PROSEGUR RESEARCH

Crime on business brief

The global context of **occupational fraud**

2023

PROSEGUR

HOME

INDEX

01

A major **occupational threat**

HOME

01 A major occupational threat

02 An analytical perspective on occupational fraud

03 A strategic vision on the phenomenon

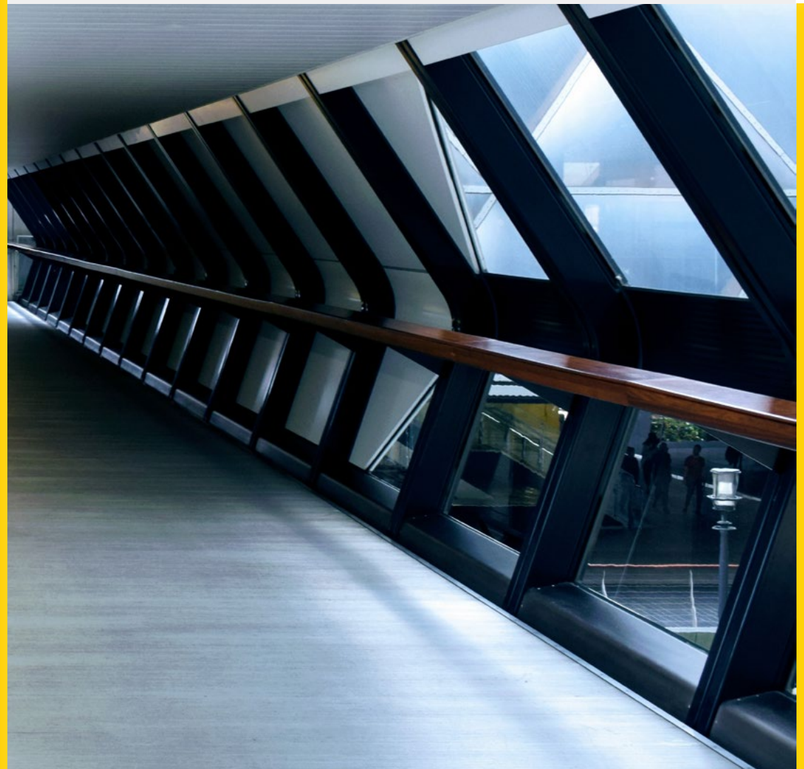
04 Trends in occupational fraud

01 A MAJOR OCCUPATIONAL THREAT

Public and private organizations face several challenges and risks to the security and business continuity, with a multitude of edges and impacts. In this regard, **occupational fraud constitutes one of the main criminal or illicit acts** with the greatest reputational, social, governance and economic impact for organizations.

Thus, this Prosegur Research report is part of a series of **studies** on **security culture,** which delves into the criminal phenomena committed within companies; in this instance, complex dynamics and the diverse contexts in which fraud crimes are committed in the **corporate environment are analyzed and assessed.**

When facing this challenge, companies must consider that there is **no known or unique solution to this problem.** Therefore, all the appropriate human and technological resources must be employed, based on an understanding of the phenomenon and with a strategic vision capable of inhibiting undesirable behaviors within the company and that, in the worst-case scenario, minimizes its impact.



At Prosegur Research, we understand *occupational fraud* as **the intentional and deliberate act** conducted by personnel within the company or third parties with **access** to the organization, for **personal financial gain and/or cause other harm of various kinds.** Actions include tampering with or falsifying records, misappropriation of assets, data leakage, or any actions that ultimately affect economic, operational and reputational stability, such as misappropriation.

Occupational threats, originated from within the company, entail great economic and information losses for the entities affected by their impact. In addition to disrupting the company's economic activity, the consequences of such threats have repercussions on its public image and reputation. However, **these events must be distinguished from external frauds,** since the latter are committed by parties external to the organization. Thus, the **ISO/CD 37003 standard,** which is currently under development, would establish that an occupational fraud must involve at least one perpetrator directly connected to the target organization.

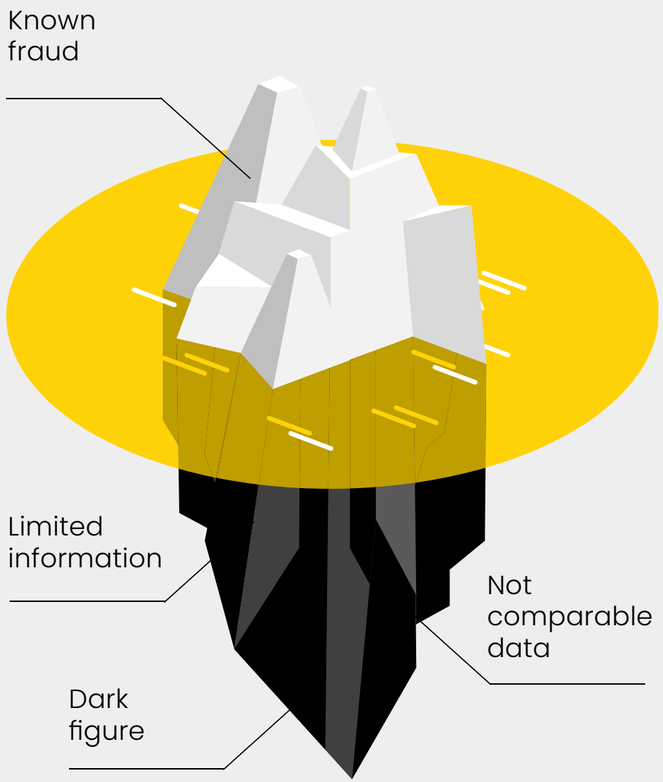
Fraud in the corporate realm exhibits a multitude of features that contribute to its intricate and complex nature, since there is **no availability of information on its incidence, which hinders the difficulties in measuring the scale and the classification of the threats, due to the underreporting of these acts** by companies. For example, according to IBM, it takes an average of **197 days to detect a data breach and up to 77 days to recover from it.** For this reason, it is a phenomenon with **a significant "dark figure"** and the existing data published in studies and reports are **scarce and hardly comparable with each other,** due to being based on case studies, which makes it difficult to create prevention and mitigation plans.

Thus, occupational fraud requires a deep **qualitative analysis and reflection** in order to **understand its drivers, trends** and, to the fullest extent possible, **anticipate its impacts and respond accordingly.**

In the given context, one of the main actors with the greatest potential impact on organizations is the so-called **insider,** i.e., a member of the company or an external a member of the company or an external worker who has or has had access to the entity by providing a service for it and uses it to carry out **voluntary and consciously actions to obtain personal benefit,** usually of an economic nature or of revenge and resentment towards the corporation.

HOME

Graph 1
The iceberg of occupational fraud



Source: Prosegur Research, 2023

No organization, regardless of its size or sector, is immune to this phenomenon, which can occur in a wide variety of circumstances and be caused by a variety of factors.

Ultimately, we must not forget that in charge of each business, whether in the workplace, on the management committee or on the street, there is a person: to understand their motivations and, above all, their demotivations, alongside with the working and organizational environment in which they function would let us generate an adequate **security culture** to eradicate, or at leat detect and mitigate, this hidden phenomenon and its important impacts.

HOME

02

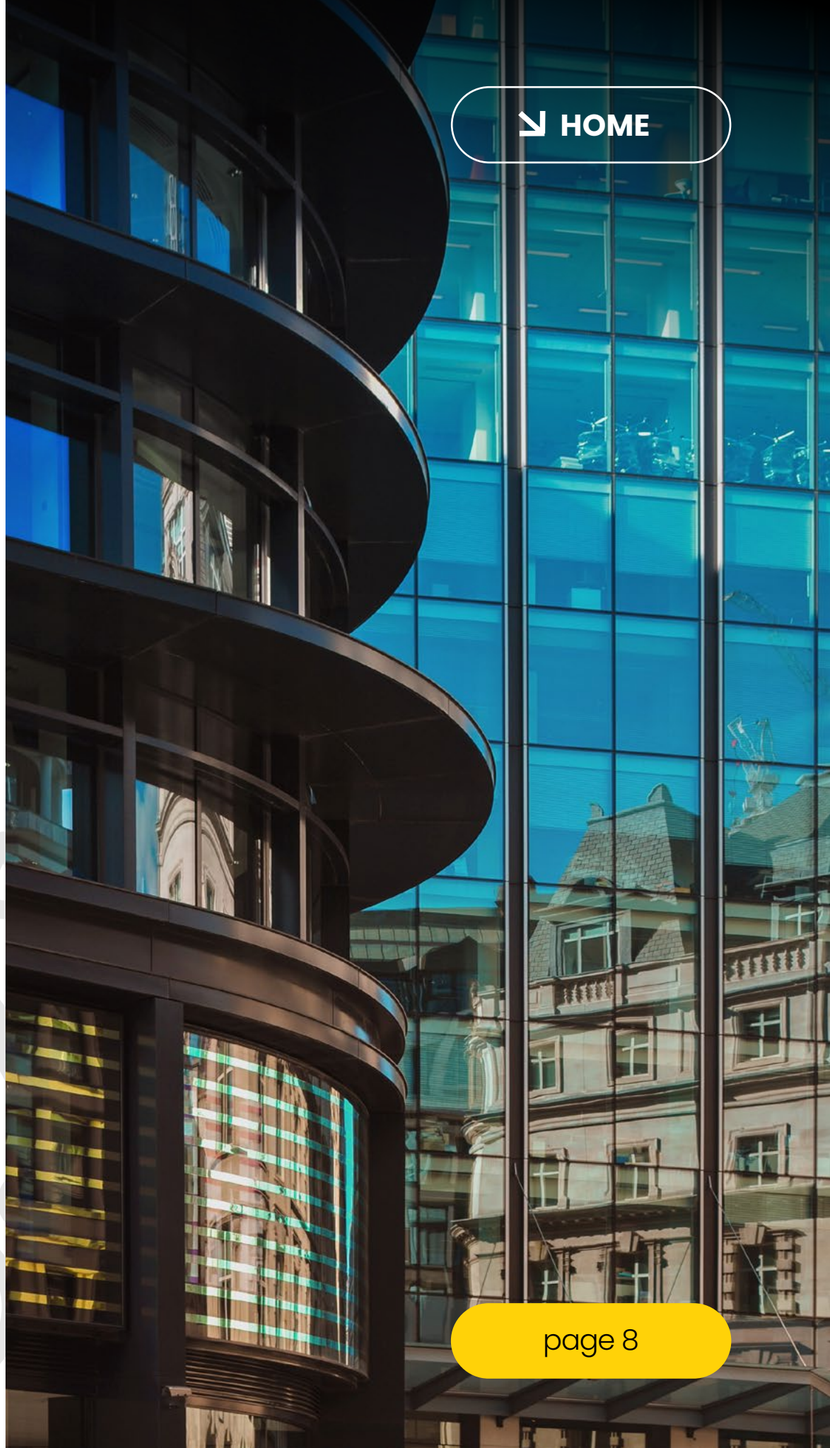
An analytical perspective on occupational fraud

02 AN ANALYTICAL PERSPECTIVE ON OCCUPATIONAL FRAUD

2.1 General explanatory models of fraud

The sector to which the company belongs, even considering that many companies are multi-sectoral, strongly influences the modus operandi and impacts of occupational fraud in each business. For this reason, **general explanatory models of occupational fraud cannot be applied to every industry and every type of company, so the characteristics of the phenomenon must be sought through a more strategic reflection.** As an example, fraud threats within the banking sector, for example, oriented mostly towards tax engineering or tax evasion, differ to a large extent from the retail or service sector, which are oriented towards theft, loss or billing fraud, among others.

Moreover, as noted above, **the impact of occupational fraud is not only limited to economic losses,** but can also affect reputation, stakeholder trust and stock quotation, access to tenders or the capacity to establish relationships with suppliers.



HOME

According to the well-known ***Fraud Tree*** by the Association of Certified Fraud Examiners (ACFE), there are three primary typologies of occupational fraud.

Asset misappropriation

This is the dimension with the most direct relationship to physical security, so it may be the most visible aspect of occupational fraud, since it as it includes offenses, such as shoplifting, false sales of stock, the theft of materials or the creation of false invoices for misappropriation.

- **Theft**
- **False stock sales**
- **Stolen materials**
- **Creation of false invoices**

Manipulation of financial data

It relates to financial assets, fraudulent accounts and tax evasion, including acts such as improper valuation of assets or fictitious income, among others.

- **Inappropriate valuation of assets**
- **Fictitious income**

Corruption related practices

Includes all those acts in which corruption has a direct influence, such as economic extortion, bribery, kickbacks or conflicts of interest.

- **Economic extortion**
- **Bribery**
- **Commissions**
- **Conflicts of interest**

Source: Prosegur Research, 2023 based on ACFE

According to the latest ***Occupational Fraud Report 2022,*** practices related to **corruption** and **asset misappropriation** are the **most common types of fraud globally** and they are often found in conjunction with each other. In this regard, there is no industry without fraud, as any company can be a victim of these crimes.

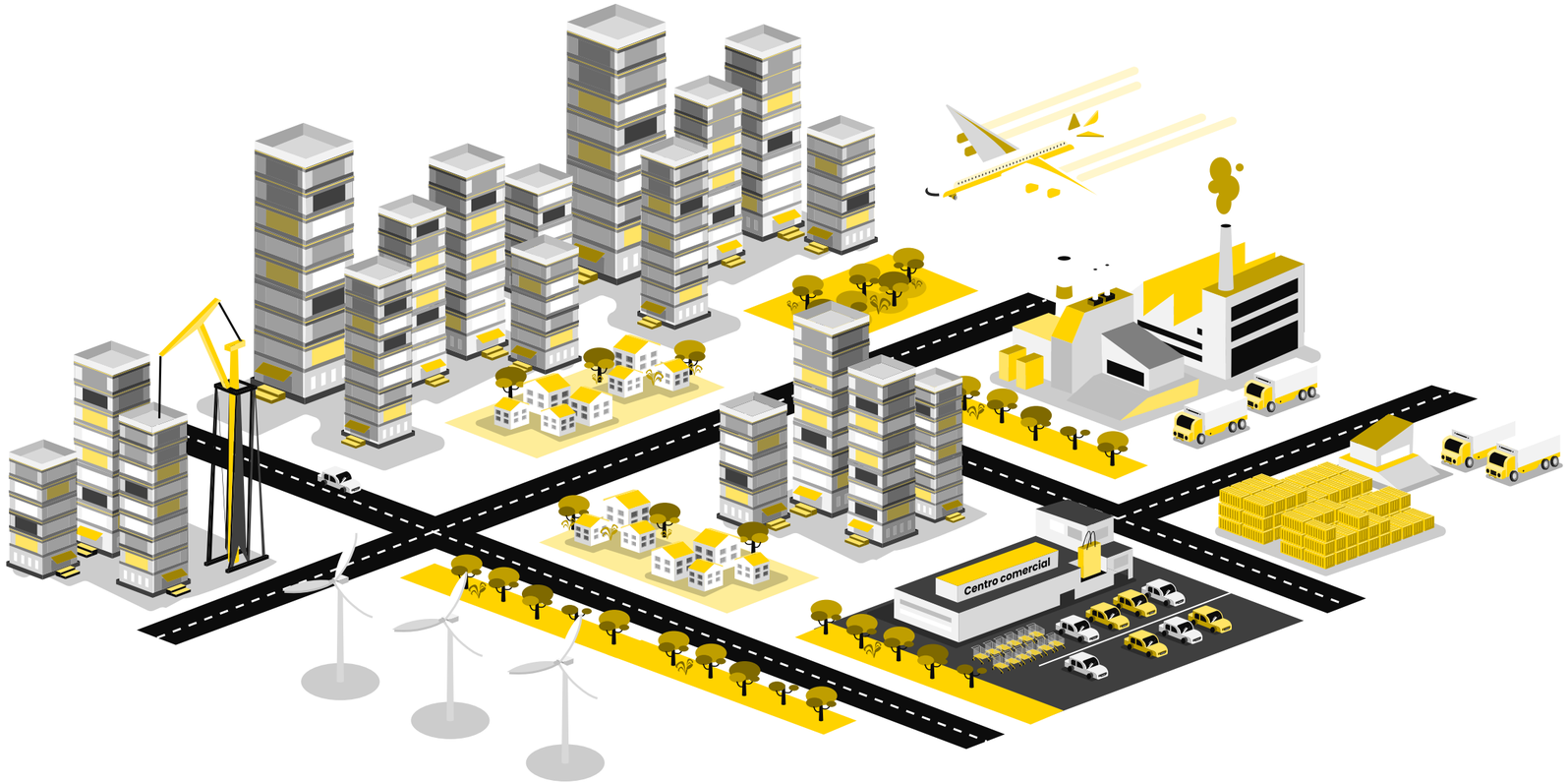
Addressing the explanation and motivations of a person to commit occupational fraud is complex. Over the last few decades, attempts have been made to explain this phenomenon, thinking about the necessary knowledge to be able to face it with guarantees and rigorousness. Among **the main explanatory models** are the fraud triangle and the fraud diamond, described below.

Graph 2
There is no sector without occupational fraud

Source: Prosegur Research, 2023

HOME

Banking and finance | Industry | Transport | Logistics



Real Estate | Energy | Retail | Technology

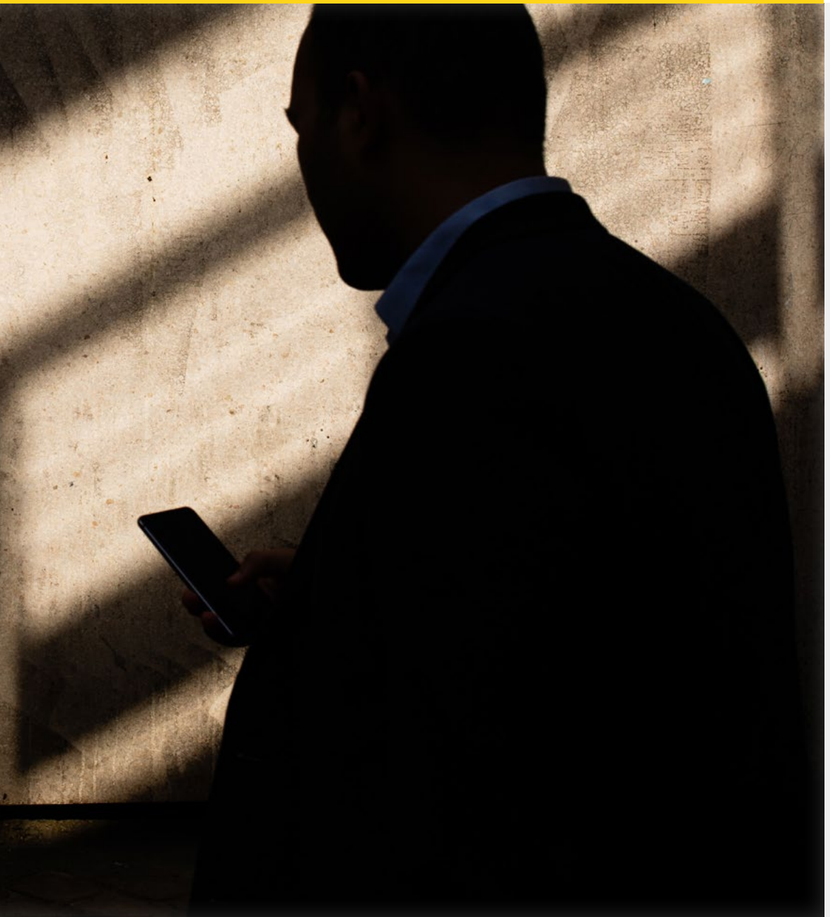
HOME

From one perspective, the **fraud triangle** is based on a model proposed by Cressey in 1972, based on ***three fundamental components to commit occupational fraud:***

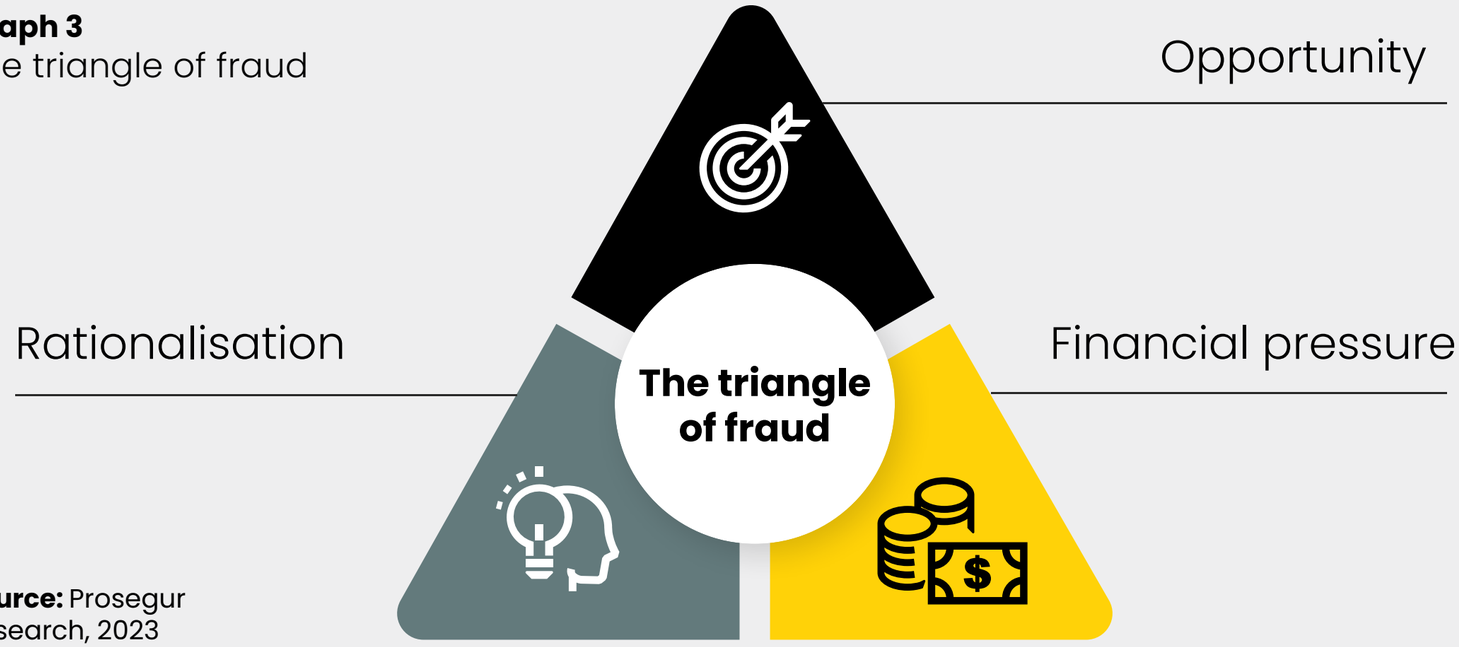
Opportunity
In order to carry out one of these actions, different circumstances must occur, such as the possibility of doing so or the absence of controls, which facilitates the perpetration of the criminal act.

Financial pressure
Also referred to as "motivation", this refers to the reason for committing the fraud, usually of a financial nature.

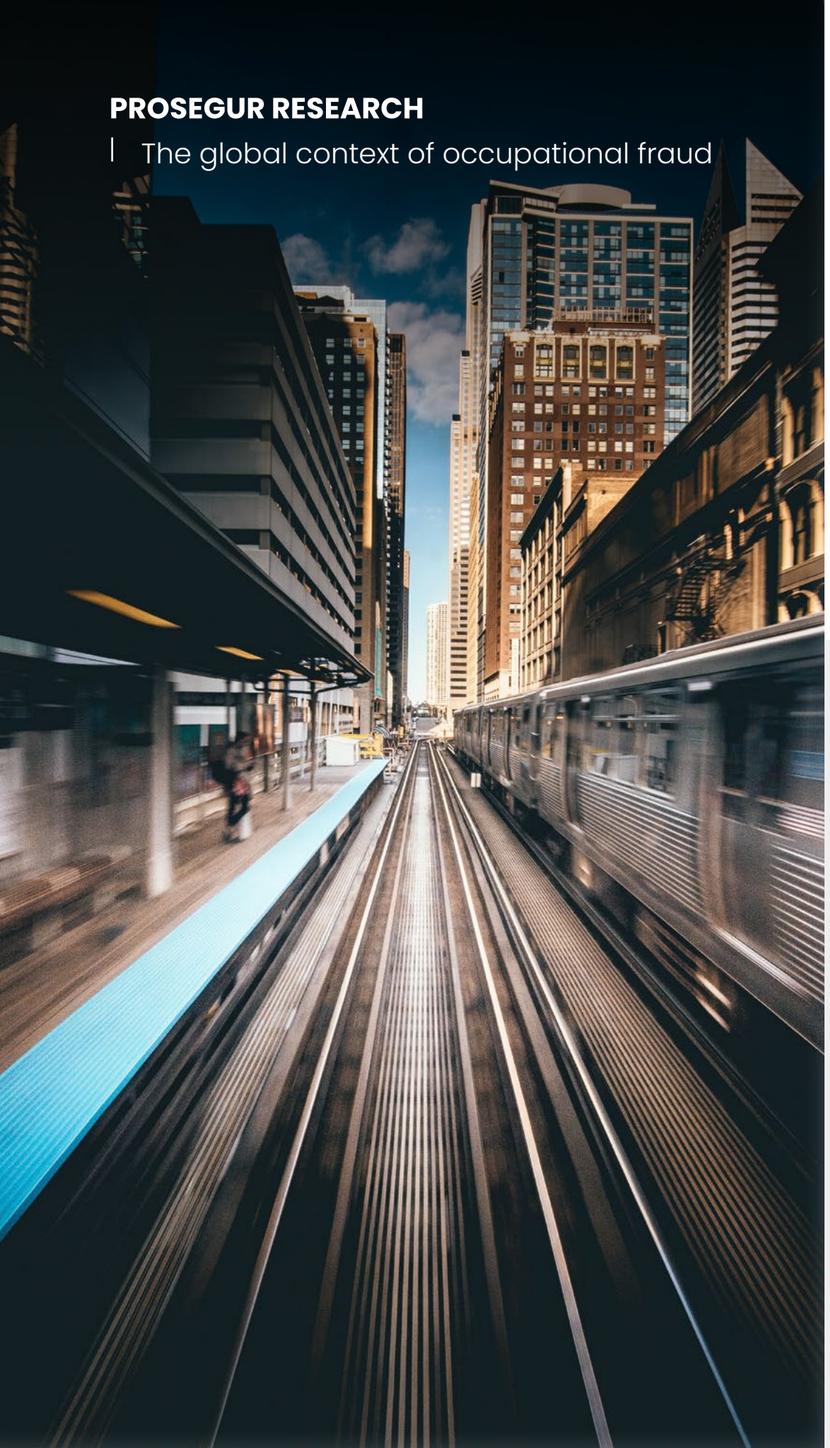
Rationalisation
The employee who commits an occupational fraud attempts to self-convince himself that the act is justified, relating to emotional and subjective aspects such as anger towards the company, apparent impunity or the perception of an inadequate salary.



Graph 3
The triangle of fraud



Source: Prosegur Research, 2023



HOME

Some criticisms of this model have led to the creation of the well-known **"fraud diamond",** which, in addition to the three elements above, includes a fourth: the **ability** to carry out the occupational fraud, i.e., the availability of knowledge and resources to do so. Furthermore, financial pressure extends to a wider range of motivations and incentives.

The absence or weakness of internal controls, lack of direction and oversight, the desire for financial gain, personal hardships or the feeling of being undervalued in the company are some of the main drivers of occupational fraud in organizations, according to a few studies, such as those carried out by **KPMG.**

Likewise, from the World Compliance Association (WCA) it has also been argued that other factors, such as **job rotation, non-segregation of duties,** or **low salaries** can lead a person who is dissatisfied with his or her job to commit occupational fraud.

Graph 4
The diamond of fraud

Source: Prosegur Research, 2023

HOME

2.2 Prosegur Research's view on occupational fraud

From Prosegur Research standpoint, the context analysis, a **contextual intelligence,** is necessary to complete the vision of occupational fraud, given that it is not a phenomenon that occurs exclusively as the decision of an employee apart from a much broader and much more dynamic context, such as global trends and internal business dynamics. Thus, all criminal phenomena develop in each **temporal and spatial context,** but it is always susceptible of being affected by a **multitude** of contextual political, social, economic or technological **variables.**

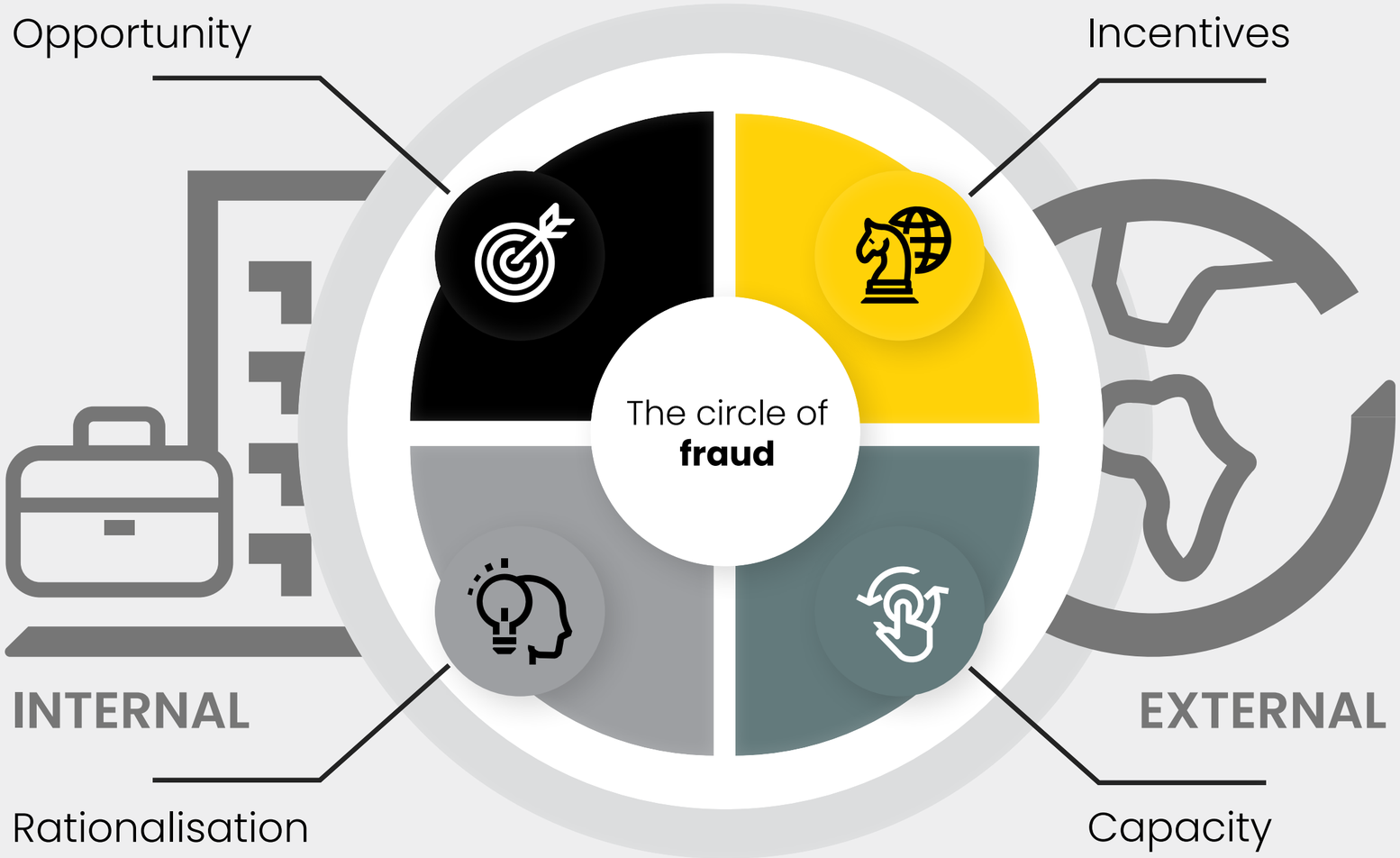
The world is currently characterized by what is being referred to as a **permacrisis,** a long period of instability and insecurity, especially in the aftermath of the COVID-19 pandemic and the Ukrainian conflict, or **polycrisis,** according to the latest World Economic Forum reports on **global risks.** In this context, there is a need for in-depth reflection on the main variables which are affecting the world currently and going forward, in addition to the **systemic effects** that the interaction between different types of risk generates, amplifying in many cases their impacts.

The fight against occupational fraud is an **integral and cross-cutting work in organizations,** as multiple and diverse departments can be affected. It is therefore important to have clarity in the responsibility hierarchy of the areas involved, otherwise a chaotic and conflicting management with duplicities, encroachment of competences or leadership problems, among others.

HOME

Graph 5
The circle of fraud

Source: Prosegur Research, 2023



Thus, **the explanation of occupational fraud cannot be separated from the analysis of the external and internal corporate context,** in addition to the four main variables that motivate a person to commit this criminal act: opportunity, incentive or motivation, capacity and rationalization.

Therefore, the economic crisis, social change, **individual empowerment,** changes in work models towards hybrid formats, or **technological development** generate transcendental impacts on criminal phenomena, such as occupational fraud or insider risk, especially affecting the motivations and objectives pursued by the perpetrators, as well as the modus operandi in which they are developed.

Thus, **from Prosegur Research we propose an occupational fraud model** based on the external and internal variables that may have an impact on this phenomenon:

A **Long view:** the impact of the external context

Societies, and consequently, the economy, policies and technologies evolve at an accelerated pace, impacting any phenomenon related to security. Thus, **insecurity is, to a large extent, a contextual situation.**

The employee of a company, regardless of whether it is public or private, **is no stranger to ambient conditions changes,** so external variables can have a decisive influence on their behavior:

1 Economic or financial instability

Interest rate hikes, inflation, falling purchasing power, housing costs or labor instability are some of the variables that can operate as an incentive for the fraudster.

2 Corruption

A high perception of corruption and the apparent normalization at all levels of society enhances the rationalization of the criminal act.

3 Uncertainty

The perception of constant risk by citizens is framed in the current context characterized by fragility, anxiety, incomprehensibility and the non-linearity of events - as the BANI paradigm presents it - following some systemic risks observed in recent years, such as the war in Ukraine or the COVID-19 pandemic, which enhances a constant state of collective and individual anxiety.

4 Complexity

The technification (the development of new technologies and digital transformation) and financial complexity favors players who have the capabilities to carry out occupational fraud, increasing the criterion of opportunity.

5 Anomie

The absence of a sense of belonging to the organization, the lack of trust in authorities and institutions and the apparent impunity, all contribute to the justification of the acts.

6 Individualism

One of the greatest challenges for companies today is talent retention, with increasing demands of employees on their working conditions, as has been observed in recent months in the adoption of remote work, for example. Citizens, generally, and workers are characterized by requirements and a progressive loss of traditional loyalty to companies.

7 Era of contradictions

Greater access to knowledge and resources nowadays, largely enabled by the Internet, increases the capacity criteria for fraud, being able to carry out actions by themselves that would have been unthinkable years ago.

B

Depth of vision: corporate culture as a differentiating element

In the internal context, consideration should be given to those issues that are affecting organizations dynamically and with highly volatility, and which can **modulate the phenomenon of fraud,** facilitating, enhancing and producing synergies between internal, external and individual contexts.

Thus, the factors that should be analyzed in each company are equally diverse.

1 Digital transformation

The capabilities of task and process automatization result in important benefits both for employees and the company, even though digital generation gaps may occur, which coupled with the issues of technological management platforms might entail frustrations for the employee.

2 The global scope of organizations

The confluence of diverse corporate and security cultures, with different habits and management styles, might sometimes imply the normalization of fraudulent actions in other countries.

3 Instability

The prevailing instability in most companies due to the technological advancement, industry evolution, and ongoing workforce adjustments or the future viability of the company are just some of the variables that may manifest as an incentive for the fraudster.

4 Multisectoral nature

Cross-cutting activities in different sectors of the corporations potentially increase the ways in which fraud can be made, which broadens the attack vectors within the company.

5 Developments in the areas of security and risks

Security is an evolving and changing concept, and security departments do not always evolve at the same time as the speed of the changes in criminal phenomena, coupled the limited resources available to them and the absence of the specialization which is key to understand occupational fraud.

6 Reactive vs. strategic

Sometimes the occupational fraud plans that corporations have in place are eminently reactive in nature, requiring the creation and establishment of prevention and anticipation plans and the anticipation of these events from the maturity of strategic models.

03

A strategic vision on the phenomenon

HOME

01 A major occupational threat

02 An analytical perspective on occupational fraud

03 A strategic vision on the phenomenon

04 Trends in occupational fraud

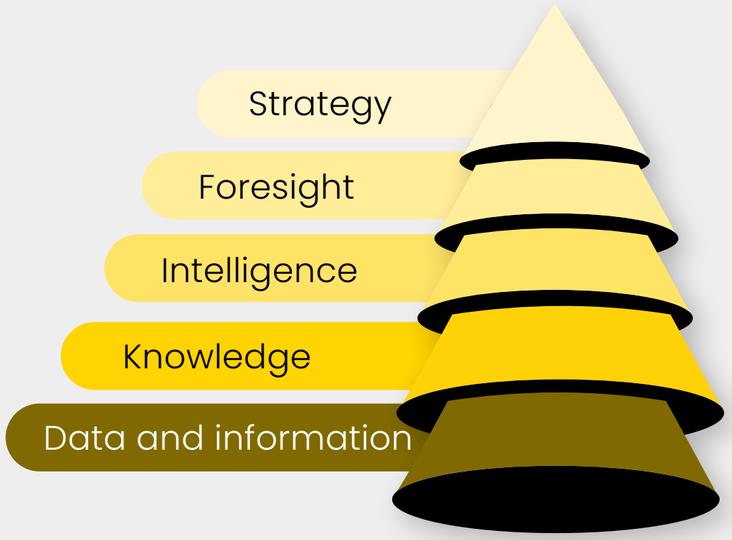
03 A STRATEGIC VISION ON THE PHENOMENON

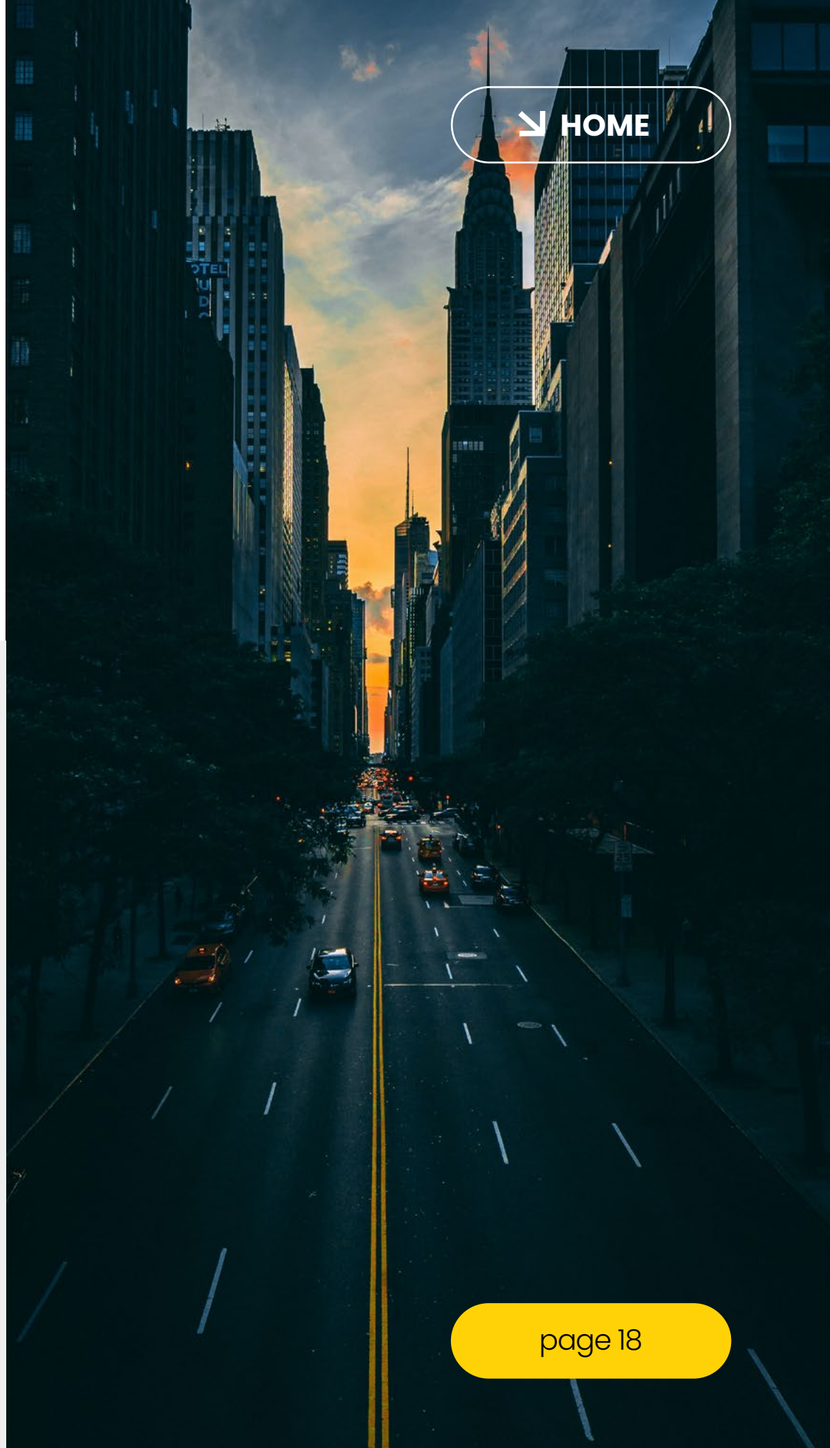
3.1 A clear organizational structure

Based on the framework of analysis described above, each organization should be **conceived as a holistic system** in order to create **structural programs** against occupational fraud. For this reason, **corporate action** must be oriented towards the **strategy** and the creation of effective prevention and reaction plans, for which **intelligence** is one of the main assets of any company.

Graph 6
The pyramid of the corporate action

Source: Prosegur Research, 2023





HOME

HOME

Occupational fraud, once it occurs, has an impact on the entire corporate ecosystem, with a multitude of departments affected directly or indirectly related to each other. From the immediate response expected from **human resources teams, risk management and compliance,** all those involved in **communication** teams must minimize their impact and effectively convey the right message to all related stakeholders.

Additionally, **security channels and information technologies** must be enhanced and improved, with the aim of ultimately reducing their impact on areas of organizational relevance such as the **financial** or **sales** one, ensuring business continuity and the operability of the of the entire organization.

All this derives in the **company culture** as a differentiating element to avoid the perpetration of occupational fraud. It is part of the organization's responsibilities to ensure the correct performance of the employee and, to the greatest extent possible, for their well-being, and it should emphasize the oversight and the criteria pertaining to environmental, social, and governance (ESG) factors and increase employee **engagement.** In this regard, companies with strong and visible ESG have a ***14% higher employee satisfaction rate.***

Graph 7
Occupational fraud
in the corporate ecosystem

Source: Prosegur Research, 2023

3.2 Risk **analysis**

Risk analysis is the process of identifying, analyzing and assessing occupational fraud risks, in order to take the necessary measures for their elimination or, at least, mitigation.

Following the analysis of the internal and external context using **detailed and methodical tools and processes,** which include some such as PESTEL, SWOT or data analysis, the risks and critical areas where fraud can occur are identified. Thus, **the sources of threats and vulnerabilities** are determined, assigning probability, impact and exposure, in order to finally **propose and adopt the necessary measures.**

Graph 8
Occupational fraud risk management

Source: Prosegur Research, 2023

HOME

A Prevention

Prevention is the main objective of a strategy against occupational fraud, creating a context so that fraud does not occur, and consequently acting to reduce the opportunity variable in the occupational fraud model, without excluding resulting consequences in the incentives, capacity and rationalization.

It is for this reason that **fraud prevention** plans, and compliance techniques are of great relevance to companies. According to the WCA, **up to 80% of companies across multiple industries admit to having been a victim of fraud,** yet more than half do not have comprehensive fraud prevention systems in place, **even though 85% of employees who commit these acts show signs of risk.**

Hence, both static nature **measures such as codes of conduct,** reporting channels and fostering a compliance culture, as well as **practical measures** including the implementation of controls, audits, monitoring and KPIs, are of interest.

HOME

B Detection

Detection is the second objective of anti-fraud strategies, although it is characterized as a **highly complex action,** given the relationship of trust on which the employment relationship is based and the involvement of a diverse variety of interconnected variables.

One of the most important aspects in the fight against occupational fraud at the time of detection are the **signals of risk,** or **"red flags",** that workers may display, **including personal, organizational and other stressors,** such as excessive pressure, high irritability, the presence of personal problems, failure to comply with compliance policies or the complexity of organizational processes and systems.

According to the ACFE, among the most common ways of detecting **fraud is reporting.** Thus, the presence **of ethical and bidirectional communication channels** between the employee and the company, as well as the performance of **background checks** and reports on personnel and managers to detect signs of impropriety, are some of the tools that can help organizations to reduce the impact of occupational fraud.

C Response

Once a case has been detected, or suspected, and always under the specific regulatory framework of each geographic region, a **comprehensive response** is required, with the aim of proving the wrongdoing, establishing the responsibility for it and obtaining sufficient and necessary evidence to be capable of taking disciplinary and/or judicial action.

This comprehensive response must be provided at all levels. On one side, **research** of the matter must be conducted by highly specialized teams with forensic expertise in relation to financial accounts, document analysis, digital forensics, intelligence analysis and field work. Additionally, after the collection of **evidence,** the actions deemed necessary, among which are the disciplinary action, disassociation from the organization or appropriate legal action. In conclusion, the analysis process cannot be neglected, in order to extract **insights on lessons learned** and to adjust existing controls and culture. Existing controls and corporate culture to reduce the chances of perpetration of this act.

A Prevention

Static actions

- Corporate policy
- Codes of conduct
- Training
- Awareness campaigns
- Ethical reporting channel

Practical actions

- Audits
- Controls
- Monitoring
- Alerts
- KPIS

B Detection

Fraudsters often exhibit **previous suspicious behavior:**

- Personal factors
- Organizational factos
- Stressors
- Behavior

C Response

Research

- Forensic Analysis
- Anti-fraud intelligence
- Field work

Evidence

- Disciplinary regime / framework
- Termination of employment
- Legal actions

Other actions

- Communication
- Learned lessons
- Adjustment of controls

04

Trends in occupational fraud

HOME

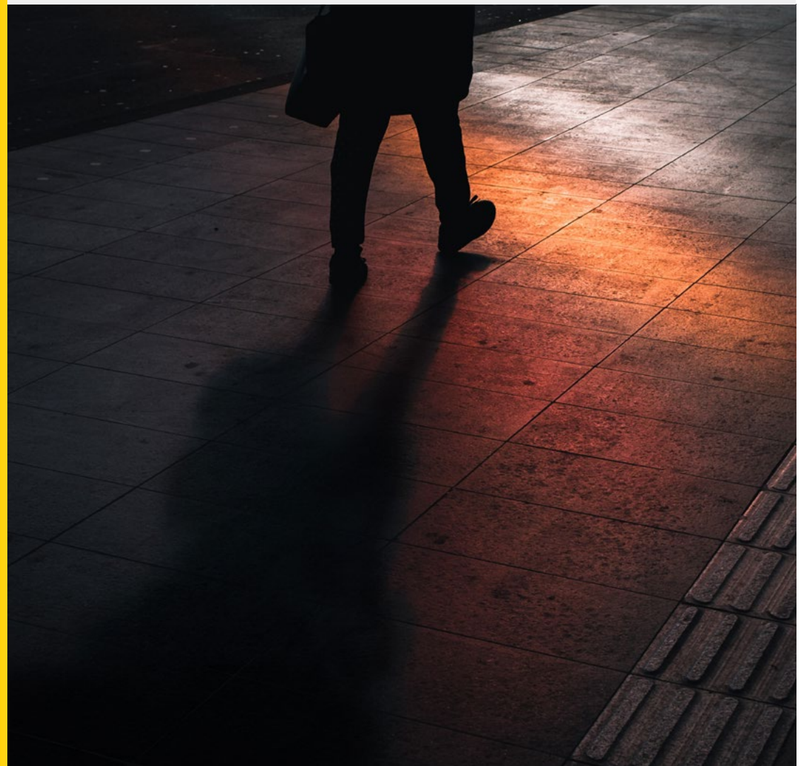
01 A major occupational threat

02 An analytical perspective on occupational fraud

03 A strategic vision on the phenomenon

04 Trends in occupational fraud

04 TRENDS IN OCCUPATIONAL FRAUD



As has been evident throughout the document, **occupational fraud is a complex,** evolving phenomenon in which innovation also plays an important role. Therefore, far from being a bureaucratic task for organizations, it must also be approached with an open and strategic mindset.

Thus, **trends in technological developments** are leading to a boom in new forms of fraud that companies need to consider when developing their prevention and mitigation plans: for example, **up to 8% of all fraud detected in 2022 were related to cryptocurrencies,** which were not originally designed for fraud but now help to commit bribery and asset appropriation. As the ACFE points out, **it is foreseeable that there will be an increase in the next years in the commission of occupational frauds related to cryptocurrency,** especially if the trend in its use by companies and society is consolidated. For this reason, it is essential to have prevention plans, investigation formulas and adequate reactive measures with the support of organizations with solvency and experience in this field.

In addition, **platforms** have gained great relevance in the operation of businesses worldwide in recent years, including financial, enterprise, social networking and communication platforms, etc. In this regard, PwC points **a new criminal modality in economic crime,** known as **platform fraud.** According to the data provided by the company, **91% of the organizations analyzed have experienced this type of criminal activity in the last 24 months.** Moreover, in more than half of the cases, these frauds involve economic losses, with additional consequences such as damage to organizational culture and reputation. In addition, **in 51% of cases, these frauds are carried out by internal sources or a confluence of internal and external threats, with organized crime playing an increasingly important role.**

On the other hand, **CEO fraud,** also known as Business Email Compromise (BEC), **is one of the fastest-growing lines of crime in recent years,** as reported in the FBI's **Internet Crime Report 2021,** driven by the adoption of **remote work,** with cases being recorded in more than 150 countries around the world. Thus, **cyber-attacks** have experienced an exponential grow up to **125% in 2021** following the COVID-19 pandemic. It is for this reason that criminals seek to gain access to the company by using company employees, usually from the C-Suit, posing as the CEO. In this regard, although it is not initially set up as an occupational fraud, the action of an employee is necessary, sometimes due to ignorance or negligence, for it to be perpetrated, therefore the **combination of internal and external sources** in this area is crucial. Thus, it is foreseeable to continue to increase in the coming years **phishing attacks, social engineering and other derivatives such as spear phishing and executive whaling** depending on the target of the attack.

HOME

The gradual integration, across an expanding array of spheres in our existence, of devices and technological systems is hampering the fraud prevention plans of many companies. According to Forbes and Experian point out, **identity theft,** enhanced by artificial intelligence and deepfakes, known as ***"Frankenstein IDs",*** whether by actors inside or outside the organization, hinders **biometric-based prevention,** therefore cybersecurity will play a crucial role in the business continuity in the coming years.

Finally, beyond the varied impacts of technology in this area, it is important not to overlook the **socio-political and economic context** in which the employee is immersed. Variables such as **economic difficulties,** high **inflationary rates** in a multitude of countries such as Venezuela, Argentina, Zimbabwe or Turkey, among others, or the **high level of social unrest can increase the risk of occupational fraud, especially if unfavorable conditions continue in the coming months** reducing the purchasing power and quality of life of citizens.

HOME

All these trends are intended to place the phenomenon in a future context, but we undoubtedly believe that this future will be positive. In pursuit of this, at Prosegur Research, we have added **three key elements of corporate culture to inhibit fraudulent behavior:**

A People with judgment make the difference

Companies undertake arduous endeavors to attract and retain talent, which includes having **employees who perform at their jobs diligently,** but **beyond the role[1]:** knowing what to do when protocol does not fit the complex and changing reality, generating value from Thoughtful innovation against fanciful notions and peddling of smoke and permeating the office with authenticity and vitality for the sake of business consolidation.

B Confidence throughout the value chain

In any business, **solvency presents as a true competitive edge;** eradicating fraudulent behavior requires the establishment of a structure of commitment from the company, which allows the professional and personal growth of employees. To this end, in the era of immediacy flooded with KPIs, we need to **de-bureaucratize based on trust in the employee** and generate spaces for new approaches of work, leadership, learning and, ultimately, existence.

C Against silo labor: generosity

Few situations are as paralyzing in a company as the departmentalization of tasks and the compartmentalization of objectives; a transparent company must encourage **systemic thinking and altruistic behavior** in its day-to-day operations. It is not about philanthropy and generosity, but rather about training the empathy of those sensible and trustworthy employees to **guide direct efforts toward the shared purpose.**

A company without purpose attracts employees without mission or values; therefore, generating a work community by including criteria, trust and generosity as part of the work environment enables overcoming the arrogance of "mine" and **building a positive future based on "ours".** This idea does not consist of forcing employees to prioritize the company over their own interests, but rather to align the objectives of each one in order to achieve a mutually beneficial outcome that serves the interests of both parties. **Prioritizing our most humane aspect** is the best way to inhibit undesirable behavior and promote a culture of safety from the nature of **good employees, which the data tells us is the majority.**

[1] What anthropologist Hutchins as early as 1995 called **Cognition in the Wild** in his studies of the navigational complexities faced by U.S. Navy crews, analyzing the cognitive work arrangements in these situations as opposed to the typical laboratory study.

PROSEGUR

We guarantee safety for people,
businesses and society as a whole.

research@prosegur.com

PROSEGUR **RESEARCH**

www.prosegurresearch.com