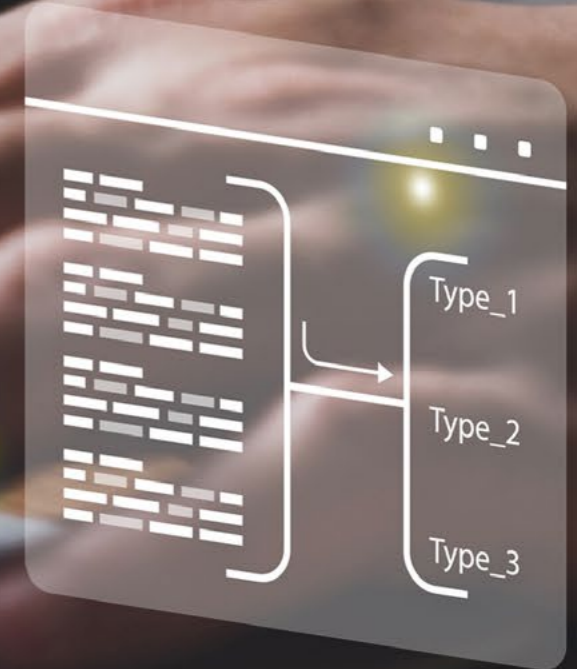
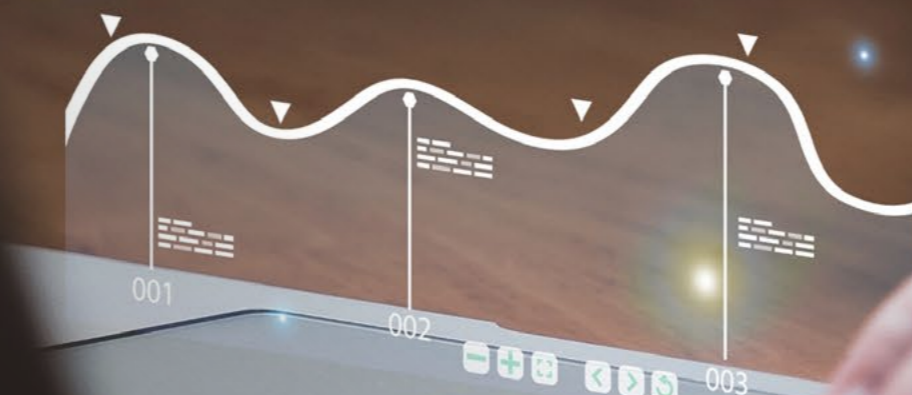


PROSEGUR RESEARCH

Hybrid Security Series

Data in hybrid security

2025



This is an **interactive document**

01

The ocean in the office

THE OCEAN IN THE OFFICE

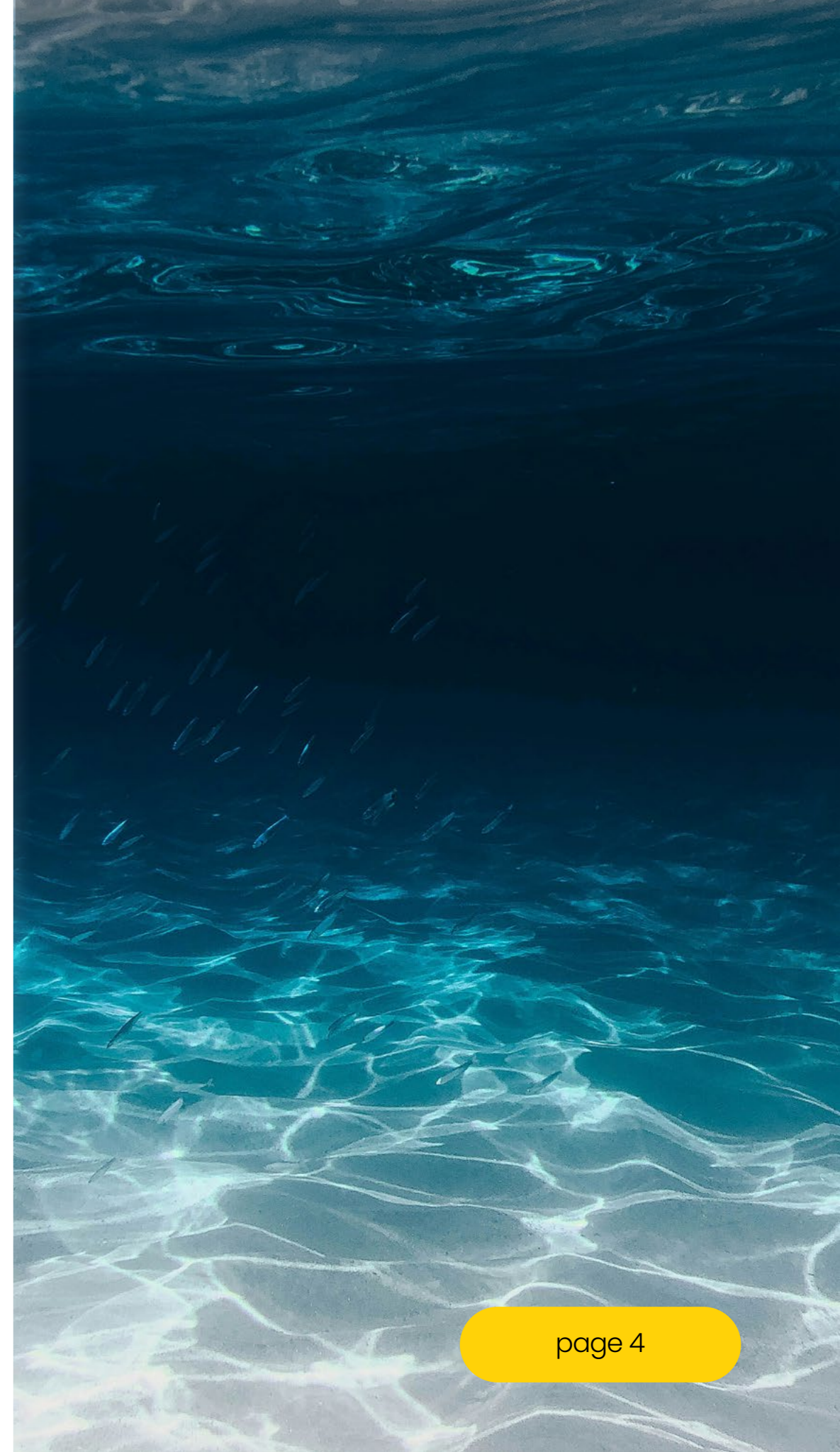


We live in the data age, flowing around us like a vast ocean of information. In this environment, the **ability to look** has become a crucial skill, a kind of compass that guides us through complexity and uncertainty. Like fractals¹, where each part reflects the whole in an infinite and repetitive pattern, data hides in its apparent chaos an underlying structure that is only revealed to those who have the insight to observe carefully.

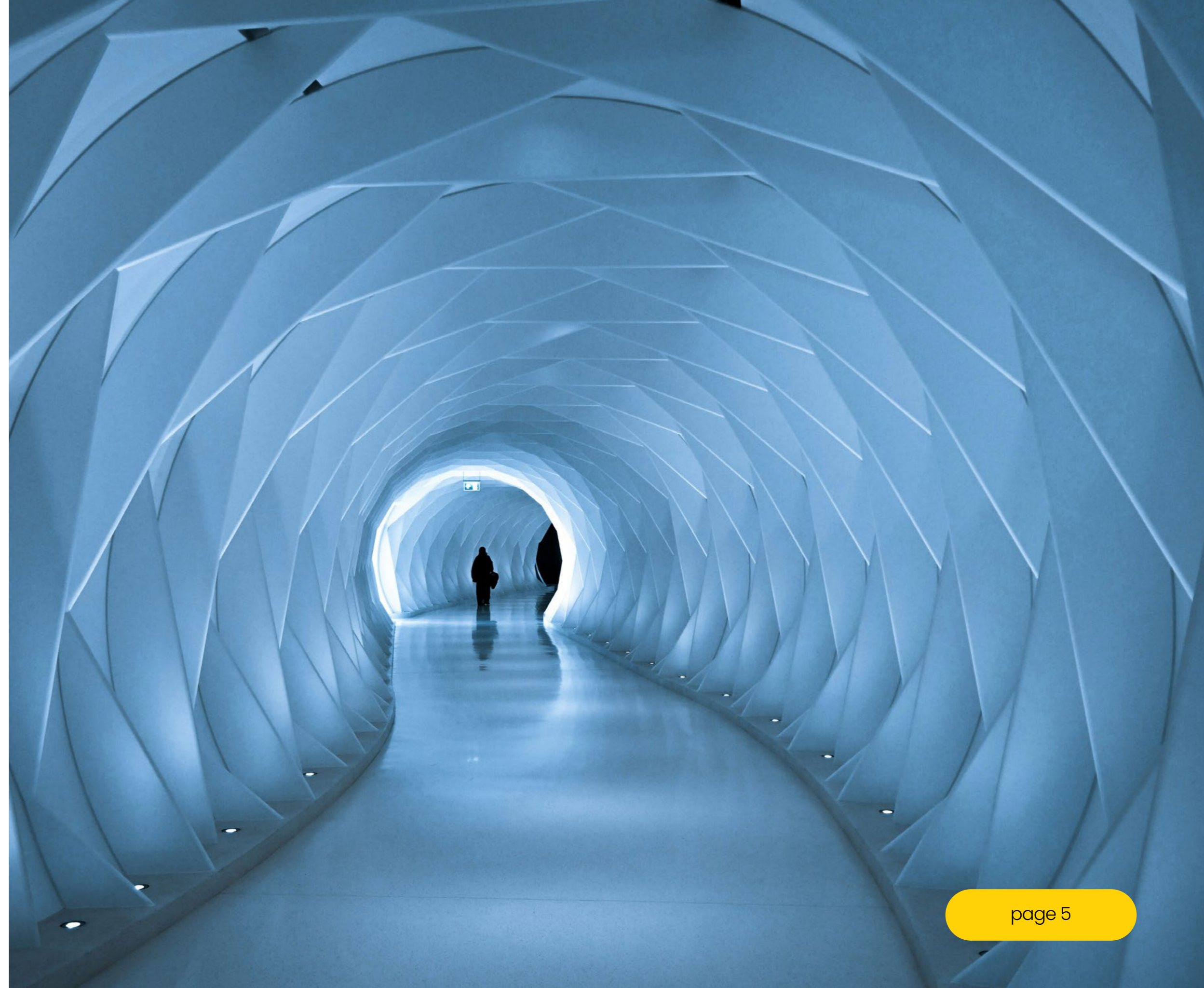
Those who master the art of data interpretation move with ease in a symbols' sea, finding patterns and connections undetectable to the naked eye, just as the jellyfish with its transparent and enigmatic body moves effortlessly in the depths of the ocean, **adapting and evolving, according to the trends.**

This is not a random ability; it must be worked on continuously and in many cases, it is created in childhood, **molded by the toys that surround us.** These first game objects, apparently simple, sow the seeds of our future cognitive and professional abilities, influencing the way we **look at our surroundings.**

¹ Fractals are geometric structures that are characterized by having an irregular, complex, and self-similar shape, which means that their pattern is repeated at different scales. In other words, if you zoom in on a small part of a fractal, you will find a similar structure (though not necessarily identical) to the fractal as a whole.



If the challenge is to **understand an ever-changing world**, where data is incessantly generated, it is clear that we must **improve our skills** to interpret the information that surrounds us. This forces us to review our analysis forms, the sources, and methodologies we use, and, above all, to **reconsider how we understand data**. We will achieve a better understanding of our paradoxical environment of data, both ordered and chaotic, if we manage to broaden and deepen our perspective, incorporating diverse views, **finding the data value** that until now we did not stop to observe.



Q2

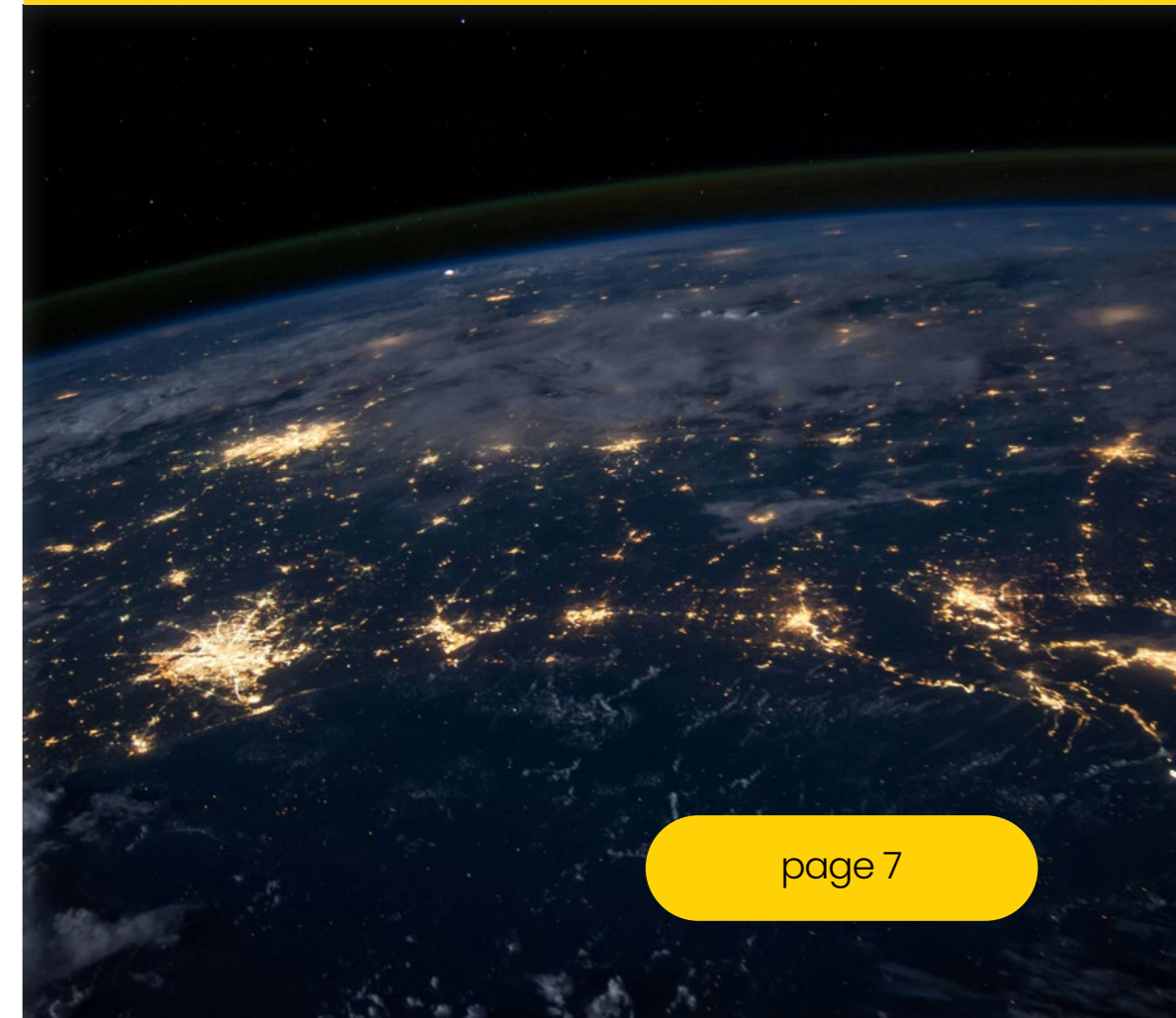
Data momentum

DATA MOMENTUM

The idea that reality is composed of a set of elements governed by superior rules and structures is not new. Just as Pythagoras explained that **everything is a number**. In the 5th century B.C., Democritus and Leucippus determined that the universe was composed of indivisible, eternal, and indestructible particles that, when combined, constituted what humanity could observe and feel. All this, based on reasoning and intuition. This is what we now call **situational awareness: ability to analyze the context** at different levels to respond to each situation in the most effective way possible.

In the top tier business environment, where agility and efficiency are essential, it is easy to be tempted to use data quickly and without a deep reflection. However, for data to become a truly powerful tool, it is crucial that companies **set aside and schedule specific times and spaces** to work with them thoughtfully. This involves not only understanding what data is, but **also critically exploring what it is for**, how it aligns with strategic objectives, and how it can produce real value. Without these pauses for analysis, making hasty decisions could become a risk, based on superficial interpretations that could divert the company course.

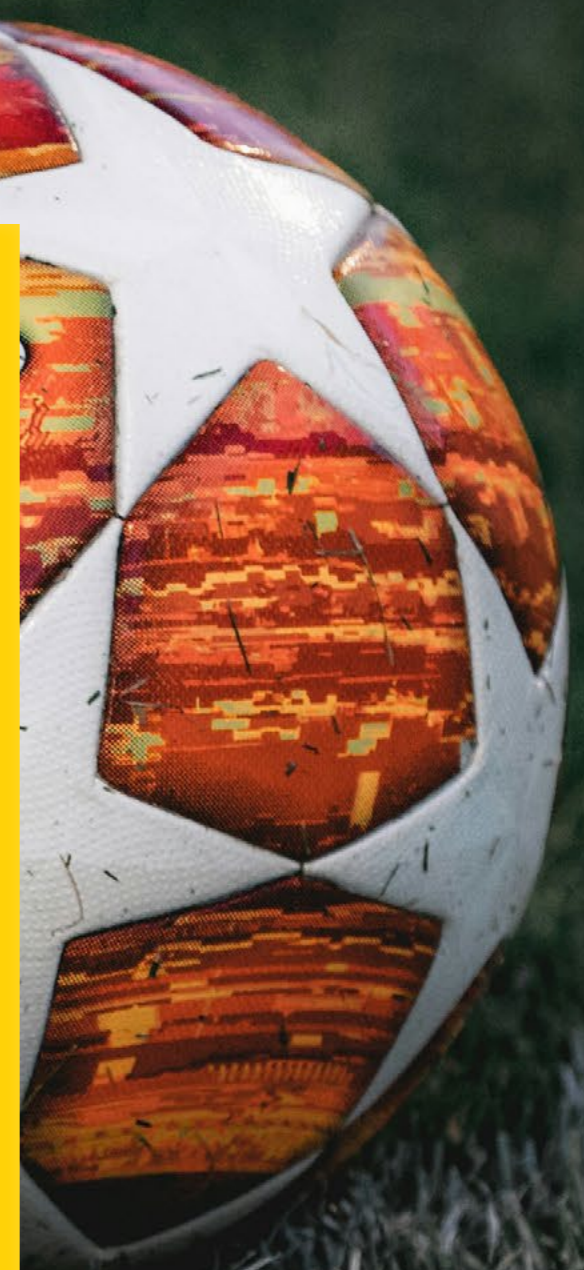
In a context where technology and data analysis methods are constantly evolving, the **upskilling** and **reskilling** need becomes critical. Employees must be equipped not only with technical skills needed to handle and analyze data, but also with **critical and creative thinking** ability about that data use. Ongoing training in these areas improves the team technical competence and fosters a business culture around data.



IN FOCUS: ANALYSIS IMPORTANCE

How important is the design of a ball in a sport like soccer? With the recent European Championship celebration, one of the silent spotlights has been placed on the championship official ball, the Fussballliebe. A group of Adidas engineers have used an innovative design that takes elements from other sports, such as golf, to ensure that the players' launches are not deflected and that the game is played properly: an invisible success, but large caliber. This is just one example of an underlying

essence in everything and everyone: mathematics and data. At the first moment of meeting, objects and processes of the environment may appear different and stranger to us. However, through their study and observation, information and data can be separated, with which interpret the fact and establish patterns and generalizations, ultimately enabling understanding and progress. From the Jabulani erratic paths of the 2010 World Cup to the 2024 European Championship Fussballliebe.

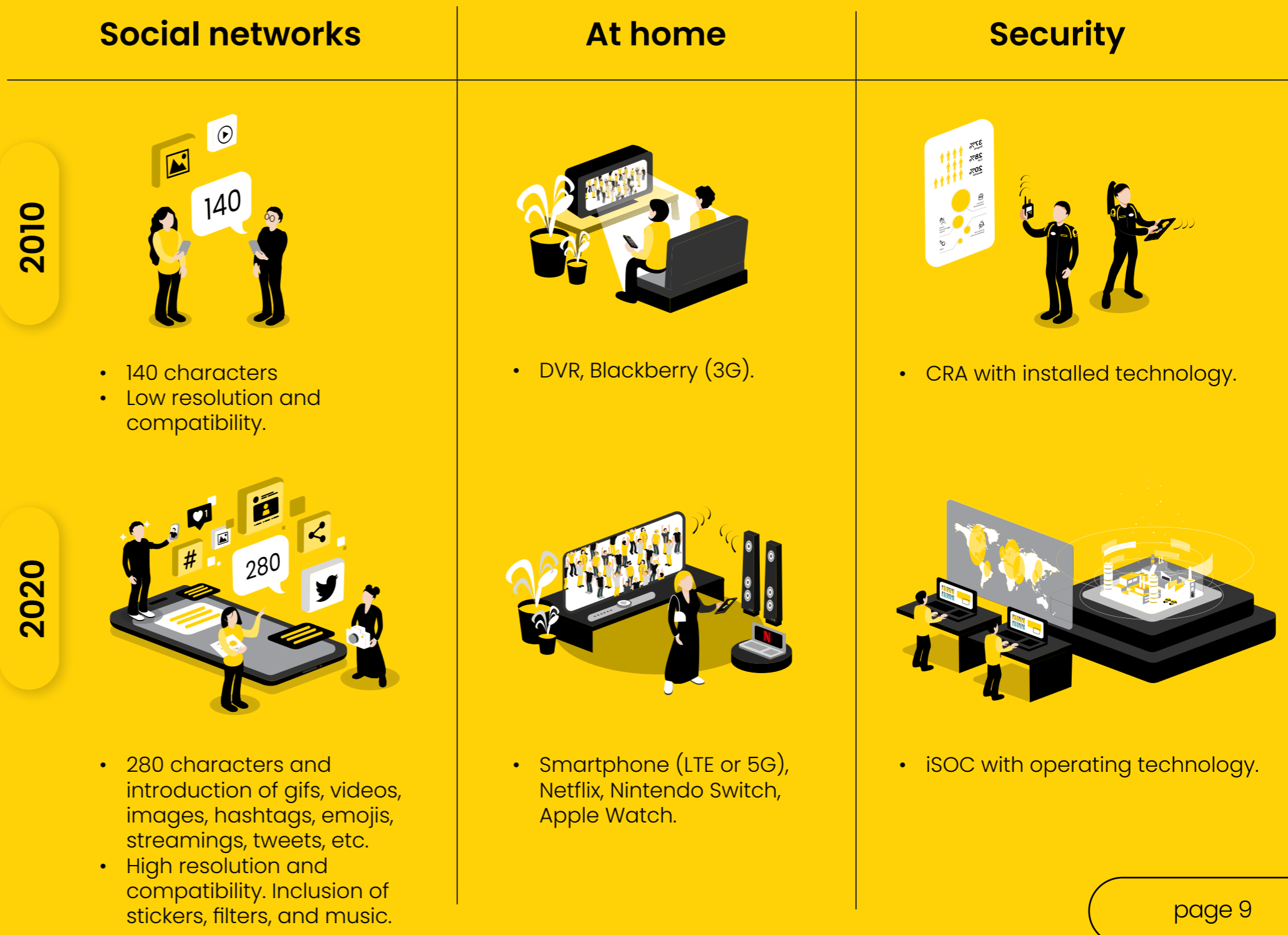


2.1. From data to insight

The data value has achieved an **unprecedented relevance in the current business** context, powered by digitization and the increasing amount of information generated in all the daily life areas.

We live in a context where **information and data do not only come from the physical environment**; our activity is also a data issuer, for example, when using certain digital platforms or being in contact with security cameras. In this new scenario, where there is a significant **data overload** and the true thing is sometimes difficult to tell apart from the false, it is important to highlight **analytical skills** when approaching information. In fact, institutions, such as the World Economic Forum point out that **analytical thinking** is one of the most demanded skills by employers today.

The growth of information density



In an environment where decisions must be made quickly and accurately, **data has become a crucial asset** that enables companies to anticipate trends and respond effectively to their customers' needs. The ability to analyze large data volumes not only facilitates the patterns and behaviors identification, but also enables organizations to develop more informed and tailored strategies to their specific objectives.

In addition, the data use in decision making means a significant improvement in operational efficiency and business profitability. By adopting a data-driven approach, organizations can optimize

their processes, reduce costs, and maximize return on investment. This is reflected in the **data-driven strategies implementation, approved by experts**, where every action is based on specific analysis, which minimizes errors risks and maximizes success opportunities. In this sense, data not only becomes a valuable resource, but also an innovation and growth driver. To optimize **decision making**, particularly in security contexts, information and data support of **both a strategic and operational nature** are of extraordinary relevance.

Otherwise, data importance also lies in its ability to personalize the customer experience. Companies

that use data to segment their market and understand the consumers' preferences can offer more tailored products and services to their needs. This not only improves customer satisfaction, but also fosters loyalty and retention, crucial in an increasingly competitive market. In short, **data value is today essential for the companies' survival and success** in a world where information is power. At Prosegur Research, according to our **hybrid security** model, we believe that **data must be analyzed calmly and in context**. This is done with the use of convergent and exponential technologies aimed at obtaining and processing it with human skills and the knowledge of security experts. This offers effective solutions in environments characterized by uncertainty, detecting threats and opportunities for organizations.



2.2. The data imperative

Following an inductive logic, **it consists of the creation of personalized answers after the raw data filtering and interpretation.** In this context the **data analytical marathon** becomes relevant: it is a conceptual model that describes the **process that companies must follow to transform data into actionable insights**, in other words, into useful information that can guide strategic and operational decisions. This approach is divided into several stages, each of which is crucial to ensure that the data collected is converted into effective actions that improve business performance.

The first step in this marathon is **data obtaining**, where the companies gather information from various sources, such as transactions, customer interactions, social networks, and other contact points. This phase is key, as the quality and relevance of the data collected will determine the success of the subsequent stages.

Once the data has been obtained, the next step is **preparation**, which involves information cleaning

and organizing to make it suitable for analysis. This process may include duplicates removal, errors correction, and data structuring into formats that facilitate their interpretation.

Visualization is the next one, where data is represented graphically to simplify its understanding. Through graphs, charts, and other visual elements, companies can identify patterns and trends that might not be evident in a raw data format.

Then we found **analysis**, where statistical techniques and algorithms are used to extract meaningful information from the data. In this phase, the aim is to answer specific questions and obtain insights that can influence decision making.

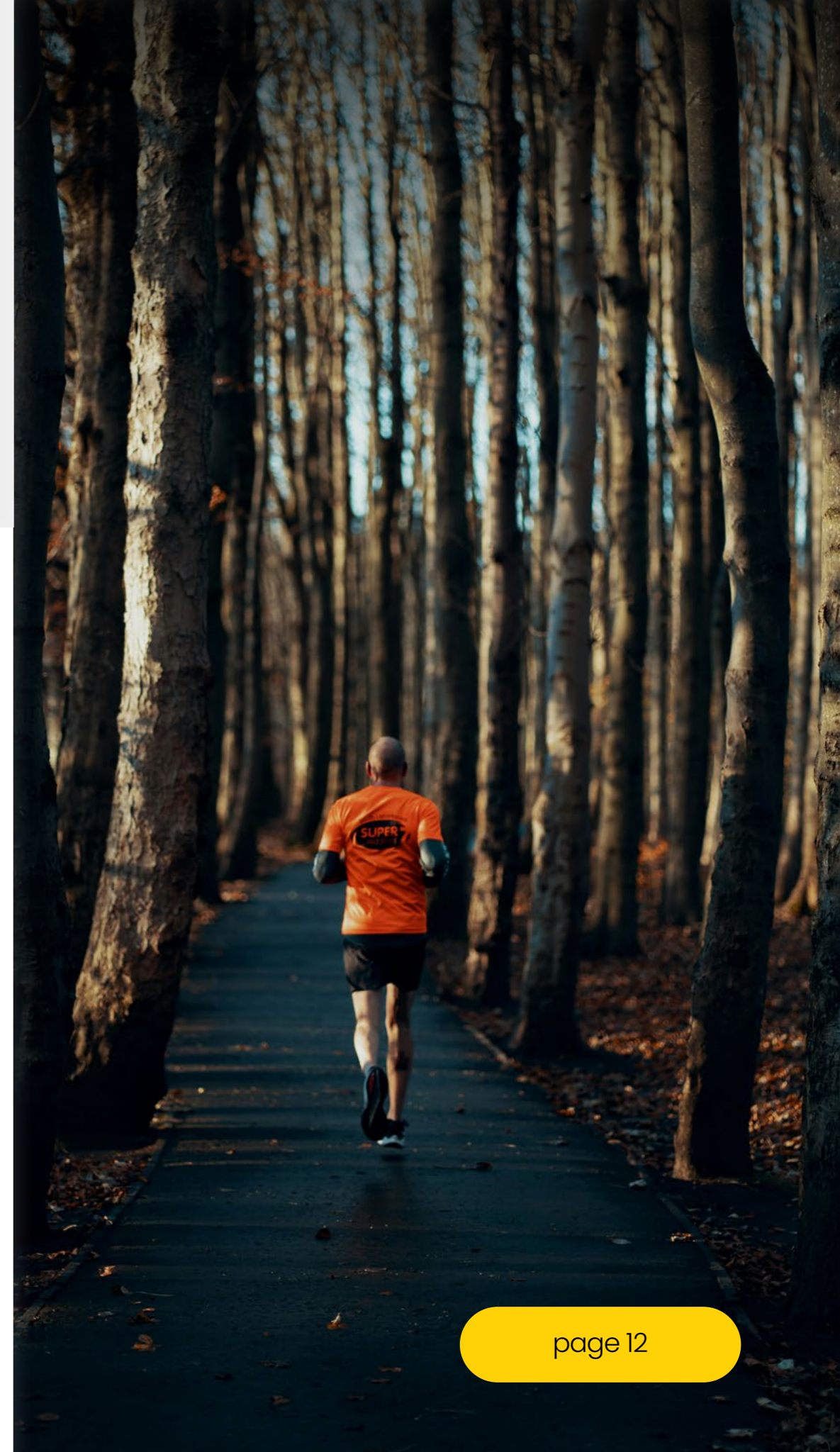
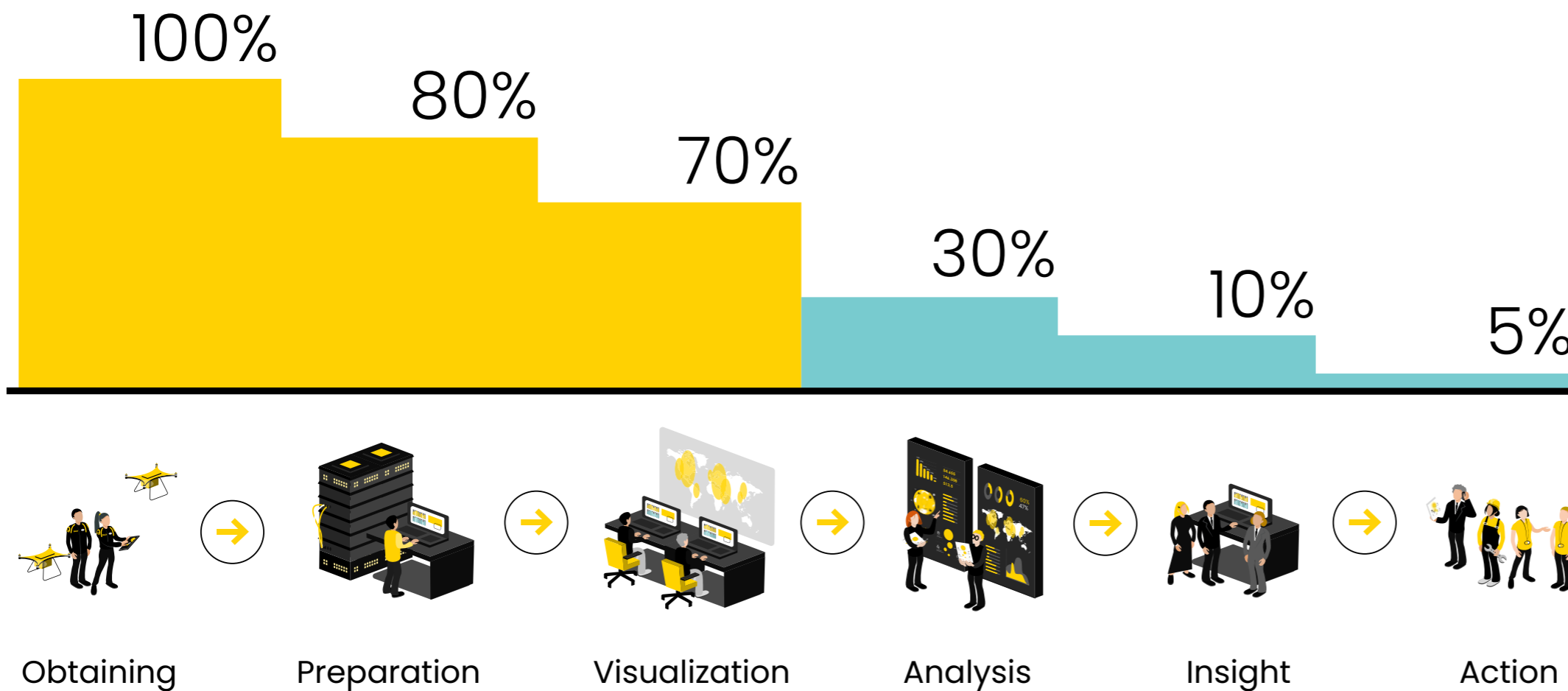
Once insights have been produced: **interpretation** or insight, where the relevance of the information obtained in the business context is evaluated. This is where the analysis is translated into concrete recommendations that can guide strategic actions.



Finally, the last step of the data marathon is **action**, where companies implement changes based on the obtained insights. This phase is critical, as many organizations remain in the previous steps and fail to take the required actions to capitalize

on the insights. A company's ability to close this "last mile" and act on the data is what really determines its success in an increasingly competitive business environment.

Source: Prosegur Research, 2025 based on Forbes.



2.3. Data value in hybrid security

Data and information extraction from the environment can be done through three mechanisms, which coordinate with each other: **open sources, human sources, and technological sources**. The data is processed in the iSOC, which from the combined use of technologies and security experts builds a comprehensive view able to produce informed and effective security solutions oriented towards optimizing decision making in the client and corporate field.



A **Open sources**



The **Internet exponential development**, in the last decades more accessible and with more operability possibilities have expanded the traditional methodologies oriented to data obtaining, increasing the range and projection of security and intelligence tasks. The data and information collection and analysis in open sources enables **real-time updating of information**, enhances **transparency**, develops **early warning** capacity in the weak signals' detection, and is able to develop **foresight trends**, extending the organization **situational awareness**. When analyzing open sources' data, it is necessary to notice the role of the analyst, capable of navigating in a sea of information and **noisy data**, determining the data reliability and validity, as well as its interpretation in a given context.



B

Technological sources



The exponential and convergent technologies adoption, such as cyberspace technology or drones, a **game changer in today's armed conflicts**, has become a fundamental aspect to produce quality inputs and outputs. Their ability to **obtain and store data in real-time as their ubiquitous presence in the environment** provides strategic data with 360-degree depth and range. These are quickly, effectively, and efficiently transmitted to **processing centers** and security experts, reducing uncertainty in decision making and improving implementation in the field.

C

Human sources



Fighting against one's own and shared **cognitive biases** and enhancing their capabilities enables the collection of valuable information and data from human sources, including security forces and corps, and security experts. In obtaining data, human sources can **interpret complex human and cultural contexts**, access interpersonal information, and adopt a flexibility and resilience position in the face of changes and disruptions in the environment in which they operate.

Inputs



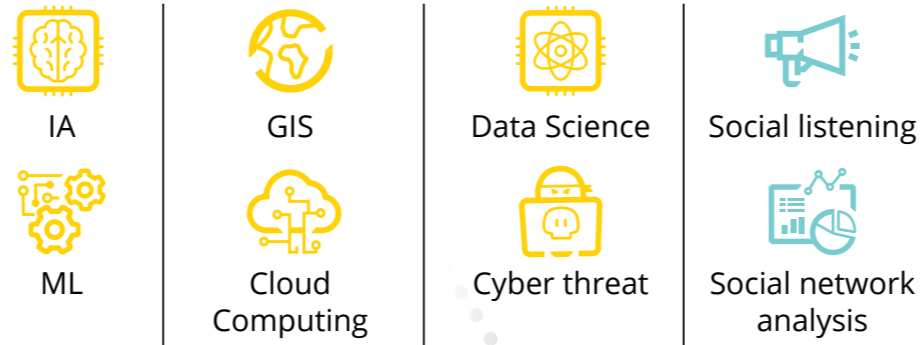
Technologies



Open sources



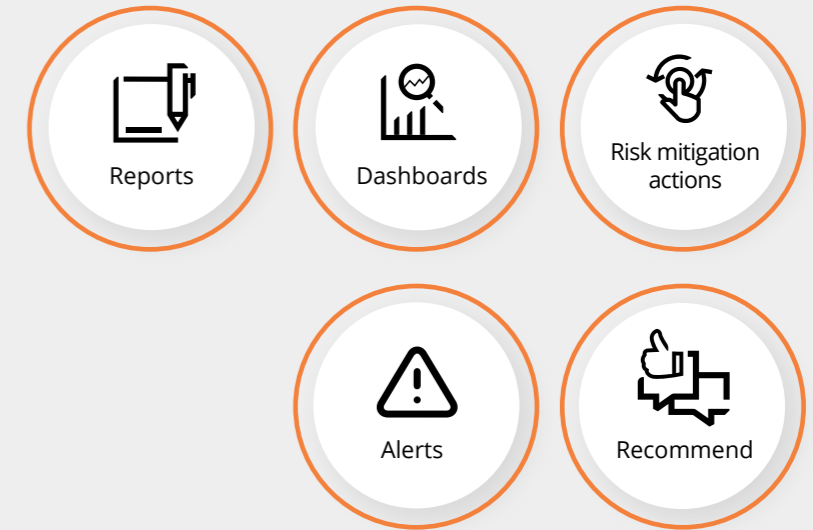
Technologies



Security experts



Customers



Corporate



Outputs

From all the data obtained from this enormous diversity of sources, an extraordinary value contribution is extracted in the hybrid security model

for the achievement of quality outputs, thanks to more innovative technologies and the experts working in and with iSOC. Examples of these can be early warnings,

comprehensive reports, and new products and services designed around the evolving needs of each customer.

1 Threat detection

Data can identify patterns and anomalous behavior that may indicate a current or potential threat. Through the analysis of large data volumes, security systems can detect unusual activity in real-time, facilitating a fast and effective response to security incidents by responsible professionals.

3 Technology research and experts

In order to integrate various technologies and experts, data is essential. Providing real-time feedback to security guards, agents, analysts, engineers, etc. This integration enables a holistic security approach, where data from different sources is combined to provide a more coordinated and effective response.

5 Intelligence for anticipation

By analyzing historical and real-time data, organizations can anticipate potential threats and vulnerabilities. Intelligence enables companies to adopt proactive measures to mitigate risks before they materialize, thus improving organizational resilience and competitiveness in the market they operate in.

2 Resource optimization

Data enables companies to place resources more efficiently, indicating the technologies and people needs in real-time. By understanding where and when threats occur, organizations can target their surveillance and response efforts to greater risk areas, maximizing the effectiveness of their security operations.

4 Personalization of services

The collection and analysis of data, when it is of high quality, allows security services adaptation to each client's specific needs, like a tailor-made suit. This includes the surveillance, technology, and intelligence solutions personalization, resulting in a more relevant and effective service.

6 Regulatory compliance

Data management in the context of security also helps organizations comply with regulations and standards related to data protection and privacy. This is especially important in an environment where transparency is a core value for trust.

7

Training and awareness

Data can also be used to train and raise employee awareness about security best practices, identifying where more training is needed and developing specific programs to address these needs.

8

Continuous improvement

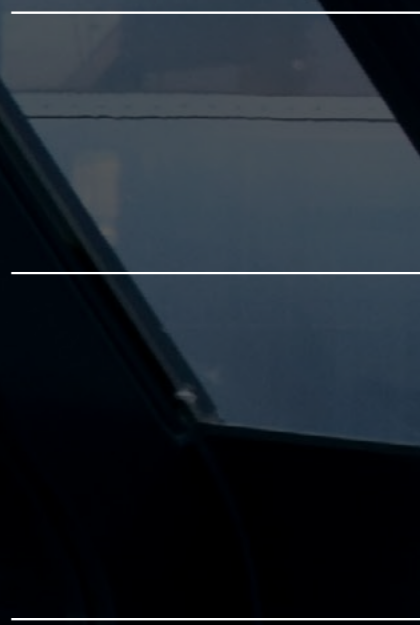
Data provides a basis for the continuous evaluation and improvement of security strategies. Thus, they allow adjusting policies and procedures for a better emerging threat addressing, understanding the flexibility demanded by the changing world.

However, this is **not only achieved by having an organization that generates the data**, we must also not forget the essential human element for strategic data use: the data culture, explained below.



OSB

Data culture: competency framework



DATA CULTURE: COMPETENCY FRAMEWORK

3.1. Information disorder

The complexity and scale of information pollution in our digitally connected world present an unprecedented challenge.

Claire Wardle, Information disorder. Toward an interdisciplinary framework for research and policy making

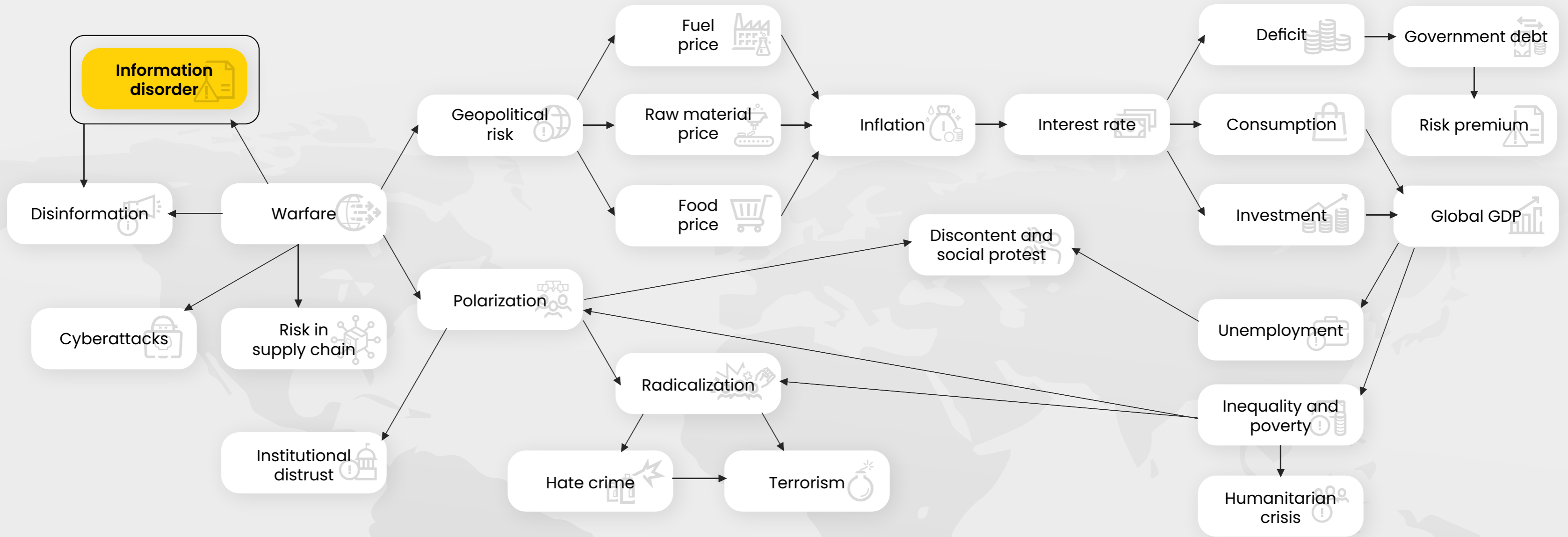


The current environment is characterized by information disorder: although information has been used for thousands of years both as an enhancer of human development and as a weapon, nowadays the exponential development of technology and connectivity has led to greater ease of access, production, and distribution of information (in a timely manner) to boost the materialization of phenomena, such as disinformation campaigns, including the so-called **fake news, post-truth**, and the **content falsification by generative artificial intelligence**. The way of understanding armed conflicts has also been deepened; its evidence is the emphasis that **international organizations** and states have placed on issues, such as **hybrid warfare** and **threats**.

Despite this, data and information technologies also have a **liberating component**, as they have **empowered** citizens by enabling new forms of protest and expression of demands against the traditional centers of power, breaking down the access barriers to these, and having an impact on the **multipolar nature** and diffused power of the current panorama.

Moreover, in the current technology implementation context with commercial purposes as **algorithms recommendation**, some judgment mistakes or cognitive biases may be enhanced, leading to **echo chambers** or **filter bubbles** phenomena.





Fuente: Prosegur Research, 2025.

In short, the **general information disorder environment affects security**, damaging confidence in institutions and democracy, manipulating public

opinion, and producing a potential negative impact for organizations. Additionally, it involves personal safety, strengthening scams and individual's radicalization

through the publication of misinformative or misleading content.

IN FOCUS: MALICIOUS DATA USE WITHIN THE BUSINESSES



The information disorder extends to the business sector, which materializes in the **data misappropriation and the information manipulation** from the perspective of employee empowerment, with progressive data access and

increasing control difficulty by organizations. In a context of permacrisis and diffused power, ***internal fraud*** shakes many companies, and ***no entity is exempt from committing this type of crime.***

3.2. The need for the human factor

To answer the information disorder era is not an easy task so the challenges to face are complex. For this purpose, is necessary to understand reality, where people and things are, and rely on technological developments able to guide us to a more secure future.

Data does not speak
itself, [but] we need
intelligent questions

*Luciano Floridi,
Menos tech y más Platón*

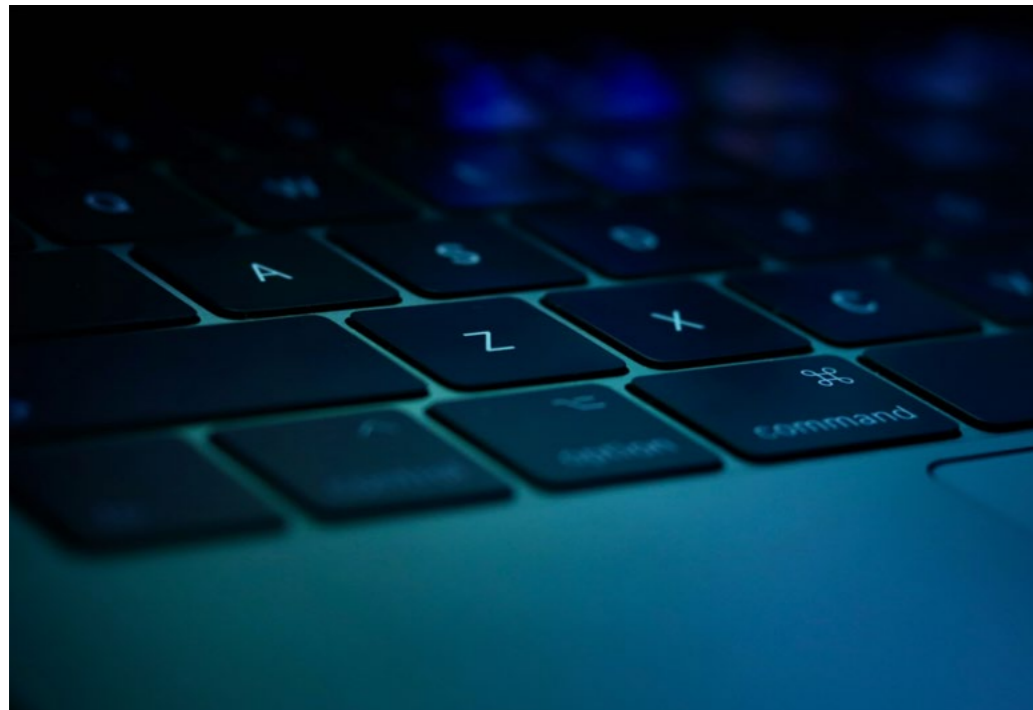
Part of that progress is now focused on **digital literacy**, aiming to work in an environment of rich information and potentially polluted. Digital literacy helps to understand that information and data have meanings and values embedded in them, and that they are not immutable realities. In other words: **data does not speak for itself**. **Rigorous professionals** training capable of examining the disponible data, providing a qualitative and contextual value is needed. **Michael Li**, founder and president of The Data Incubator, goes a step further when explaining that before companies can monetize data they must first understand it. **Being data literate is a competitive imperative** both for companies and for their employees.

In the information disorder context, and as a set of personal and structural competencies, today's literacy **fight disbelief and distrust** by developing the experts and citizens **critical capacity**, mastering digital tools to understand meanings, and messages in data and information.



3.3. Data skills in hybrid security

In the **hybrid security** conceptual framework, and related to data, **four types of skills** have been identified, creating a **systemic approach** so each category complements the rest. These are located transversally at the organizational and human level.



A Security skills

In **uncertainty and information disorder environments**, professionals must acquire and enhance political, economic, social, and environmental skills aimed at managing the risk that information and data possess. For example, **knowing the physical security requirements** of a given infrastructure helps to determine the needs of the service by analyzing historical data on intrusions into it.

In addition, **legal, regulatory, and business best practices knowledge** ensure operational services optimal management. ISO 31030 is a clear example on trips and travel risk management. In the current context, in which the **digital area** has a major role to play, skills in the field applied to security are essential for maintaining business continuity. As an example, stands out images collection by technological sources, such as drones, in accordance with current regulations.

Likewise, **regular updating of security protocols**, such as actions in case of bomb threats, partially minimizes the risks faced by customers or users.

Lastly, given the existing sources diversity: news, reporters, reports, think tanks, social networks, etc., hybrid security professionals must learn to **handle, manage, and properly use a correct knowledge base**. In this regard, **early alerts detection** about security incidents helps risks prevention that may affect organizations; for example, identifying social unrest that could affect the supply chain at critical or strategic points, such as seaports with high commercial activity, which can help readjust in a timely manner the strategic planning of potentially affected corporations.

B

Digital skills

Digital skills ensure the optimal handling of those tools for collecting, processing, and analyzing a multitude of data sources –video surveillance cameras, drones, robotics, etc.

First of all, **the design, implementation, and use of technologies to obtain information and data** stand out. Accelerated technological cycles (the constant introduction of new tools and functionalities) together with obsolescence, require professionals to constantly adapt to new tools. The drones' implementation in perimeter surveillance services has not replaced the connected security guard but has created the need for professionals with greater specific knowledge in their use and handling. In addition, these devices provide valuable supplementary information, such as aerial images or access to remote locations.

Otherwise, technological development creates new business opportunities and consequently **new professional growth niches**. Examples of this are the traditional use of land vehicles or the recent jet skis incorporation to port surveillance services,

requiring professionals who know how to use them efficiently.

Secondly, the exercise of **competencies linked to technological and digital know-how** is relevant. Organizations must be aware of the **latest technological trends** and study their integration into the business line, noting their evolution and expectations, relying on models, such as the **Gartner hype cycle** or the **three horizons of growth and innovation**. In this regard, some of the latest relevant trends with impacts on the security sector are linked to reconfigurable intelligent platforms or computer vision for image analysis.

Therefore, multidisciplinary teams of experts must operate with both basic and advanced technological tools. In this scenario, **digital and data literacy** is by professionals consolidated as a necessary and widely demanded skill, developing competencies oriented to the effective use of the technologies took in the workspace.



C

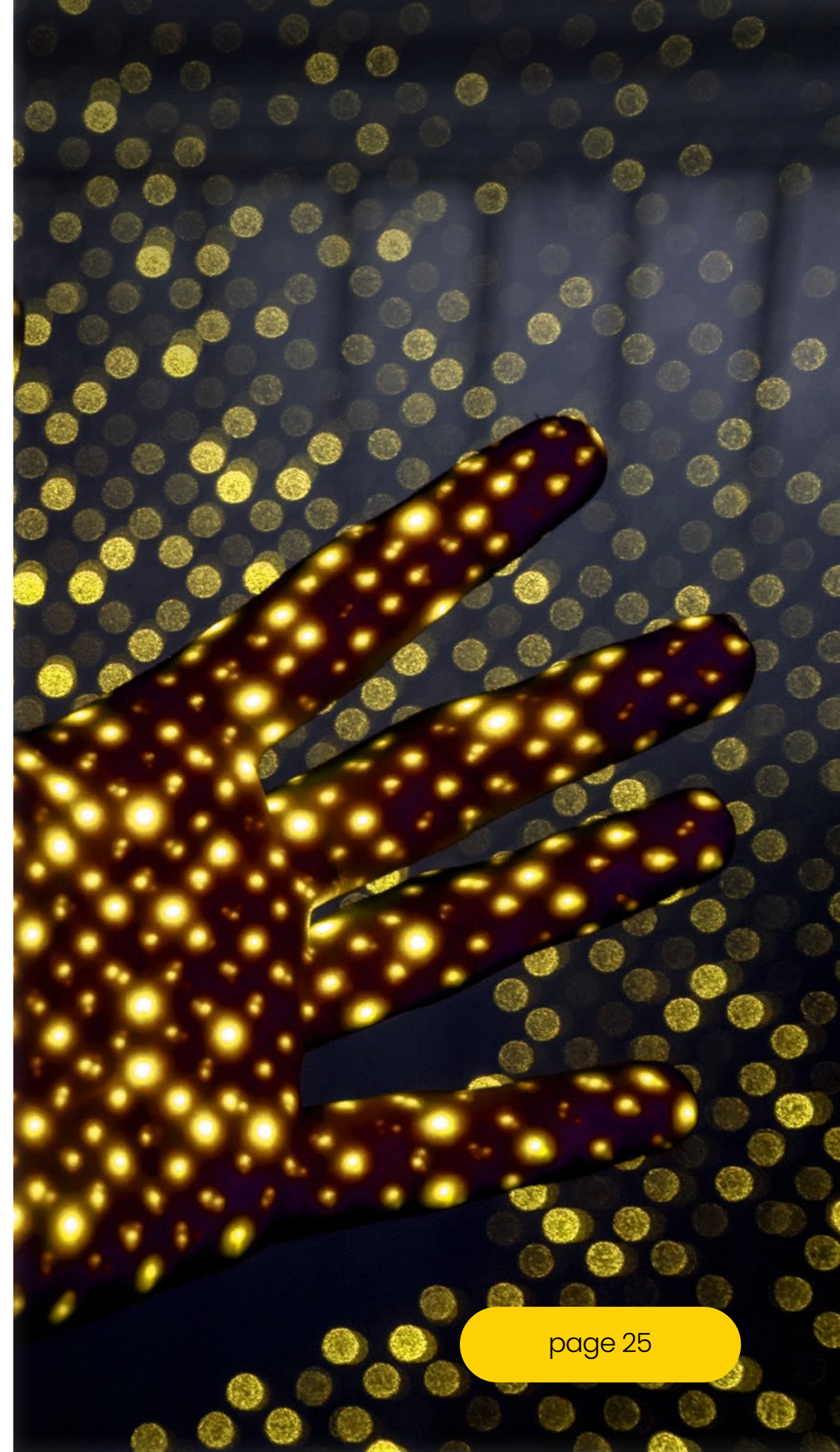
Human skills

These are eminently human competencies, based on a qualitative aspect or *soft skills*. **Data on its one has no meaning so the skills of security experts are essential**, such as complex problem solving and creativity **-think outside the box-** in order to add real value to information and to avoid making approximation mistakes, such as **McNamara's fallacy**.

With the large data volume that organizations handle today, **critical thinking and information analysis** is one of the most relevant aspects for data management and to advance in the marathon to the last mile. Thus, the ability to identify patterns and relationships, as well as to assess their impact, among data that affect customers' business operations is one of the main skills in demand. For example, a security incident, such as a theft, at a particular point does not necessarily indicate that there is a problem. However, modus operandi identification similar in different geographical locations, within a short period of time may require the deployment of mitigation and prevention measures.

Likewise, the ability to **disaggregate information** from different sources and then integrate them under the same meaning is a necessary skill to work in dynamic environments, fitting in the general context of recombinant data in hybrid security.

Otherwise, **responsibility** is critical to understanding and managing the ethical implications of data management. **Integrity and confidentiality** to ensure privacy, good customer relations, best governance practices, and the limits set by law can only be carried out by the best employees trained in the area. Examples applied to competencies include respect for privacy in the case of review of recordings by operators of residential areas.



D

Self-management skills

Obtaining and processing data can be a complex process, as information is cluttered, contaminated, and in large volumes in the information environment. In order to be able to navigate effectively in changing and emotionally challenging environments, experts must develop added value behaviors in the hybrid security model. These include resilience towards environmental disruptions, for example, in the constant updating of data in open sources; **frustration tolerance** in accessing information, which may be incomplete, disrupted, or deleted; or **flexibility** in dealing with large complex and messy data volumes.

In daily operations, the time sometimes goes against security professionals. The **immediacy** required in risk situations results in the need for professionals who know how to prioritize and stay calm. For example, in crisis situations as a violent context in a social unrest, requires workers to ensure a quick and efficient response.

Thus, in the acquisition and enhancement of these skills, **active learning** and, as a whole, working in **multidisciplinary teams** is of great help, whose members are able to provide differentiated but complementary views on the data obtained and their implications for safety and business lines.



In summary, the data culture in companies is essential for several reasons that directly impact their ability to compete and adapt to an ever-changing business environment. First, **a data culture fosters informed decision making**: when employees at all organization levels value and use data in their daily work, reliance on assumptions is reduced, which in turn minimizes errors risks and biases, and if there is quality and properly contextualized data, **accuracy improves** in strategy planning and execution.

Furthermore, a strong data culture promotes **collaboration and transparency** within the organization: sharing data and analysis across departments facilitates a more integrated and cohesive approach to address problems and opportunities. This not only improves communication,

but also enables teams to work together more effectively, exploiting different perspectives and understandings to generate more flexible, customer-tailored solutions with the Security-as-a-service vision.

Data culture also **drives innovation**, so when employees feel empowered to data exploring and experimentation, they can identify new business opportunities, optimize existing processes, and develop products or services that better meet market needs. This **proactive mindset** is essential for companies to stay relevant and competitive in a world where technology and consumers expectations are constantly evolving.

Meanwhile, data culture contributes to **organizational agility**; in a business environment characterized by

uncertainty and fast change, companies that adopt a data-driven mindset can adapt faster to new circumstances. The ability to analyze data in real-time enables organizations to respond more effectively to market trends, customer needs, and emerging challenges.

Finally, fostering a data culture also helps companies develop **greater confidence in** their people-aware **decisions** throughout the entire hybrid security model. When employees see that decisions are based on specific data and rigorous analysis, a sense of security and legitimacy is created in the actions taken; this not only improves motivation and consequently team performance, but also strengthens the company's reputation before its customers and partners.

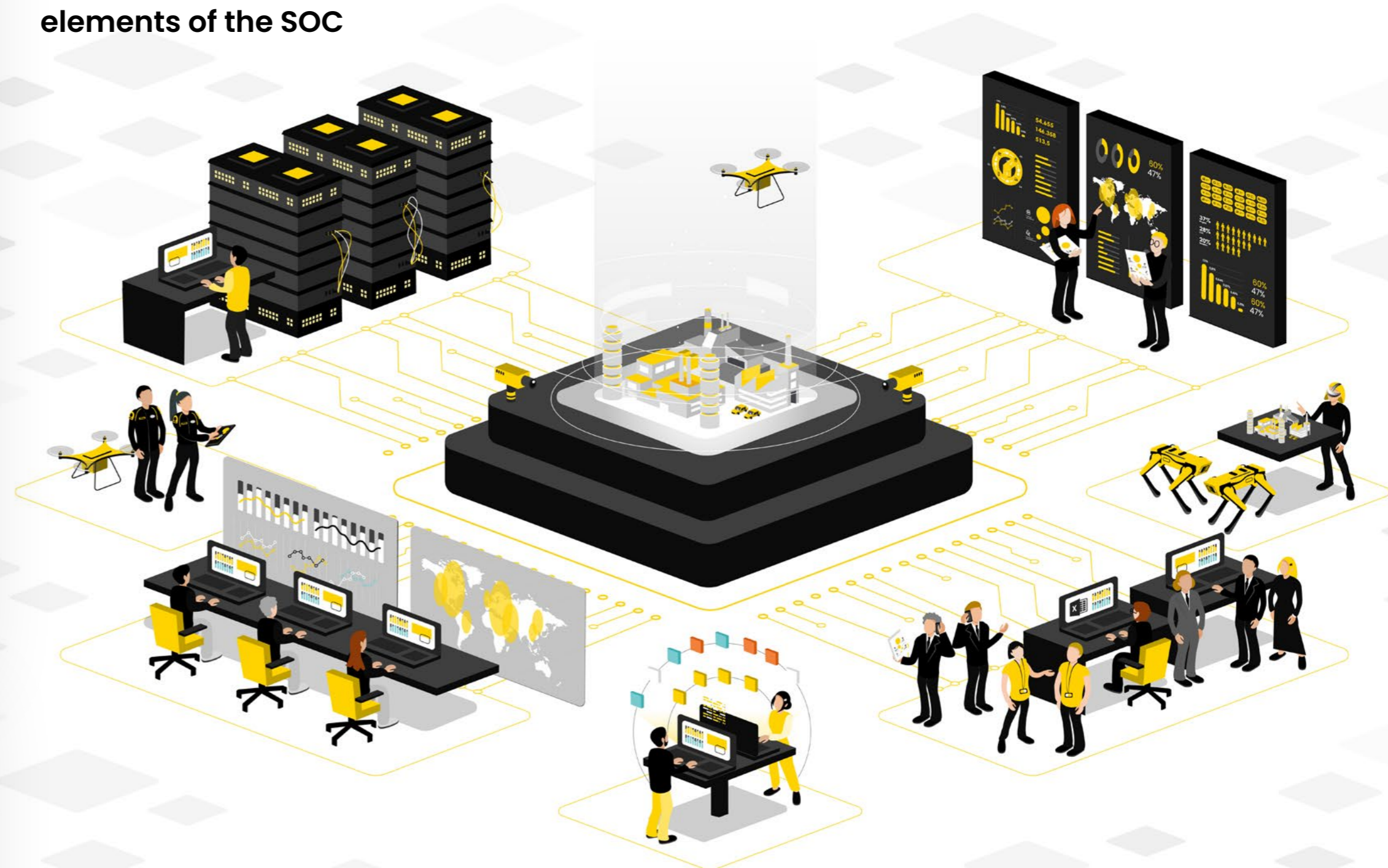


Data becomes valuable when it evolves in an **appropriate ecosystem**, when it can be correlated with certain interest topics. Therefore, the data quantity, quality, and integration will determine its value.

Its strategic exploitation derives from the integration of all these sources worked by the best security experts and the most innovative applied technologies. At iSOC, data is used to provide immediate operational and strategic response; in the hybrid security model it is transformed into intelligence, which allows to anticipate and mitigate risks, taking advantage of experience to produce a high-level processing complexity. Thus, it leads us to **present and future action, managing uncertainty** and anticipating security challenges.

This is the key to the security paradigm shift we are experiencing: technological convergence and the data intelligent use in the **iSOC** allow us to anticipate changes, **alongside with the world in its transformation.**

Functions and core elements of the SOC



Source: Prosegur Research, 2025.

04

Data for reliable
hybrid security

DATA FOR RELIABLE HYBRID SECURITY



We live in an era where **data generation is relentless** and is deeply transforming our world, altering not only our societies, but also our very nature as human beings. If we look to the past, we can find interesting parallels with the **way technology and information have been welcomed and understood** throughout history. In the early 20th century, some experts believed that the telephone, by eliminating the personal contact need, could lead into social isolation. Even much earlier, Mary Shelley's 1818 novel *Frankenstein* was a warning against using technology to play God, and how it might blur the lines between what is human and what is not.

Or to go back even further, we find in Plato's *Phaedrus*, around 370 BCE, a reflection by Socrates suggesting that writing could be a detriment to human memory, since once something is written, we would no longer need to remember it. These historical concerns invite us to reflect on the skills we will need in the present and near future.

In this context, **connection is vital for integration**, needing understanding models of the world, such as hybrid security and the iSOC, its brain, which are deeply linked to the data culture. This culture requires a shared understanding and **collective commitment** to take advantage of the full data power, without falling into the paralysis trap by analysis.



In this case, Prosegur Security works with more than a million connected devices and more than **160,000 experts who strategically manage more than 1.5 million security events and data per year.**

Data overload can be paralyzing, but this reality also calls us to action. To overcome this paralysis, we must all actively contribute; collaboration and cooperation is what promotes the world civilization, as Louis Klein states with his famous quote **“the more integration advances, the greater the common benefit.”**

At Prosegur Research we know that this means building **trust among people, having the determination to promote change, and collaborating to integrate** different perspectives and knowledge. All this is achieved when there is coherence in projects and ideas, and when *we all speak the same language*, what means that we share common and consensual terms and definitions. This also requires reflection and a lot of dialogue, which is: adequate context and quality contact. Thus, we achieve an **intelligent integration** that allows us to make the world a safer place.



We guarantee the safety of individuals,
companies, and society as a whole.