PROSEGUR RESEARCH

Hybrid Security Series

People in Hybrid Security

2024

PROSEGUR SECURITY

This is an **interactive document**

01

People as priority

01

PEOPLE AS PRIORITY

People are the main protagonists of 2024, as we already warned from **Prosegur Research,** and it is **up to each one of us to understand the big changes that are approaching.** Adapting, anticipating or even taking advantage are the three -ings that we aim to go by.

> " If there is something in us truly divine, that is the will. Through the will we affirm the personality, we temper the character, we defy adversity, we rebuild the brain, and we improve ourselves every day.
>
> **Santiago Ramón y Cajal**

From a systemic vision and understanding the impacts and interdependence of the global world, **Donella Meadows** gives us **14 interesting tips for operating in a "world of systems."** In this report we will explain the context in which we must receive these under the business transformation that we are experiencing, as well as the specific security environment, of increasing complexity, where these tips can become critical.

Graphic 1
Tips from Donella Meadows for a systemic world

1. Get the beat.
2. Listen to the wisdom of the system.
3. Expose your mental models to the open air.
4. Stay humble. Stay a learner.
5. Honor and protect information.
6. Locate responsibility in the system.
7. Make feedback policies for feedback systems.
8. Pay attention to what is important, not just what is quantifiable.
9. Go for the good of the whole.
10. Expand time horizons.
11. Expand thought horizons.
12. Expand the boundary of caring.
13. Celebrate complexity.
14. Hold fast to the goal of goodness.

Source: Prosegur Research, 2024 based on Donella Meadows, 2024.

Ultimately, as opposed to the obsession for control and prediction, Meadows explains that **systems cannot be controlled, but (re)designed.** In other words, to learn to dance with these complex systems. Hence, living in a world of systems also implies the ability to calculate, to distinguish truth from lies, along with rationality, imagination, and ethics, among others.

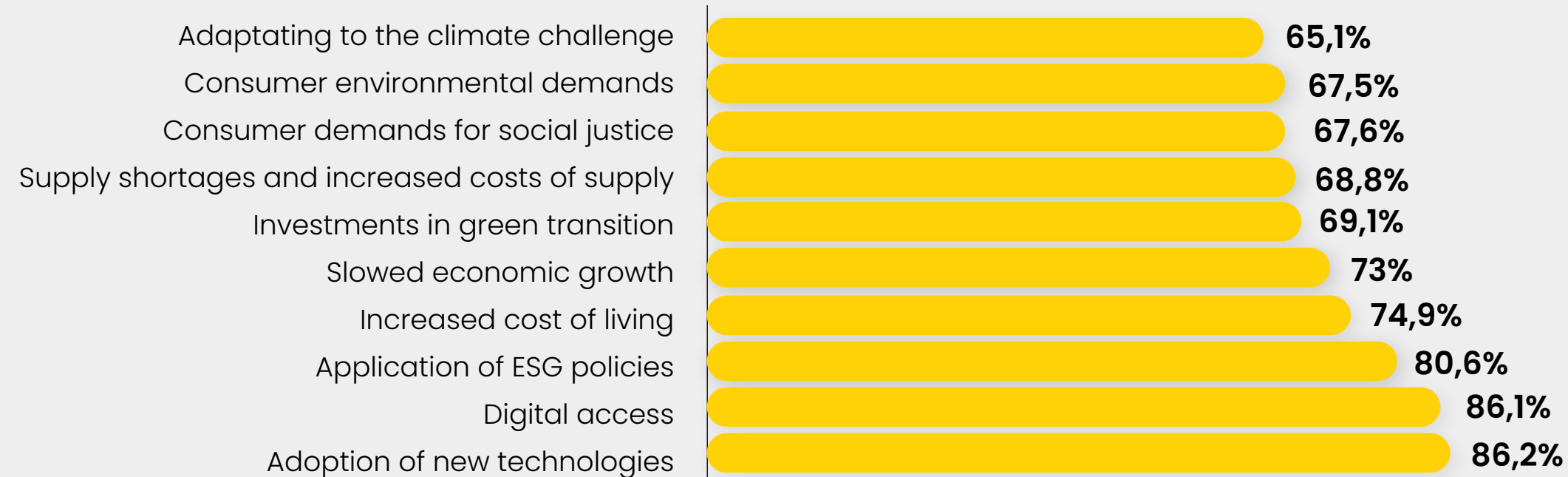→ (A) **Skills for**
a changing world

The constant transformation of the environment in which we are immersed requires a continuous **capacity to adapt to changes** at all levels, from technological or climatic to economic and political. Widespread uncertainty is leading to **growing tension and concern among workers,** with a demand for their well-being, decent living conditions and a working purpose towards a common goal, which has been reflected in recent phenomena such as the **Great Resignation.**

In this sense, drivers such as technology, demographics or socioeconomic conditions are having a profound impact on the way work is carried out, allowing for a resetting of the labor market at a global level.

- According to Adecco, **one in two workers wants to change jobs,** mainly looking for a higher salary, even though up to 44% would agree to remain in their organization if they are committed to **career progression and reskilling efforts.**

- According to the World Economic Forum's **Future of Jobs Report,** up to 60% of all employees will need to review and **learn new skills and knowledge** by 2027 in a process known as **reskilling.**

Graphic 2
TOP-10 drivers for business transformation as % of opinion

Source: Prosegur Research, 2024 based on *WEF*

Adaptating to the climate challenge	65,1%
Consumer environmental demands	67,5%
Consumer demands for social justice	67,6%
Supply shortages and increased costs of supply	68,8%
Investments in green transition	69,1%
Slowed economic growth	73%
Increased cost of living	74,9%
Application of ESG policies	80,6%
Digital access	86,1%
Adoption of new technologies	86,2%

Already in 2019, the Organization for Economic Cooperation and Development (OECD) indicated that **in the next 15 years up to 32% of all jobs in the world would radically change** due to new technologies, making reskilling and re-skilling workers more necessary than ever before. However, studies by Boston Consulting Group (BCG) point out that only 24% of organizations show a clear connection between corporate strategy and reskilling efforts, despite the fact that almost 70% of employees want to learn new skills and skills to remain competitive. Thus, the Future for Work Institute highlights the need to incorporate **new team management practices based on skills** as the axis for the future of work.

Even so, the existing data guide us towards an **optimistic future:** the WEF defends that technologies for such sectors as diverse as as agriculture, e-commerce, cybersecurity or robotics will be positive for the labor market over the next five years.

Thus, there are many variables that directly or indirectly affect the reconfiguration of the global workforce. As an example, the WEF argues that **economic and geopolitical trends have created divergent** outcomes in the labor markets of different geographic regions. While **high-income countries** experience **competitive labor markets, low- and middle-income countries** face an **unemployment higher** than prior to the COVID-19 pandemic, which in places like South Africa stands at more than 30%.

Additionally, Future of Skills notes the **seven megatrends** that will determine the future of work and of the human skills necessary for 2030:

Technological progress

Digitalization, automation and greater connectivity are some of the areas that are transforming the business activities of multiple organizations. According to the 2021 **Digital Leadership Report,** 60% of companies have moved their operation centers to the cloud. Moreover, data from PricewaterhouseCoopers points out that almost 40% of employees are concerned about **the risks of job elimination** due to automating processes, whereas 71% consider that technology will never be able to replace human skills. Therefore, over the next years technological progress will shape the labor market, attracting new talent within areas and cutting-edge knowledge such as cloud, computing, collaborative platforms, or data analysis.

Globalization

The increasing interdependence of markets and companies over the last decades has allowed them to cut costs, generate employment, and share knowledge and products across multiple countries. Nevertheless, in the recent years we are observing a certain setback in this regard, including protectionist discourses and the imposition of different measures such as tariffs or company reshoring back to their countries of origin. This reality is partly a brake on globalization, particularly in key sectors such as technology.
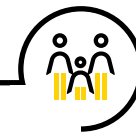
Demographics

The aging of the population and the drop of the birth rate in most Western countries is creating a generational gap with diverse behaviors regarding consumption and employability. A clear example is the Millenial and Gen Z's search for purpose, causing additional social tensions at different levels, such as the necessary investments in infrastructure, pensions or healthcare, among others. All of this may lead to the need to reorient labor markets towards countries that in the coming years or decades will experience a demographic explosion with young working-age populations, especially in Asia and Africa.

Sustainability

The effects of the climate challenge can cause severe impacts in sectors such as agriculture, tourism or energy, so that the jobs of the so-called "green economy are vulnerable to the effects of consumer behaviors and policymaking. In addition, other effects can be derived, such as (1) food insecurity, which could exacerbate structural problems like poverty; or (2) increasing conflicts, i.e., of geopolitical, economic, and social nature between various states and affecting ultimately to the global economy and to the labor market.

Urbanization

While currently it is estimated that 50% of the world population lives in large cities, by 2050 the figure is expected to reach 70%. Industrial attraction and the concentration of professional opportunities in large cities are two significant trends for the labor market, although possible changes in tax policies, climate challenges, urban violence, the necessary investment in infrastructure and public services, and the consequent public debt ratios are potential sources of conflict for the coming decades as well.

Growing disparity

The progressive difference between income and wealth constitutes one of the greatest challenges for societies, which is causing a decrease in purchasing power and a reduction in the middle class, shifting the distribution of income towards the upper and lower extremes. That said, education, public investment and political action can impact the labor market in the coming years, without ruling out possible sources of conflict such as social instability, polarization, or distrust towards governments.

Political uncertainty

Political instability can negatively affect strategic sectors of many states, especially those where political decisions have a direct impact, such as defense, construction, health or energy. Therefore, uncertainty can generate repercussions in the labor market, increasing competitiveness between countries to attract investment or reallocate resources towards companies with greater productivity.

All the above can give rise to **a multitude of future scenarios** in the matter at hand, depending on the trends outlined so far evolve and shape labor markets around the world. In this sense, PwC points out **four possible future scenarios for work in 2030:**
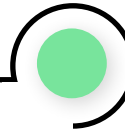
Red World

Marked by innovation, market niches and the absence of rules, companies that innovate the most and abide by agility, speed and product customization would be more likely to succeed, although this scenario presents serious organizational challenges such as the need for constant innovation and business competition to attract talent in critical skills.

Blue World

Multinational organizations and consumer choice would be the axes of the future in a highly capitalist market, so the employability and permanence of workers in companies depends on their success and relevance, in addition to there being additional threats such as business mergers or cyber-attacks.

Green World

Sustainability goes beyond words into actions, prioritizing ecological awareness in the labor market. Ethical standards favor worker loyalty towards companies with a firm green purpose, in addition to its association with work flexibility and trust between employee and employer. Therefore, the construction of brand image, communication, threat prevention and compliance may be some of the most relevant areas for companies.
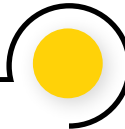
Yellow World

Employees and companies working together in favor of common well-being and social justice, so that loyalty and work commitment are not oriented towards the brand, but towards the existing shared feeling of fighting for the same cause. Ethics, transparency, and political-social action of organizations are therefore some of their top priority challenges.

01

02

03

04
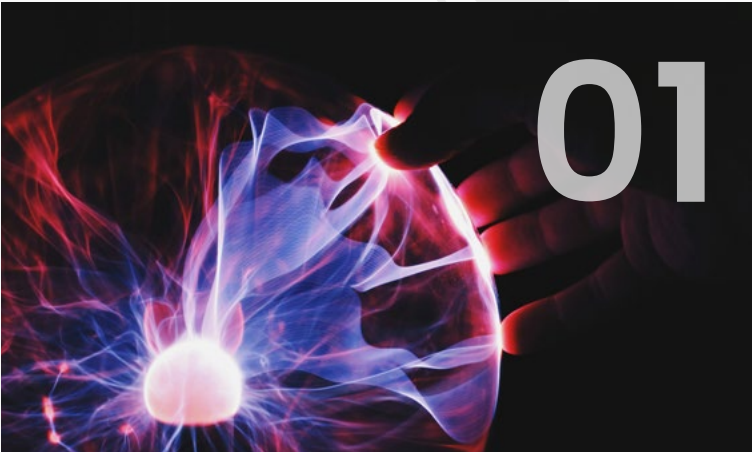
→ (B) **The skills**
for the future

For all of the above reasons, **the skills needed today are already changing rapidly: technical skills** continue to be relevant, but more purely **human skills such as communication and collaboration** are gaining in importance. Thus, interaction with new technological developments and the ability to learn new knowledge have become fundamental skills in a **constantly evolving work environment.**

According to the WEF, some of the jobs with the worst expectations for the future are related to repetitive tasks such as administrative tasks, while sustainability specialists, security analysts, business intelligence analysts or renewable energy engineers will be some of **the fastest growing in the short to medium term.**

However, social variables must be envisioned when analyzing the future labor market, since **demography as an axis of the future** shows disparate results. In this regard, some data show that the automation of jobs in countries like South Africa could lead to the **destruction of more than three million current jobs** by 2030.

Faced with this panorama, different companies and international institutions are studying the skills that will make a difference in the value of workers, who generally must compete in **stressed, saturated markets, with high competitiveness for the same position and, sometimes, with overqualification for the task to be performed.**

The WEF's Future of Jobs Report 2023 highlights a range of skills needed for Wef highlights a series of necessary skills and which will mark a competitive differential value in the worker over the coming years:

Graphic 3
Top 10 professional skills for the future according to WEF:

1. Analytical thinking
2. Creative thinking
3. Resilience, flexibility & agility
4. Motivation & self-awareness
5. Curiosity & lifelong learning
6. Technological literacy
7. Attention to details
8. Empathy & active listening
9. Leadership & social influence
10. Quality Control

- Cognitive skills
- Self-efficiency
- Management skills
- Tech skills
- Social skills

Source: Prosegur Research, 2024 based on *WEF*

Besides, the Organization for Economic Cooperation and Development (OECD) points out that there are *three groups of essential skills for work in the future:*

Ⓐ

Cognitive & meta-cognitive skills, which involve mental processes such as arithmetic, linguistic, knowledge, verbal, and non-verbal abilities. The latter also implies creativity and critical thinking.

Ⓑ

Social & emotional skills, which allow for certain behaviors and emotions to arise and cultivate relationships with others, such as empathy and collaboration.

Ⓒ

Practical & physical skills, which relate to the ability to operate with tools and operations such as information and communication technologies.

02

The skills of
security experts
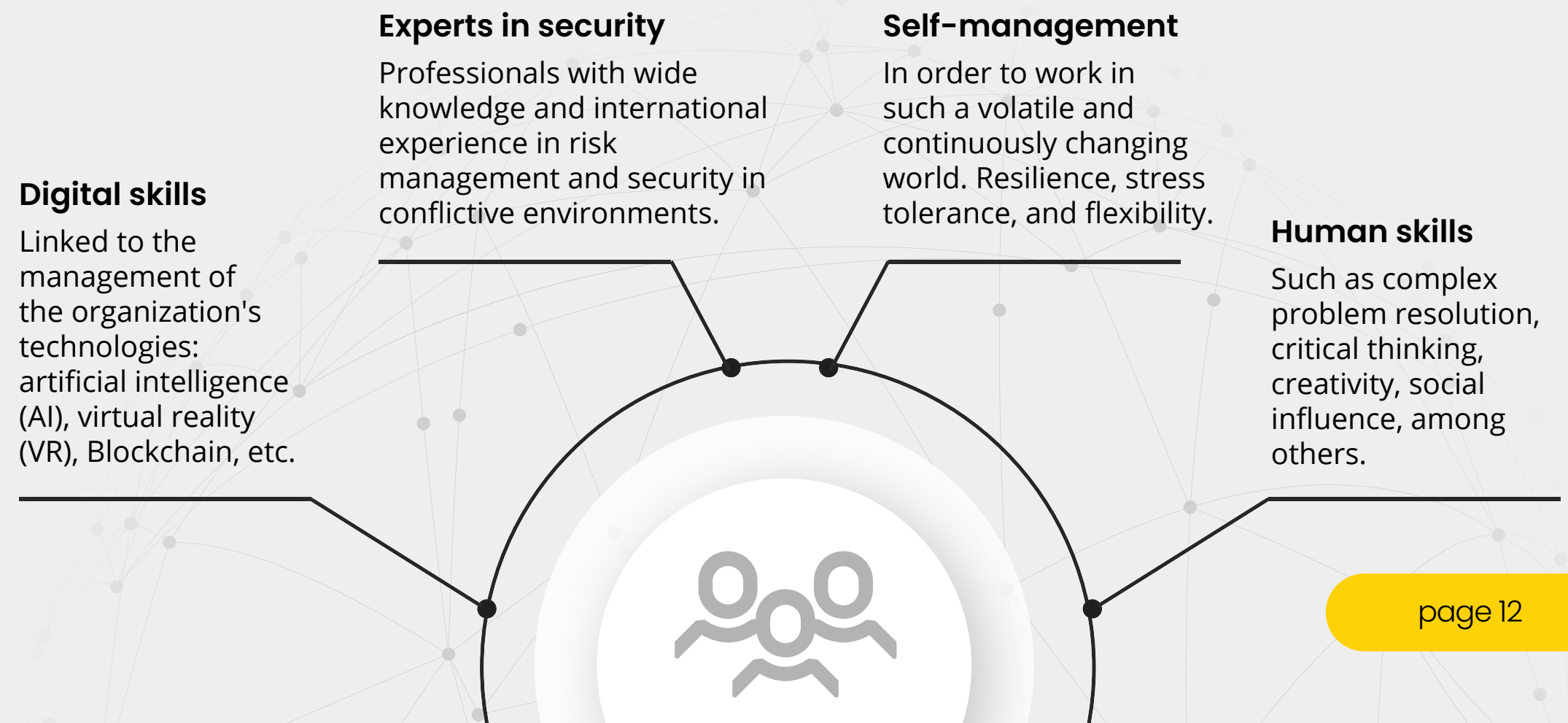
02

THE SKILLS OF SECURITY EXPERTS

At Prosegur Research, we understand that the **hybrid world** in which we live requires different skills: we cannot live in the present with the tools of the past. Human skills are absolutely fundamental and irreplaceable, so we must **seek to empower workers by enhancing their skills through the lever of change that is technology.**

The key lies in the alignment between human resources, equipped with knowledge and experience, with the appropriate technological means, with the aim of adapting to constant changes in the environment. In the words of Xavier Marcet, machines can synchronize, but they cannot sense complicity. Nowadays, it is necessary to

build complicity in corporate environments that do not cancel the empathy, patience, respect, or generosity that characterizes teams of people who work in harmony and for a shared objective.

Thus, **at Prosegur Research we believe that there are four main categories of skills, knowledge, aptitudes,** and attitudes that best prepare the worker for the changes in the labor market that are approaching in the future and that best show **the pillars of the so-called hybrid security:**

Experts in security

Professionals with wide knowledge and international experience in risk management and security in conflictive environments.

Self-management

In order to work in such a volatile and continuously changing world. Resilience, stress tolerance, and flexibility.

Digital skills

Linked to the management of the organization's technologies: artificial intelligence (AI), virtual reality (VR), Blockchain, etc.

Human skills

Such as complex problem resolution, critical thinking, creativity, social influence, among others.

1 Security **skills**

The constant volatility of financial markets, geopolitics or social instability in many countries are some of the variables that daily affect the business continuity of organizations, regardless of the sector to which they belong. These factors can lead to large economic losses or serious damages to the brand image. Therefore, professionals with extensive knowledge and experience in risk management and security are required. As such, professionals with extensive knowledge and experience in risk management and security are required who adapt what happens to the business framework in which they operate, understand the transversality of the processes and analyse the changing reality with a systemic vision, covering issues such as the following:

Political component
This involves all aspects related to political decisions and geopolitics that can directly or indirectly affect the economic expectations of a company, as well as its image or reputation, with the possibility of decreasing its value. In this way, regulatory uncertainty, current legal frameworks, disinformation or interstate conflicts should be a matter of special interest for any security expert.

Economic component
The economy influences all daily decisions of any company, so economic risk, understood as the possibility of generating monetary or investment losses that hinder compliance with the company's strategic line, must be present in any risk analysis. These analyses must tackle key matters such as inflation, asset prices, fiscal deficit, economic interdependence, or disruptions in the supply chain.

Social component
It is linked to the possibility of generating climates of discontent, polarization, uncertainty or conflict on the part of citizens or civil groups.

In this way, social activism, polarization, demonstrations, and labor conflicts can directly impact the assets, reputation, and brand image of organizations.

Environmental component
Companies are not independent from the physical environment in which they operate. Therefore, experts must consider those variables with the possibility of direct and indirect impact on infrastructure, workers, or business activity itself, along with expanded diseases, pandemics, workplace accidents or extreme weather events.

Physical security component
Physical threats should never be underestimated, as they can cause damage to the organization's tangible or intangible assets. For this reason, expertise on common crime in the territory where the company operates, on the impacts of organized crime, vandalism, intrusion, scams, kidnappings, assaults, and on the consequences of possible terrorist attacks are elements of crucial relevance for any risk analysis.

2 Digital **skills**

Related to the management of technologies in the organization, these skills are essential to correctly perform professional works. In fact, according to Qlik and The Future Labs, **data literacy** will be the most in-demand skill for workers in 2030. Therefore, workers need to know the applications of **the most cutting-edge and disruptive developments,** such as virtual immersion technologies, artificial intelligence, quantum computing, blockchain, robotics or the Internet of Things, among others.

Digital component
Translating human behaviour into the digital realm entails understanding the differences and similarities, and understanding the impact of the changing digital environment on all areas of business, especially security. The incorrect and/or malicious use of technologies can lead to disruptions in business activity or potential vulnerabilities in infrastructures. Therefore, knowledge of variables such as digitalisation, industrial espionage, cyber-attacks, criminal applications of robotics or drones, the applications of artificial intelligence in identity theft or the risks in the encryption of information due to advances in quantum computing is vital to guarantee the correct performance of any company.

Technological component
Technical changes continue, and keeping up with the most **innovative technologies** inevitably requires so-called 'hard' skills and competences. Understanding not only the use, but also the design and implementation of technologies is becoming increasingly important for security experts: established technologies such as the Internet of Things, cloud, robotics and artificial intelligence, expanding technologies such as biometrics, blockchain, augmented reality and 5G, as well as potential disruptive technologies such as 3D printers, mixed realities and quantum computing will all shape the future of security, which will undoubtedly have an important technological component.

3

Human skills

To perform jobs in changing environments and multifunctional jobs, we must make use of purely human capabilities that can become the differential value in a worker:

Analytical and integrative thinking

Hybrid challenges require employees to have the ability to analyze the environment in an agile way and decompose problems into various parts. Supported by the latest technology, they must identify innovative solutions adapted to the needs of each client and situation.

Complex problem solving

Solving problems for which there is still no solution is something intrinsically human. Experts empowered by technology do it every day to address the complex reality and confront hybrid challenges that require unique solutions.

Critical and innovative thinking

Hybrid security professionals analyze information from any channel with fairness, honesty, and objectivity to ensure the best protection of people, assets, and businesses.

Creativity and generation of ideas

Technology is the great ally of security experts when we apply human creativity to develop innovative processes. Identifying new formulas to improve our response to incidents and enhancing service efficiency while maintaining the highest level of security are constant initiatives in this competitive alliance.

Empathy

Experts recognize the needs of companies and individuals because they put themselves in their shoes and thanks to that they manage to identify the appropriate security solutions for each physical or digital environment in which they operate.

4 Self-management **skills**

Self-management and leadership skills are necessary in the turbulent environment around us. The world requires adaptation, flexibility, frustration management and, ultimately, resilience to transform challenges into opportunities:

Leadership and teamwork
The best hybrid security experts lead teams and generate social influence on people to be able to absorb all the technological potential at their disposal. Responding in a joint and coordinated manner by all the actors and tools involved in each service is essential to offer comprehensive security in hybrid environments.

Flexibility and resilience
In security, experts learn to work under pressure, manage their emotions and adapt to constant changes in the environment. Therefore, agile mental models are essential to learn from each new technological advance and make it available to customers.

Active learning and learning strategies
Disruption is constant in current hybrid environments. Therefore, security experts are constantly learning and adopt different learning strategies depending on the context, applying the relevant digital tools in each situation.

03

Hybrid security
professionals

03

HYBRID SECURITY PROFESSIONALS

The contribution of people in terms of **understanding the context and their ability to innovate** are key aspects from a strategic perspective, especially in a world of increasing complexity like the current one, and specially in a **context of expanding security** that will undoubtedly demand new skills, specifically **within the sector.**

> 66 We are moving towards a world where traditional risks not only persist but grow along with an additional complexity. Threats arise from increasingly unexpected and diffuse sources, and so the concept of Security is expanded to include other issues not previously considered.

Fernando Abós, CEO of Prosegur Security

Although technology plays a crucial role in today's world and even if data are strategic for an adequate service, the truth is that the **human factor is essential for success.** Skills such as critical and creative thinking, as well as adaptability, are essential. Both technical knowledge and human skills are fundamental. A company with cutting-edge technology but missing trained security personnel will not cope with today's rapid changes and risks accordingly. **People are, ultimately, the central axis of hybrid security,** those who conduct the tasks, make the decisions and, on a daily basis, they are the most responsible for the services.

Let us remember the inspiring words of **Lieutenant General Gan** on how to choose a candidate for an expedition to the North Pole: accept our mistakes without looking for other culprits, accept the mistakes of others without resentment, and be able to join other people to change the world. If we look closely, all these criteria refer to the way of working, giving extraordinary weight to social skills. In the world

of security, this becomes even more critical, since **teamwork is essential** when responding to incidents with a multitude of people involved in the services:

security guards, analysts, operators, etc. Let's have a look at the role of some of them.

CONNECTED SECURITY GUARD

In the current yet complex context, marked by unpredictability and the convergence of threats, it is essential to adopt a systemic approach in the provision of surveillance services. In this way, the security guard, by being connected to a Security Operations Center (iSOC), sees his response skills strengthened through access to a wide variety of data and technologies, which allows constant feedback on the flow of information between all parties involved.

Main functions

- Surveillance and patrolling, both static and dynamic.
- Protection and/or transportation of goods.
- Response to emergencies or alarm signals.
- Filing of complaints against illegal acts.
- Real-time data collection.
- Support in search and rescue efforts for missing people.

- Detection of prohibited substances or dangerous objects.
- Access & identity control.
- Management of masses and flows of people.
- Collaboration with state security forces and bodies.

Empowering technologies

- Incident recording and management software.
- Communication: smartphones and devices such as two-way radios.
- Video management and remote access to cameras.
- Personal safety devices.
- Intrusion detection: alarms, scanning & sensors.
- Biometric, video surveillance & GPS technology.

Featured skills

- Security competencies: prevention & risk analysis.
- Technological skills: use of surveillance and communication systems for security.
- Human competencies: communication, empathy & situational awareness.
- Self-management skills: flexibility & resilience.
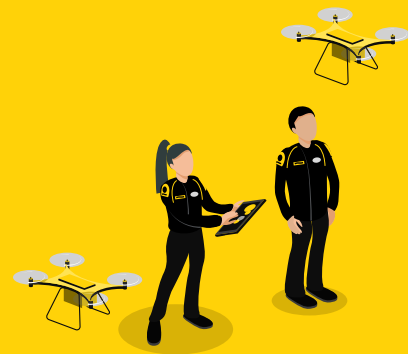
DRONE OPERATOR

An operator or guard empowered by drone technology enhances operational efficiency allowing them to cover more ground or surface in shorter periods of time. Additionally, increasing response capacity and surveillance scope provides competitive differentiation in business terms, and ultimately improving the company's reputation.

Main functions

- Air surveillance & patrol (sports and industrial facilities, events, etc.).
- Perimeter surveillance in areas with difficult access, both static and dynamic.
- Emergency response.
- Real-time data collection.
- Support in search and rescue efforts for missing people.
- Surveillance of critical and sensitive infrastructures.

- Automation of surveillance patrols.
- Environmental protection such as forest fires.
- Detection of anomalies through the use of sensors (thermal, pressure, etc.).

Empowering technologies

- Platforms for management of drone operations from control centers.
- Coordination of Operations between control center and Pilot.
- Planning of recurring flights.
- Implementation of AI layer.
- Monitoring and recording of streaming video from SOCs.
- Control of flight hours of pilots and drones.
- Tools for controlling technical signals, maintenance & incident management.

Featured skills

- Security competencies: knowledge of drone regulations and aerial surveillance capacities.
- Technological competencies: experience in drone operation and maintenance.
- Human competencies: analytical thinking and situational awareness.
- Self-management skills: flexibility and active learning.

iSOC OPERATOR

The operator of an iSOC, often known as digital guard or TIER 1, is a crucial component to the effective functioning of security operations. Their work extends to real-time monitoring of indicators and behaviors, as well as the coordination of responses to incidents. These operators are usually the first line of reaction in security situations.

Rapid evolution in the security ecosystem means constant changes in security incidents, along with the creation of new methods to commit establishment thefts. Additionally, technological development requires iSOC operators to actively acquire new skills in security and technology.

Main functions

- Real-time monitoring of events, behaviors & security signals.
- Initial triage of security-related incidents.
- Immediate response to basic security-related functions and incidents.

- Communication with specialized teams or security guards on the ground.

Empowering technologies

- Platforms for the management and storage of visual content.
- Use of advanced visual analysis algorithms and artificial intelligence techniques to understand and extract information from videos.
- Systems for the coordination and efficient management of problematic situations.
- Tools and systems designed to identify and prevent unauthorized access or malicious activities.
- Technologies to ensure regulatory compliance and manage over possible vulnerabilities in systems and networks.

Featured skills

With the aim of guaranteeing correct analytical thinking before each event that may occur to equally guarantee business continuity.

- Security competencies: knowledge and capacity in cybersecurity and risk analysis.
- Technological competencies: knowledge and capacity in cybersecurity.
- Human competencies: communication and analytical thinking.
- Self-management skills: teamwork and active learning.

DATA ANALYST

In the current data era, the data analyst is configured as a fundamental role for the correct operation of any large company, since through advanced collection and analysis techniques, large sets of data are explored and evaluated with the aim of advancing in the data marathon and the knowledge chain –the one in which data is transformed into information, which results in knowledge to give rise to intelligence–.

Main functions

- Analysis of data and indicators to identify trends and patterns of (in)security.
- Compilation and integration of information from various channels.
- Design, cleaning, preprocessing and data modeling for the creation of databases and dashboards.
- Identification of patterns, trends and correlations between large volumes of information through data analysis and data mining techniques.

- Development of predictive models based on quantitative data and historical data.
- Identification of indicators of compromise (IoC).
- Optimization of corporate resources and processes.

Empowering technologies

- Use of various programming languages to analyze and consult data in relational and non-relational bases.
- Implementation of technologies to process and large volumes of data by means of algorithms and algorithms and machine learning.
- Information storage in systems adapted to manage flexible data structures.
- Visual representation of data using specialized tools.
- Automation of processes and work sequences to improve operational efficiency.
- Systems integration and data transformation to guarantee interoperability between different platforms and formats.

Featured skills

- Security competencies: risk analysis & privacy.
- Technological skills: mastery of tools, databases, analysis & visualization.
- Human skills: critical thinking.
- Self-management skills: active learning.

INNOVATION ENGINEER

The constant evolution and technological convergence results in the need to maintain flows of innovation in security services for each client, with hyper-personalized measures adapted to each need in this matter. An innovation engineer, with cross-departmental expertise, provides a holistic view of the business landscape, being able to anticipate various trends and ride the crest of the wave of progress, thus promoting a culture of innovation that makes a difference from the main competitors.

Main functions

- Collaboration and development of innovative lines of security products.
- Identification of business opportunities.
- Search for external collaborations and/or financing alternatives.
- Management of internal and external communication.
- Internal training on new products.
- Initial go-to-market strategy.
- Research and analysis of market trends and technological lines.

- Implementation of improvements in the organization's operations.
- Technical, product and business validation of new solutions.
- Technical advice on innovation.
- Promotion of business culture based on technological progress.

Empowering technologies

- Use of communication technologies and tools to facilitate interaction and collaboration between teams.
- Implementation of AI and computer vision systems to perform advanced analysis and recognition tasks.
- Application of robotics and drone technologies for the development and control of autonomous devices.
- Use of sensors and data acquisition platforms to collect information from the environment.
- Implementation of video surveillance and biometric systems for user security and authentication.
- Integration of GPS and augmented reality technologies to improve location and user experience.

Featured skills

- Security skills: knowledge and capabilities for risk management and emerging threats.
- Technological skills: knowledge on emerging developments and market trends.
- Human skills: curiosity and learning capacity. Empathy and resilience. Communication and persuasion skills, vision, leadership and team empowerment.
- Self-management skills: leadership and active learning.

INTELLIGENCE ANALYST

The intelligence analyst adds value to the entire business chain, since their function, following the classic cycle of intelligence, is linked to the collection of information, its analysis, and its evaluation. All steps combined to finally produce actionable intelligence, i.e., information that facilitates decision-making. The intelligence analyst is characterized by the ability to anticipate threats and events that may impact different levels of an organization (people, assets, assets, infrastructure, reputation, business continuity). For an intelligence analyst, especially in the fields of security, organized crime, terrorism or risk analysis, it is crucial to have a variety of tools and software that allow them to collect, analyze, and present data and information effectively and securely.

Main functions

- Analysis of data and indicators to identify trends and patterns of (in)security.
- Compilation and integration of information from various sources.
- Update or maintenance of databases and dashboards available to the client.
- Preparation of reports and presentations that support business decision-making.
- Collaboration with incident response teams.

Empowering technologies

- Data collection and extraction: use of various open sources and web scraping techniques to obtain relevant information.
- Data analysis and visualization: highlighting analysis, big data and handling statistical analysis packages through AI and machine learning.
- Cyber-intelligence tools: use of software specialized in digital forensic analysis and penetration testing to protect systems and networks.
- Management and analysis of geospatial information: use of tools to work with spatial data, cartography, and satellite images.
- Social network monitoring and community analysis: social listening (SL) and social network analysis (SNA) tools and software.
- Collaboration and project management: use of platforms to organize and communicate effectively in projects and tasks.

Featured skills

- Security competencies: analyses of risks, threats & vulnerabilities.
- Technological skills: mastery of data analysis tools and diverse sources of information.
- Human skills: critical thinking & creativity.
- Self-management skills: teamwork, active learning & flexibility.

page 25

PRESALE & COMMERCIAL

The strategic value of a pre-sales and commercial technician for hybrid security lies in their ability to maintain a systemic vision of the organization and the needs of each client, generating relationships of trust and supporting the strategic line of the corporation. Thus, both to maintain the company's operations and to promote long-term improvements, their work is essential.

Main functions

- Adapt security services to the needs of each client.
- Support in the company's strategic line.
- Research and analysis of market trends.
- Analysis of needs and/or improvements in security processes and services.
- Implement improvements in the organization's operations.
- Identification of business opportunities.
- Generation of income and development of trust-driven relationships with stakeholders.
- Participation in negotiations and tenders.

Empowering technologies

- Customer management platforms (CRM) to manage and organize interactions with customers, as well as to manage information related to sales and marketing.
- Test environments & simulations to demonstrate and test systems in a controlled environment before implementing changes or launching products to the market.
- Tools for the creation and presentation of technical documents.
- Systems to manage relationships, collaboration & communication, as they facilitate interaction and collaboration between internal and external teams.
- Resources to obtain sales intelligence and competitive analysis.

Featured skills

- Security competencies: awareness of new products and services in the sector.
- Technological skills: experience with project and client management tools.
- Human skills: negotiation, communication & empathy.
- Self-management skills: leadership & resilience.

When we talk about people in hybrid security, we are not talking about a group or a job, but about **teams of experts with different skills that are integrated** to leverage the human factor in a cohesive way with technologies and data.

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

04

Leading innovation
from experience

LEADING INNOVATION FROM EXPERIENCE

At Prosegur Research we know that it is teams of experts who lead companies to success, in their firm commitment to the purpose of what they do.

People are the driving force of the world. They transform lives and businesses, they make good or bad use of technology and data, and they are the ones who truly generate improvements in the efficiency and effectiveness of all types of services.

On the road to innovative leadership, **the human factor** must be at the centre of the entire organisation because it is what provides the **mindset or growth mentality,** from which to evolve towards forms and processes with greater agility, efficiency and sustainability. A company will only be as innovative as its employees as a whole, and like a system that feeds back on itself, as Meadows said, **organisations with a purpose and culture of innovation will attract the most talented,** creative and teamwork-minded people.

From the hybrid security model, purpose and culture align its three essential elements: people, technology and data. Technology being the great lever of change, it is the human factor that makes the most of technologies and data in a constantly evolving environment. Moreover, the contribution of experts extends beyond this, bringing **contextual intelligence and innovative capacity** to the organisation's entire value chain.

Hybrid security is made up of **people empowered** by the most innovative **technology** that allows them to make strategic use of **data.**

For this reason, **hybrid security considers people as a priority,** so that attracting and retaining talent are essential commitments. These can be materialised in a wide range of actions for its employees, such as **continuous and specific training programmes, diversity** and **empowerment** initiatives or the promotion of good internal communication, as well as prioritising its activities based on **humanist pillars.**

Prosegur, as a leading global security company present on five continents, has more than 170,000 employees who **are committed every day to making the world a safer place,** positioning Prosegur as **the second largest employer** in Spain. To this end, as an international company, it **reinvests more than 70% of its gross profit in people,** mainly in the remuneration of human talent, which is the key to its innovative leadership.

Investing in long-term leadership with a humanistic vision is what makes it possible to achieve success with the best professionals, which is only the starting point for the following future challenges that we will face together.

PROSEGUR
SECURITY

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