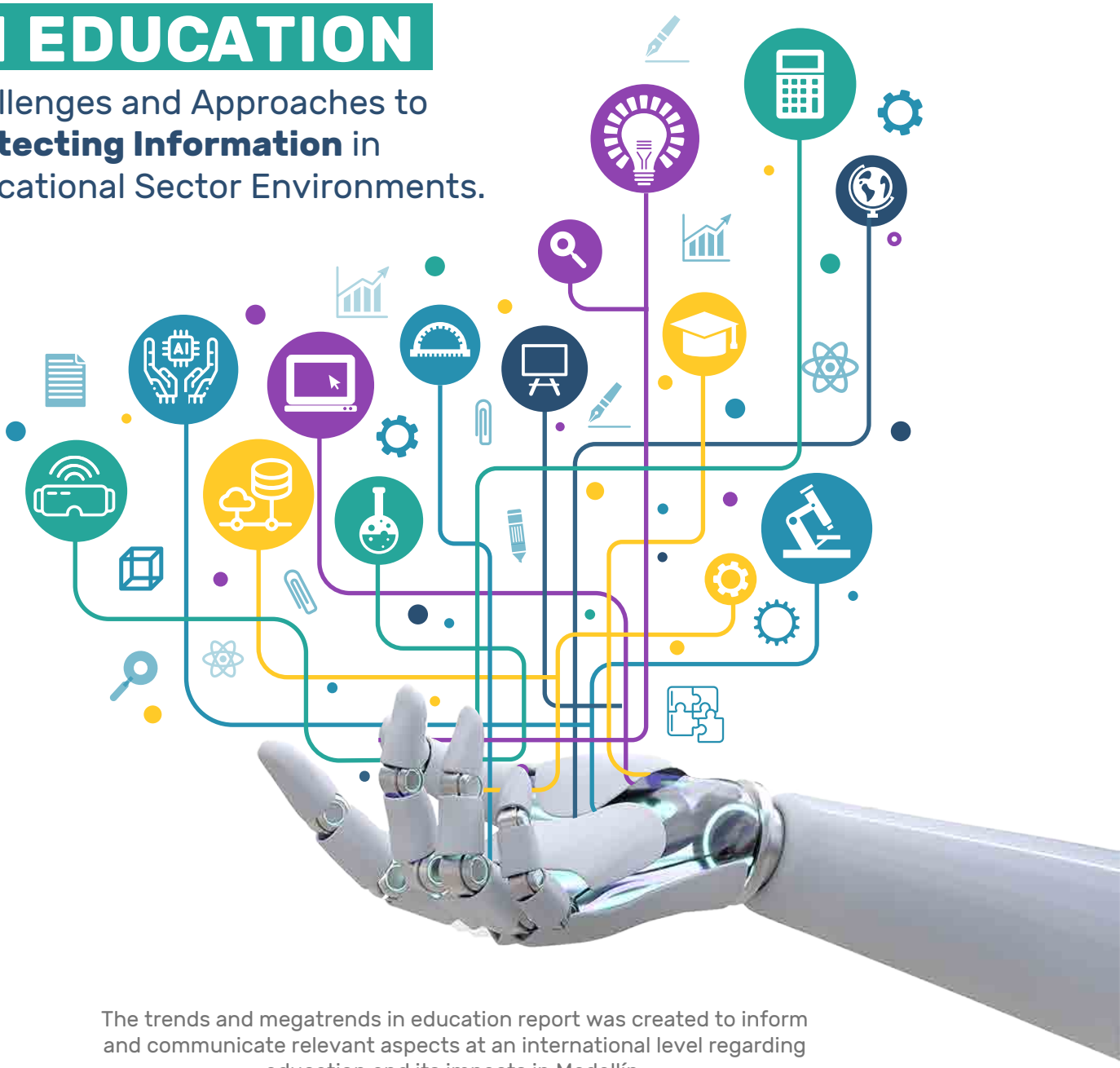
OBSERVATORIO de Sapiencia

Report N° 2 - 2023

TRENDS AND MEGATRENDS IN EDUCATION

Challenges and Approaches to **Protecting Information** in Educational Sector Environments.



The trends and megatrends in education report was created to inform and communicate relevant aspects at an international level regarding education and its impacts in Medellín.

SAPIENCIA
Agencia de Educación Postsecundaria de Medellín

Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

Challenges and Approaches to **Protecting Information** in Educational Sector Environments.

The post-pandemic reality has brought about an exponential increase in the use of technological tools and infrastructure for everyday activities. However, as interaction and dependency increases so do **cyber risks and attacks**. According to the World Economic Forum's Global Risks Report 2022, post-pandemic cybercrime has increased post-pandemic cybercrime increased significantly by 600% worldwide and 133% in Colombia. These numbers are occurring in a context of conflicts in Europe, a generalized increase in prices or uncontrolled inflation, and a inflation, and a growing interest in volatile cryptocurrencies (World Economic Forum, 2022).

The targets of these so-called cyberattacks have been diverse, ranging from small businesses around the world to multinational giants such as Telefónica and Equiflax. Even U.S. government institutions like the Florida Supreme Court have not been spared. In Colombia, companies like Sanitas, Audifarma, and EPM have fallen victim to this type of attack. Furthermore, educational institutions are also among the primary victims of cyberattacks due to the operational characteristics that facilitate the development of these intrusions into the technological infrastructure of schools, universities, technical, and technological centers.

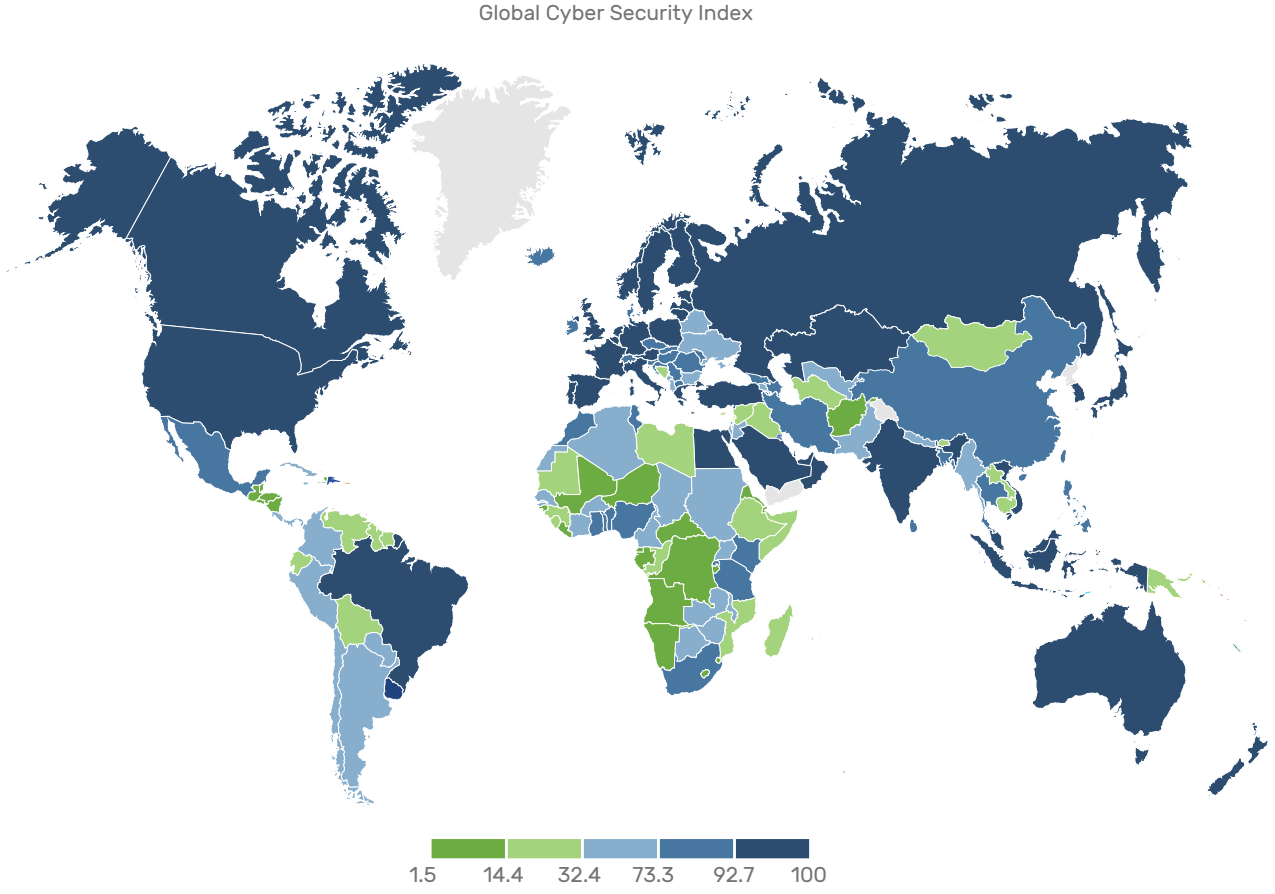
It is important to highlight that the volume of attacks on educational institutions is as high as that of large corporations. For example, the Universidad Javeriana in Bogotá and Cali, as well as the Universidad Autónoma de Barcelona, have fallen victim to **ransomware** attacks. In these cases, the main servers of the institutions are affected and become vulnerable **to data loss.** As a security measure, it is necessary to isolate all their services to prevent the spread of the attack. However, this measure comes with associated risks, such as service disruptions, decreased productivity, the possibility of temporary data loss, and extended recovery times. It is crucial to implement additional measures to mitigate these risks and **ensure the protection of the institution's systems and data.**

However, the percentage of the budget allocated to managing cyber risks in educational institutions, in general, is considerably lower compared to the attention it receives in the corporate sector. According to recent studies, while companies allocate an average of 10% of their information technology budget to cybersecurity, educational institutions allocate only around 2 to 3% of their budget to safeguard against cyber threats.

As a result of the above, the incidence of attacks in the education sector increased in 2022: a 56% rise in primary and secondary education and a 64% increase in higher education, compared to **ransomware** attacks in 2021. This represents a 44% increase since 2020, as reported in the cybersecurity trend reports by Microsoft and Sophos for 2022. As of 2023, 190 cyberattacks have been recorded so far, indicating an 84% surge in attacks in the education sector compared to 2022. These data prompt a global-scale question: **Does the country, and particularly the Special District of Science, Technology, and Innovation in Medellín, face cybersecurity challenges in ensuring data security?**

In order to understand the phenomenon facing globalized society, **the results from the 2020 Global Cybersecurity** Index are presented. This index aims to identify the primary challenges and advancements in terms of **digital security gaps** in over 193 countries worldwide. Since 2015, this measurement has been conducted based on five main pillars: **1.** Regulatory Framework, **2.** Technical Advancements, **3.** Organizational Strategy, **4.** Capacity Development, and **5.** Cooperation. Through these indicators, the objective is to assess and compare the state of cybersecurity on a global scale.

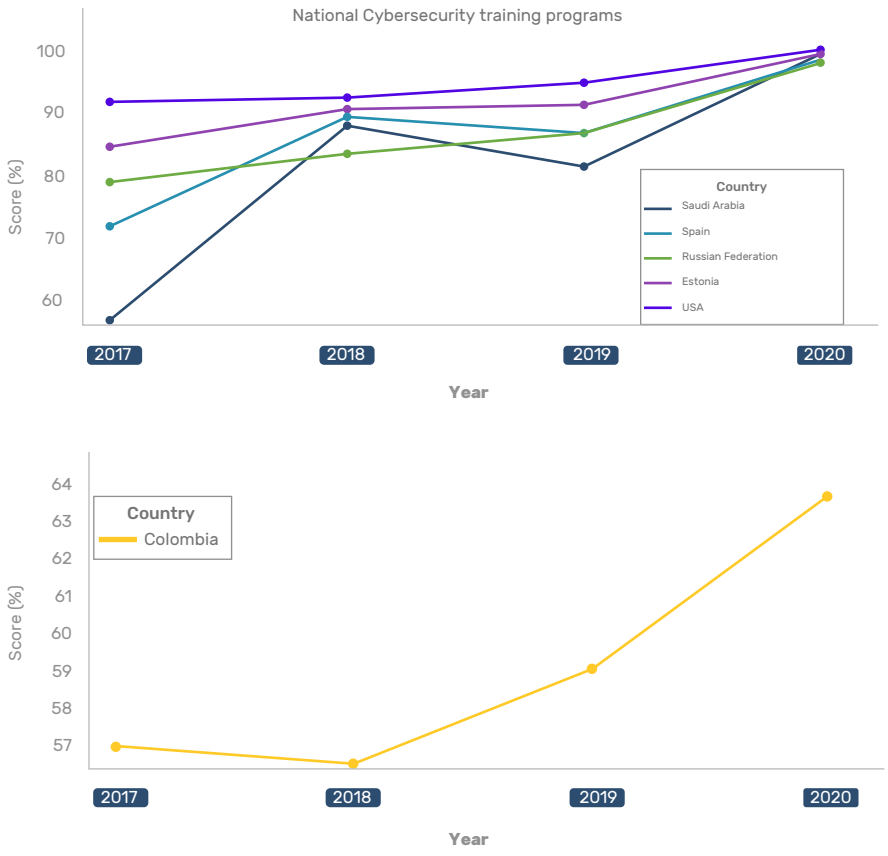
Graph 1. Subindex of National Training in Cybersecurity Programs Worldwide.



Source: Global Cybersecurity Index - European Commission.

Paradoxically, according to the Global Cybersecurity Index calculated by the International Telecommunication Union (ITU), the programs offered by educational institutions in Cybersecurity have increased until 2020. However, there is a current **global deficit of qualified personnel with these skills to counter the various forms of cyberattacks** in organizations in general and educational institutions in particular. While the subindex's trend tends to rise (see Graph 2), it is important for Colombia to offer early cybersecurity training to further enhance its level of expertise and workforce capacity in this field.

Graph 2. Behavior of the Subindex of National Training in Cybersecurity Programs in the Top 5 Countries in the World and Colombia for the Period 2017-2020.



The subindex of national training in cybersecurity **programs measures the quantity of educational programs** (including professional ones) related to cybersecurity. This graph illustrates the increase in the curricular offerings of such programs both globally and in Colombia.

Source: Global Cybersecurity Index - International Telecommunication Union (ITU).

Taking into account the aforementioned, in addition to the lack of trained personnel to prevent and combat various forms of cyberattacks, one must consider **the rapid advancement in the development of disruptive technologies.** These technologies have provided tools for carrying out cyberattacks from various perspectives. A well-known example is phishing and identity theft, which have become common in the post-pandemic reality due to the use of artificial intelligence. These attacks are characterized by generating personalized emails and text messages that appear legitimate, with the goal of deceiving users into downloading infected files or malicious software. Their primary objective is to extract confidential and sensitive personal information, including passwords, credit card numbers, banking data, home address, and/or phone numbers. By gaining access to this information, cybercriminals can commit identity theft, carry out fraudulent transactions, engage in extortion, or even sell the data on the black market.

In May 2021, the American insurer Colonial Pipeline fell victim to an attack by the 'DarkSide' group. Utilizing traditional **hacking tools** combined with artificial intelligence techniques, they managed to infiltrate the company's computer systems and encrypt their data. The group demanded a Bitcoin ransom to unlock the encrypted information. This attack jeopardized the fuel supply in a significant portion of the East Coast of the United States (Sardanyés, 2021).

In this sense, traditional training schemes face cybersecurity challenges, particularly for the Special District of Science, Technology, and Innovation in Medellín. Firstly, as mentioned earlier, educational institutions exhibit deficiencies in their technological infrastructure concerning **security protocols** and personnel training, impacting not only the information technology sector but also other involved stakeholders. Secondly, **the lack of timely training** in this technology field is a challenge, as Colombia does have academic programs dedicated to cybersecurity, but mostly at the postgraduate level.

Estos programas buscan formar profesionales especializados capaces de **enfrentar los desafíos y amenazas en el ámbito de la seguridad cibernética**. Sin embargo, es importante promover la creación de programas académicos a nivel de pregrado y fortalecer la formación en ciberseguridad desde etapas tempranas de la educación. Un ejemplo de esto son los cursos de **Talento Especializado,** ofertados por Sapiencia, que ofrece formación especializado en diferentes campos de la industria 4.0, entre ellos está la formación en ciberseguridad.

These programs aim to train specialized professionals **capable of addressing the challenges and threats in the field of cybersecurity.** However, it is essential to promote the creation of undergraduate academic programs and strengthen cybersecurity education from the early stages of education. An example of this is the courses of **Talento Especializado** offered by Sapiencia, which provide specialized training in various fields of the Industry 4.0, including cybersecurity training.

References

Jurgens, J., & Bissell, K. (2022). Global Cybersecurity Outlook 2022 in collaboration with Accenture. January.

Sardanyés, E. (2022). Cyberattacks launched with Artificial Intelligence. https://www.esedsl.com/blog/ejemplos-de-ciberataques-lanzados-con-inteligencia-artificial