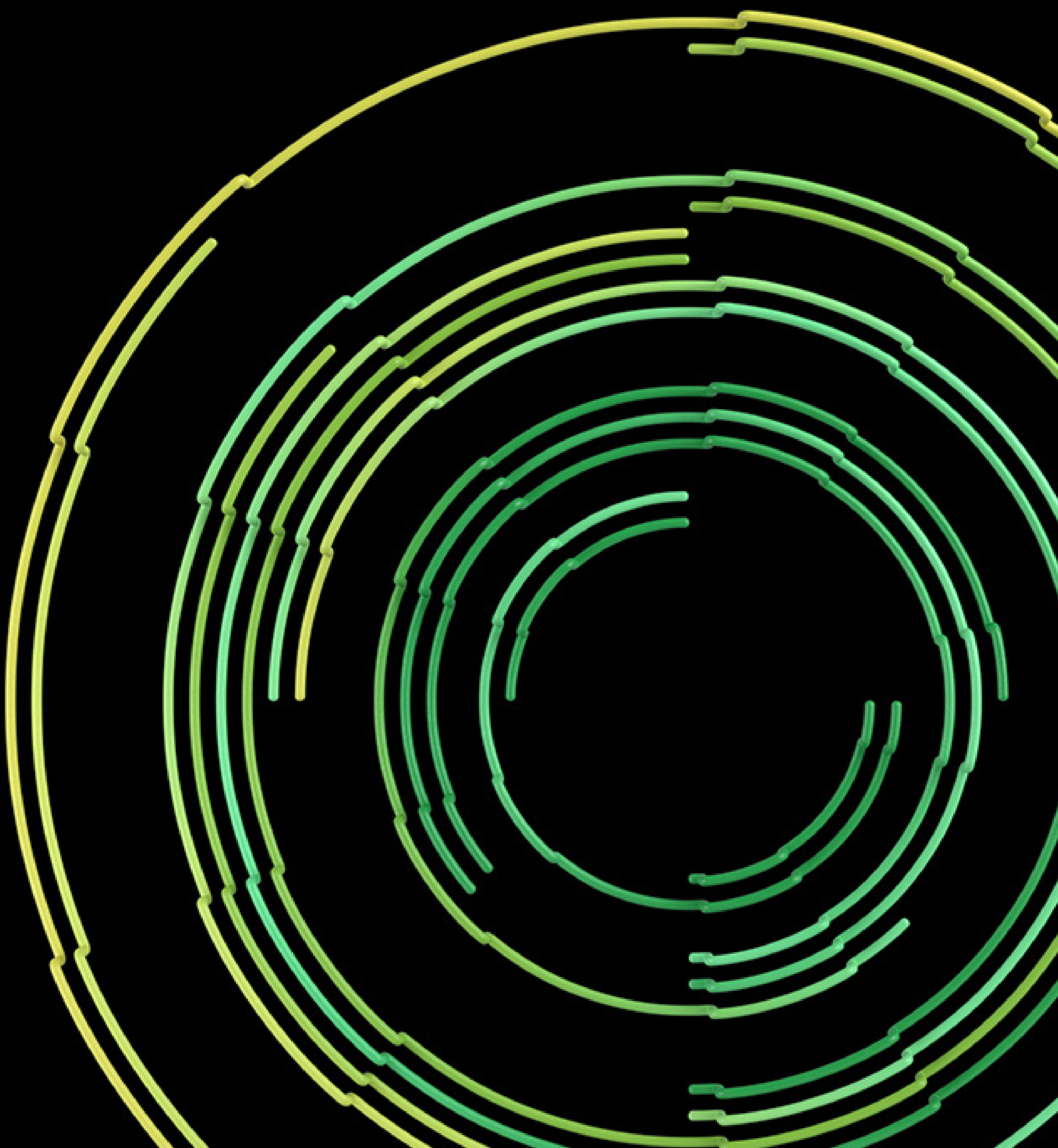
Deloitte.

*Together makes progress*

# An X-ray of ***occupational fraud*** in Latin America



# Introduction

To understand how organizations in Latin America are dealing with occupational fraud by 2026, we conducted a regional survey targeting companies operating in Chile, Colombia, Costa Rica, Mexico, Panama, Peru, the Dominican Republic, and Uruguay. The objective was clear: to identify not only the incidence of fraud, but also the actual ability of organizations to prevent, detect, investigate, and respond to fraud.

The results confirm an uncomfortable reality: occupational fraud is widespread in Latin America. Almost two out of three companies admit to having identified at least one case in the last 18 months, with asset theft being the predominant scheme. However, this high incidence coexists with a widespread perception that there may be undetected fraud within organizations, which reflects awareness of vulnerability in control mechanisms.

The analysis also shows that, although most companies have reporting channels and internal controls, the sophistication of technological mechanisms to prevent and detect fraud early is still limited. Detection continues to rely heavily on internal reporting and manual review processes—such as periodic audits, reconciliations, and transaction analysis by staff—while the use of advanced analytics and Artificial Intelligence (AI) remains, in most cases, in the early stages of exploration.

Another relevant finding is the partial visibility of the financial impact. A significant proportion of companies fail to accurately quantify losses associated with fraud, making it difficult to assess the impact and, with this, prioritize investments in prevention. Likewise, the times of investigation and closure of cases, as well as the absence of formal protocols in some organizations, suggest fragmented and poorly standardized responses.

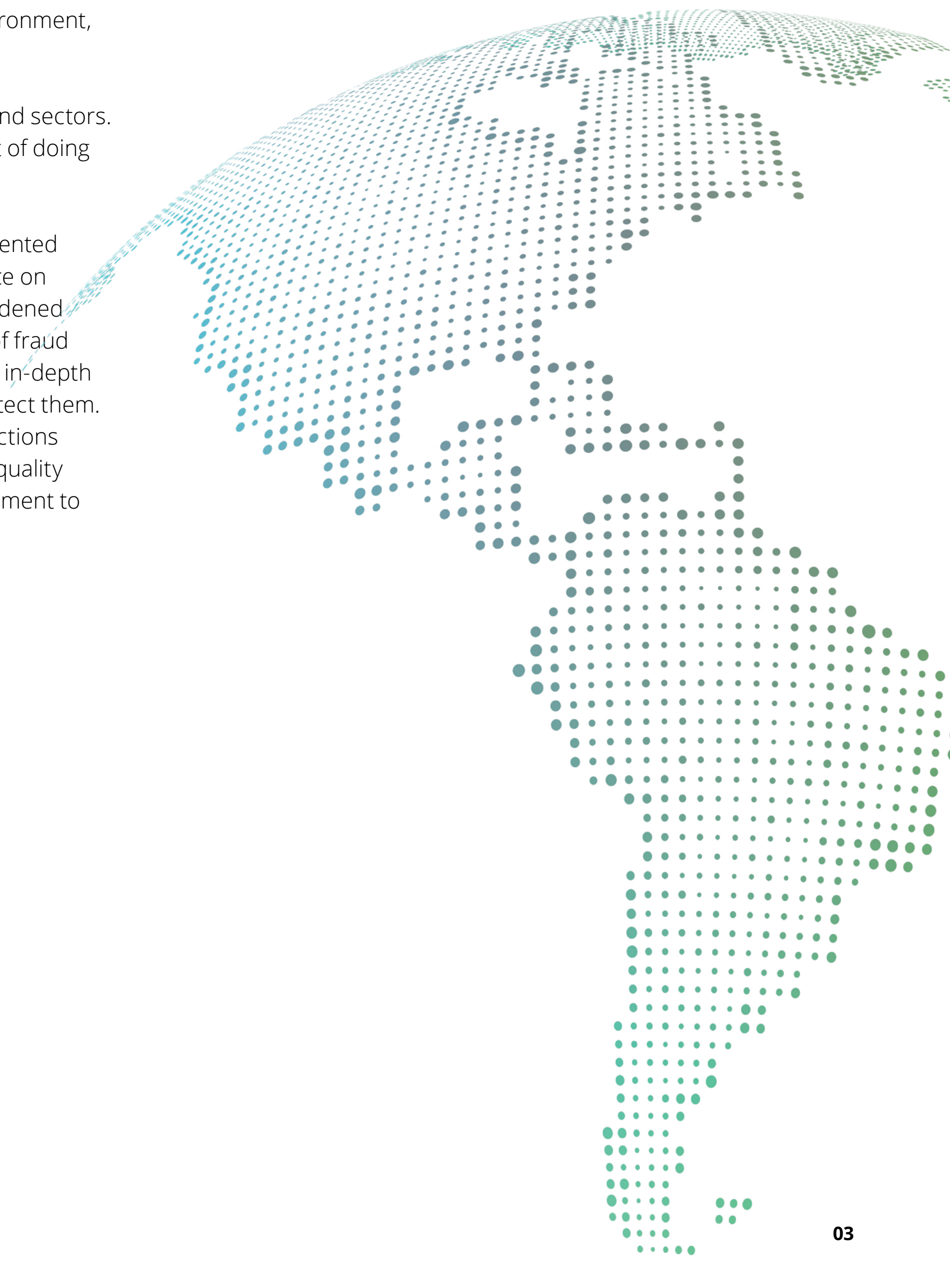
This paper explores these findings and raises a central question for business leaders in Latin America: are organizations truly prepared to address occupational fraud as a strategic risk by 2026, or are they still managing it as an isolated incident? The following pages offer a clear snapshot of the current state and open the conversation about what needs to change to close the gap between control, culture, and organizational resilience.

# Occupational fraud as a structural symptom

The understanding of occupational fraud has evolved: it is no longer explained solely by individual failures, but as a structural consequence of economic, organizational, and technological factors. Globally, the Association of Certified Fraud Examiners (*ACFE*) revealed, through a study carried out in 138 countries – with 1,921 cases – that the organizations included in its analysis collectively lost just over 3,000 million dollars (million) due to internal fraud in 2024, with an average loss of 1.6 million dollars per case1. These are figures that, transferred to emerging economies, acquire an even more significant impact due to narrower margins, less sophistication of controls and greater gaps in informality.

Latin America faces this risk in a particularly complex environment, marked by macroeconomic volatility, pressure for results, accelerated but incomplete digitalization processes, and heterogeneous regulatory frameworks across countries and sectors. These conditions can normalize fraud as an accepted cost of doing business, often outside the strategic agenda.

In addition, the transformation of work models, the fragmented outsourcing of critical functions, and the increased reliance on digital systems have weakened traditional controls and widened the risk surface. Added to this is a greater sophistication of fraud schemes, supported by technology, internal collusion and in-depth knowledge of the processes, which makes it difficult to detect them. In this context, occupational fraud transcends control functions and becomes an indicator of organizational maturity, the quality of corporate governance, and the ability of senior management to balance growth, efficiency, and control.



# High incidence and overconfidence in fraud detection

The survey findings reveal an important starting point: 64% of companies identify at least one case of fraud in the last 18 months (Figure 1). In contrast, 32% say they have not detected events of this type, which confirms that occupational fraud is not a marginal phenomenon, but a common experience for most organizations in Latin America.

Contrary to what might be expected, the internal perception does not reflect full confidence in the detection mechanisms. Almost 7 out of 10 respondents believe that fraud has occurred in their organization without having realized it, compared to 3 out of 10 who disagree with this possibility (Graph 2). This result suggests a relevant awareness of vulnerability and possible gaps in control mechanisms, rather than a perception of security.

**Figure 1. In the last 18 months, has your company identified any cases of fraud?**

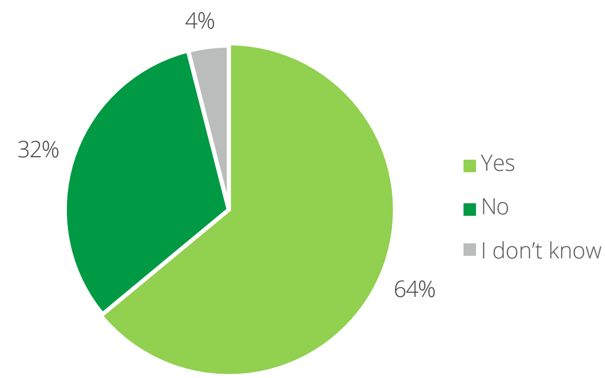
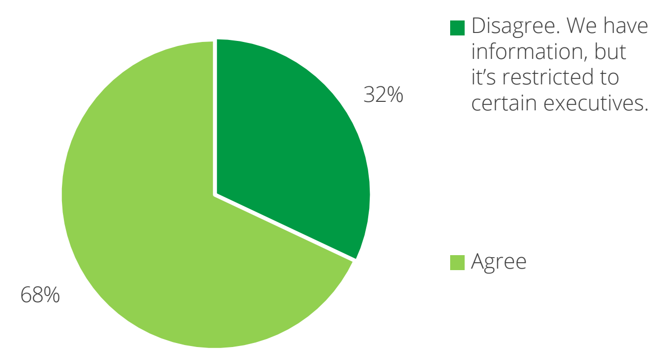



**Figure 2. Do you think that fraud has occurred in your company without you having realized it?**




Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

The predominance of asset theft as the main form of fraud (40%) suggests that organizations continue to be more vulnerable in their basic operational controls, especially in processes that involve direct handling of cash, inventories, payments, physical goods or authorizations of financial resources. On the other hand, the relative weight of conflicts of interest (12%), although lower, should not be underestimated, since they do not constitute fraud *per se*, but can act as triggers for fraudulent conduct when they converge with undue incentives, discretionary decisions, undeclared relationships and weaknesses in transparency and oversight mechanisms (Graph 3).

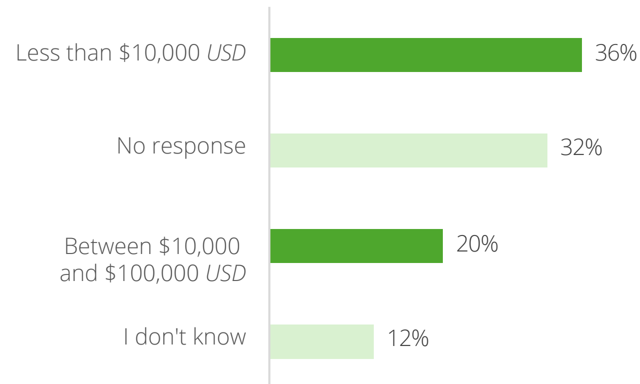
The fact that a proportion of respondents (8%) are unable to identify the type of fraud that occurred could reveal an additional weakness: limitations in the processes of investigation, classification and subsequent analysis of cases. Not only does this make it difficult to understand the real risk, but it reduces organizational learning capacity and the effectiveness of future preventive actions.

When evaluating the economic impact of fraud, the results reveal a significant dispersion: 36% of companies report losses of less than 10,000 dollars (*USD*), while 20% estimate impacts between 10,000 *USD* and 100,000 *USD* (Graph 4). However, 44% of respondents say they do not know the financial impact or prefer not to answer.

This lack of financial visibility is a critical finding in itself. Detecting fraud without quantifying its impact limits decision-making, makes it difficult to priorities investments in prevention and reduces the real perception of risk by Senior Management.

**Figure 3. If it had occurred, what type of fraud was it?**


**Figure 4. Do you know what the financial impact has been?**




Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

# Reliance on traditional mechanisms in the face of increasingly complex risks

Internal Audit's leadership in fraud investigation (48%) reflects an approach focused on identifying and correcting incidents once they have already occurred, rather than anticipating them through integrated preventive mechanisms. The secondary involvement of the compliance function (16%) reinforces this reading, showing a still reactive approach focused on regulatory compliance rather than comprehensive risk management (Exhibit 5).

The absence of a team in charge in one part of the organizations, as well as the dispersion of responsibilities among multiple areas, reveals a fragmented governance of fraud, particularly in the detection and investigation functions. This lack of clarity in the assignment of roles can translate into delayed responses, inconsistent criteria, and a reduced capacity to institutionalize learning at the organizational level. The results suggest that, although fraud is recognized as a relevant problem, its management is not yet consolidated as a clearly defined strategic function that integrates prevention, monitoring and response.

In terms of the level of capacity to investigate fraud – considering technical knowledge, defined processes and available resources – 80% consider their team to be "somewhat prepared", while 16% perceive it as "very prepared" and a minimum part "poorly prepared" (Graph 6). This perception contrasts with other findings of the study, particularly the absence of formal protocols in a relevant proportion of companies.

**Figure 5. Who is in charge of fraud investigation in your company?**

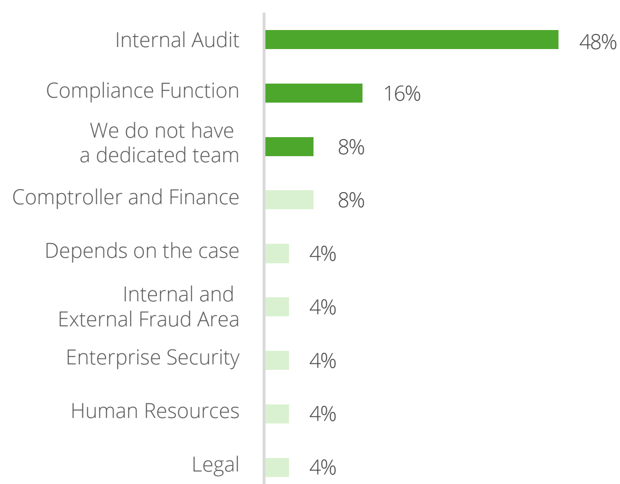
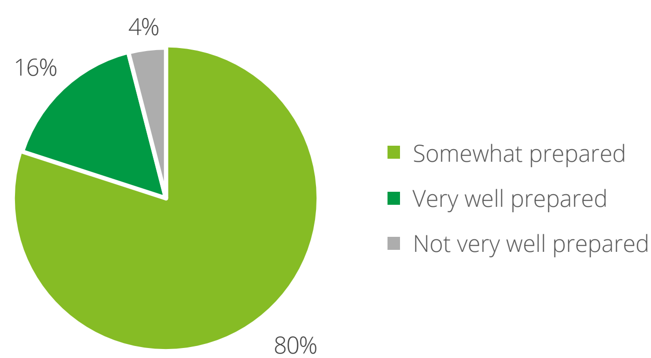



**Figure 6. How prepared do you think the team in charge of investigating fraud is?**




Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

From a preventive perspective, the survey shows relevant progress, although with clear limits. Graph 7 indicates that 92% of companies have an anonymous reporting channel and Graph 8 shows that 56% provide fraud prevention training at least once a year. However, 2 out of 10 organizations surveyed declare that they have not carried out training.

Even more worrying is the reliance on traditional mechanisms, as 84% of organizations use internal reports and employee complaints as the main detection tool, while only 4% use automated monitoring and anomaly detection systems (Figure 9). This confirms that prevention remains predominantly reactive and manual.

**Figure 7. Does the company have an anonymous reporting channel to report, among other things, fraud?**

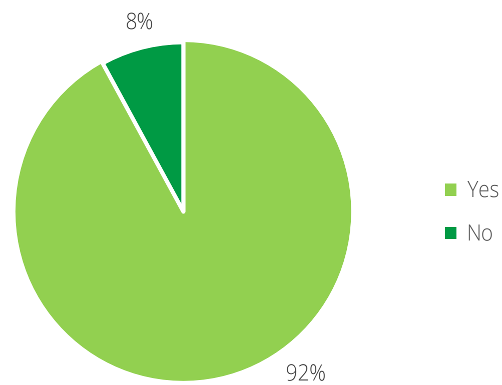



**Figure 8. How regularly does your company deliver fraud prevention training?**

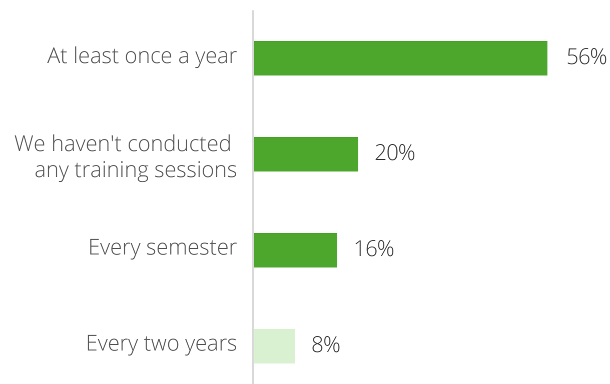
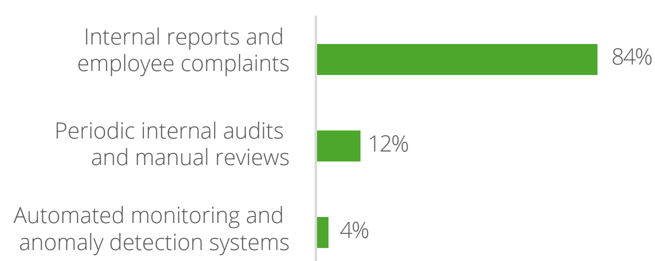



**Figure 9. What tools does your company use to prevent and detect fraud?**




Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

# Internal controls and investment: sufficient today, insufficient for tomorrow

The effectiveness of internal controls is evaluated moderately: 76% of the organizations surveyed consider their controls "moderately effective" and 16% rate them as "very effective" (Graph 10). Overall, the results show that there is a recognition of the presence of controls, but also that they have not yet reached an optimal level.

This perception aligns with the levels of investment observed in the survey. Although almost half of the organizations have a budget considered reasonable for fraud detection (48%), a relevant proportion operate with limited resources or without specific allocation (Graph 11). The fact that only a marginal group has a considerable budget (4%) shows that the recognition of fraud as a risk does not always translate into investments proportional to its frequency and impact.

This gap reinforces a predominantly reactive approach, in which resources are allocated to managing incidents that have already occurred rather than to strengthening preventive capacities, limiting progress towards more mature risk management models.

**Figure 10. How do you assess the effectiveness of internal controls in preventing and detecting fraudulent activity?**

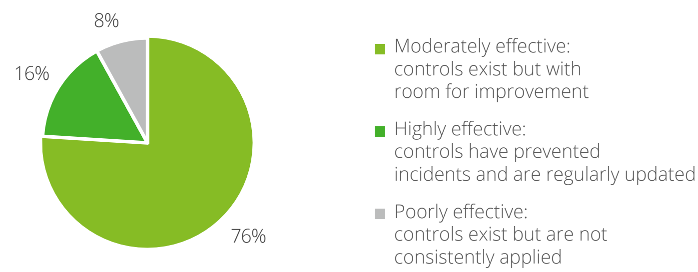
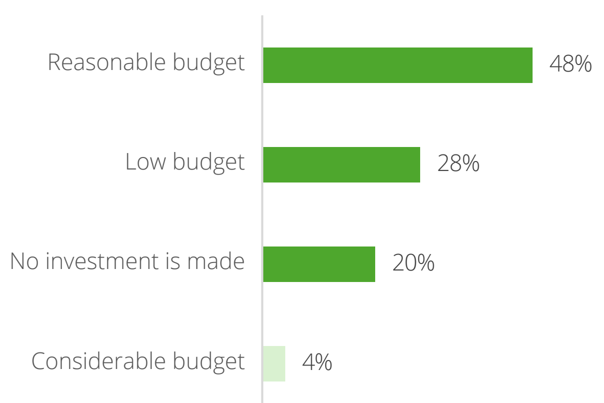



**Figure 11. What level of investment is allocated to fraud detection?**




**Investment levels for fraud prevention and detection**

**Considerable budget**
It includes cutting-edge technological tools, specialized training and prevention campaigns

**Reasonable Budget**
It includes some technological tool, some training and occasional prevention campaigns

**Low budget**
Sporadic hiring of external teams for investigations

**No specific investment is made**

Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

Our study confirms that AI is already on the strategic agenda: 60% of companies are in the exploration or implementation phase and 8% are already actively using it for fraud prevention and detection (Graph 12).

This technological advancement occurs in parallel with ethics and compliance programs of unequal maturity. Almost 6 out of 10 responses say (Graph 13) that they have a formal program with metrics and periodic evaluations, but, overall, 4 out of 10 organizations lack solid schemes, either because they do not measure in a structured way or because they do not have a program. In addition, technological adoption without a solid ethical and governance basis represents an additional risk.

**Figure 12. Has your company considered implementing AI-based solutions to improve fraud detection or prevention?**

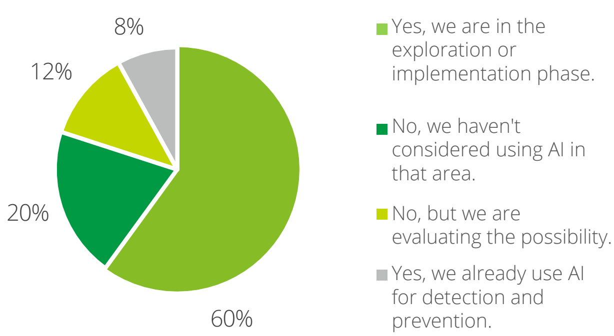
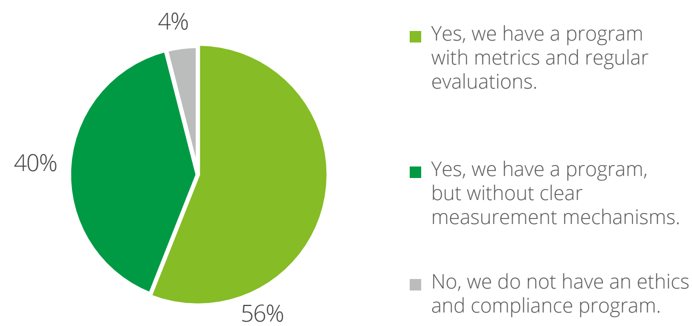



**Figure 13. Does your company have a formal ethics and compliance program in place? How is its effectiveness measured?**




Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

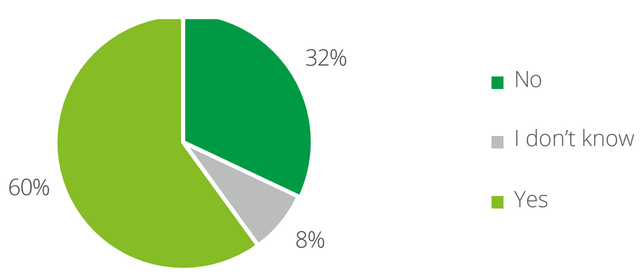
# Fraud response: protocols, timing, and consequences

The second half of the survey delves into the ability of organizations to respond to fraud. The first finding reveals that 60% of companies report having a formal protocol for fraud investigations, while 32% admit not having one (Graph 14). This dispersion shows that, although a significant part has made progress in the formalization of processes, gaps persist that can generate improvised, inconsistent responses or those dependent on key people rather than institutional structures.

Regarding resolution times, 48% indicate that the closure of a case takes between one and three months, 28% manage to do it in less than a month and 12% require more than three months; while the remaining percentage is not clear about the duration of the process (Graph 15). These differences reflect disparate levels of preparedness, resources, and internal coordination, where each delay—in addition to increasing financial losses—amplifies the reputational and legal impacts associated with late fraud management.

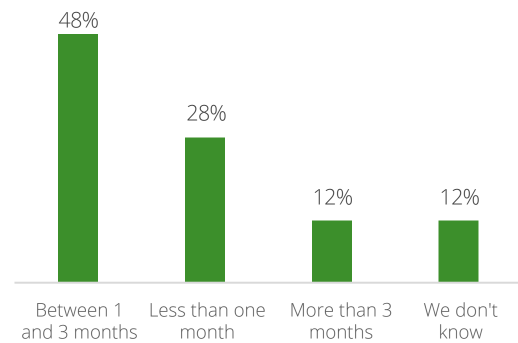
Regarding the actions taken, 72% choose to file a legal complaint, 20% resort to the dismissal of the person responsible and, to a lesser extent, 4% do not take specific measures (Graph 16). The latter group is particularly critical, as the absence of clear consequences weakens the deterrent effect, increases the risk of repeat offenses, and sends ambiguous signals about the organization's real commitment to integrity and accountability.

**Figure 14. Does your company have a formal protocol in place to investigate fraud?**



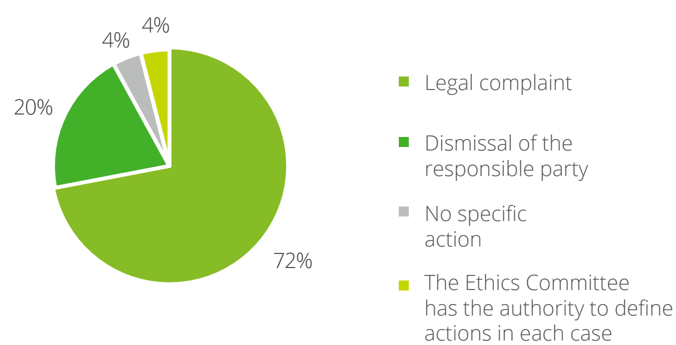

Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

**Figure 15. How long does it take on average for your company to close the fraud case?**




Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

**Figure 16. What actions does your company take when fraud is detected?**




Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

# Risks, internal control and organizational maturity

Another aspect that we detected is related to risk management, which has gained visibility in the organizational agenda. Eight out of 10 respondents consider this issue to be the responsibility of the Board or the General Management, suggesting a growing recognition of its strategic relevance (Figure 17). However, the fact that 12% still limits it to the area of Internal Audit reveals that, in some companies, risk continues to be approached from a technical and operational logic, rather than as a corporate governance responsibility.

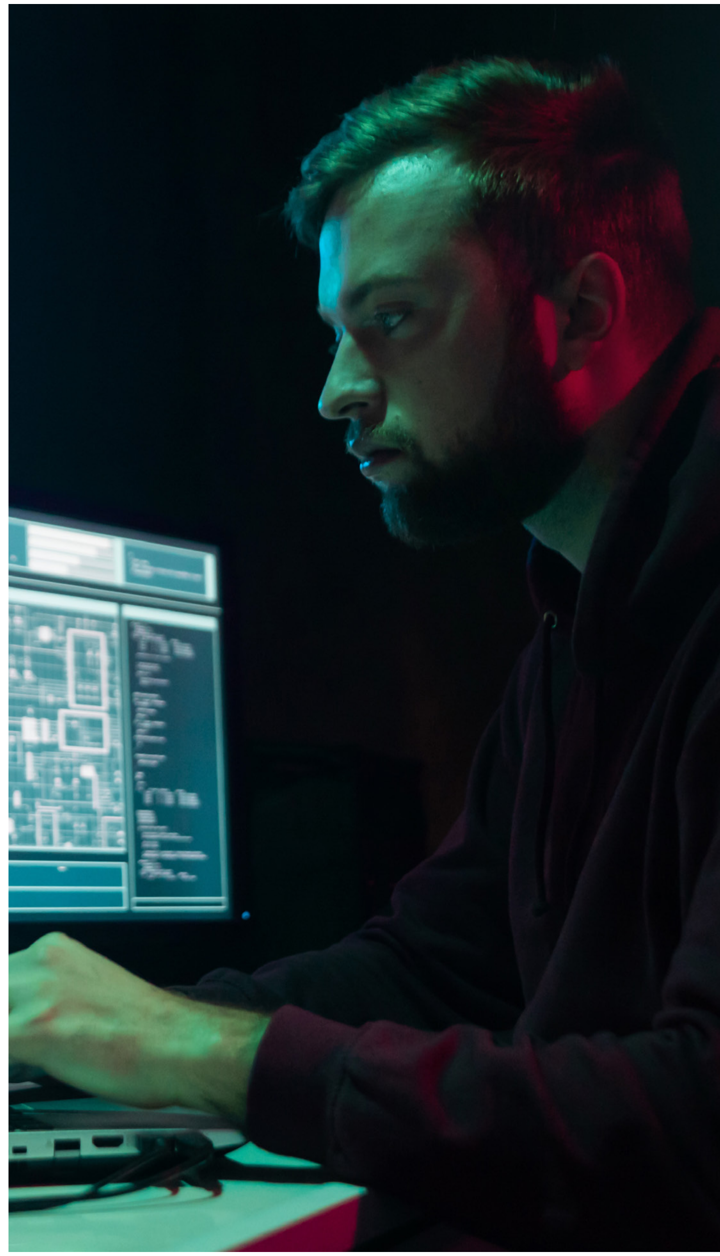
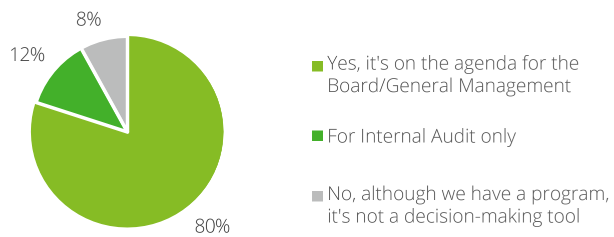


**Figure 17. Is risk management a priority in the company?**



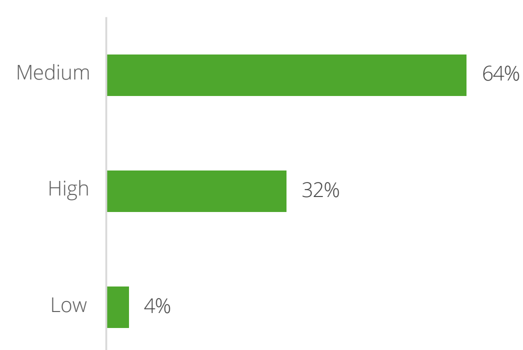

Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

However, this positioning on the agenda does not translate homogeneously into levels of maturity, since 64% are at a medium level, 32% at a high level, and the rest at a low level (Graph 18). This distribution helps explain why less than half (48%) perceive themselves to be truly prepared, while a relevant proportion admits to having only theoretical plans (36%) or facing slow and disorganized responses (Figure 19). Taken together, the results reflect a gap between the stated importance of risk and the actual ability to manage it consistently and effectively.

**Figure 18. How mature is risk management in your company?**

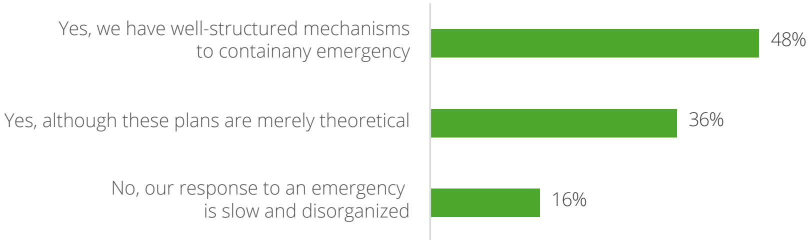
**Risk Management Maturity Levels**

| |
|---|
| **High**<br>We proactively identify, measure, and mitigate risks |
| **Medium**<br>We have risk management processes but they are not consistent |
| **Low**<br>Sporadic and isolated efforts |




Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

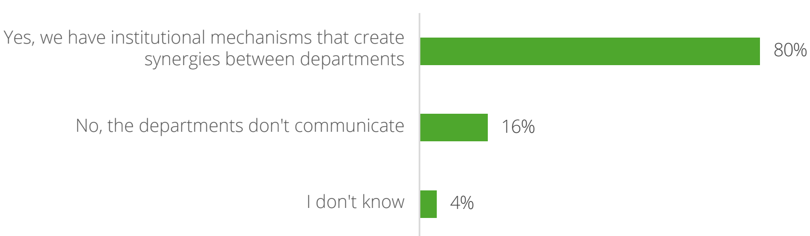
**Figure 19. Do you think that the company is prepared to give a timely response to when risks materialize?**




Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

The synergies between risk, fraud and internal control are present in most organizations, but they are not universal. Although 80% claim to have integration mechanisms, 16% recognize that the areas do not communicate adequately (Graph 20). This lack of coordination limits the holistic view of risk, fragments decision-making, and reduces the effectiveness of controls, particularly in contexts where risks are cross-cutting and rapidly evolving.

**Figure 20. Are there synergies between risk management, fraud prevention, and internal control?**

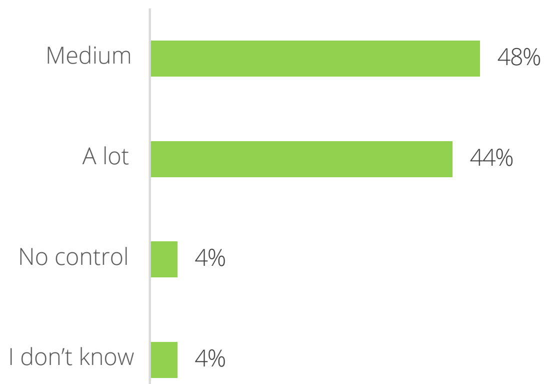



Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

# Diffuse responsibilities that affect the consistency of internal control

The perception of the internal control framework is mostly positive, although with relevant nuances. Almost half of the organizations consider that their scheme offers a medium level of control, while 44% perceive it as robust and 4% openly admit not having sufficient controls (Graph 21). In terms of practical responsibility, the allocation is heterogeneous: although a significant proportion is distributed among all areas (40%), in other cases it falls on specific functions such as Internal Audit, Internal Control or Comptroller (Graph 22). This dispersion suggests different approaches to the ownership of control, with direct implications for its consistency and effectiveness.

**Figure 21. How much control does your internal control framework provide?**




**Levels of control provided by the internal framework**

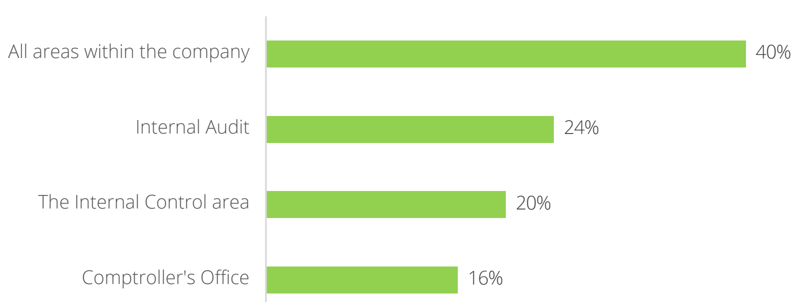
**A lot**
Our control model gives us assurance regarding risk mitigation, fraud prevention, and compliance.

**Medium**
Our model is efficient but it does not give us the security or confidence we need.

**No control**
We have notorious deficiencies in the processes, the materialization of risks and fraud is latent.

Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

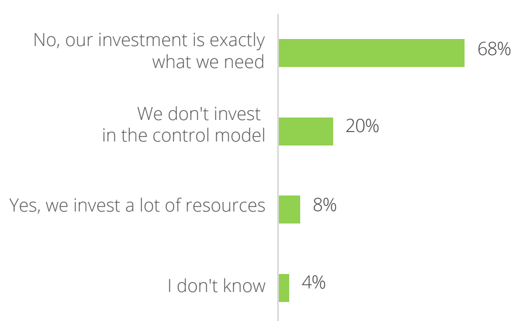
**Figure 22. Who are the internal control officers? Not in theory, in practice**



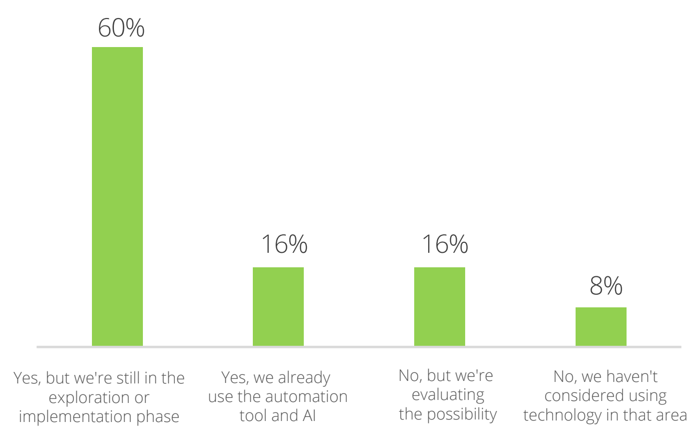

Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

The above reading is complemented by the reported investment levels. Although 68% do not consider investment in internal control excessive, a fifth of organizations do not allocate specific resources, which reinforces the idea of structural underinvestment (Graph 23). At the same time, although 6 out of 10 are exploring the use of technologies, there is still a relevant segment that has not considered them or barely evaluates them, which limits the potential for modernization and scalability of controls (Figure 24).

**Figure 23. Do you consider that the internal control model represents a considerable expense for the company?**



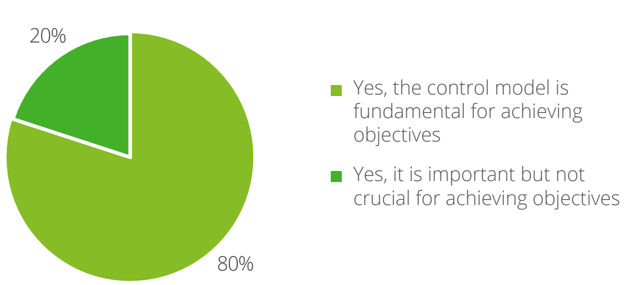

**Gráfica 24. Have you considered using innovative technologies to increase the efficiency of internal control?**




Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

Finally, internal control is widely recognized as an enabler of business objectives: 80% consider it basic to achieve them. However, the fact that 20% perceive it as only important but not crucial reveals a relevant conceptual gap (Figure 25). This vision can translate into inconsistent priorities, where control remains a necessary requirement, but not fully integrated into the strategy and decision-making of the business.

**Gráfica 25. Do you consider that the control model is necessary for the achievement of the company's objectives?**




Source: Survey "Radiography of occupational fraud in Latin America". Deloitte Insights.

# Conclusion

The results confirm that occupational fraud in Latin America is a structural and recurrent phenomenon, not an emerging risk. Its high incidence, the persistence of traditional schemes and the mostly reactive detection show that many organizations still manage them as isolated events, without addressing the systemic weaknesses that cause them.

Looking ahead to 2026, the challenge is not to eradicate fraud – an unrealistic expectation – but to raise anti-fraud maturity in a sustained way. This requires moving from reactive to preventive approaches, effectively integrating risk management, internal control, and technology, as well as strengthening accountability at all levels. The survey sends a clear signal to Senior Management: the level of fraud experienced by organizations is not an isolated phenomenon; it is a direct indicator of its governance model, the effectiveness of its controls and the maturity of its strategic decisions. Companies that incorporate it into their strategic agenda will be able to protect their value and sustain the trust of their stakeholders.

In this context, fraud does not define organizations; their level of preparation does. The real difference in 2026 will not be in whether fraud occurs, but in how prepared companies are to detect it early, learn from it, and strengthen their ability to respond. That is the line between vulnerability and resilience.

# References

01. Association of Certified Fraud Examiners (ACFE), *"Occupational Fraud 2024: A Report to The Nations"*. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

# Contact

**Israel Zagal**
**Advisory and Consulting Partner**
Deloitte México
izagal@deloittemx.com

**José Claudio Treviño**
**Partner of Forensic & Financial Crime**
Deloitte México
jotrevino@deloittemx.com

**Contact Center**
+52 55 5080 6633
centrodecontacto@deloittemx.com