UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO

RENATA FARIA GOMES

Connecting Technology and Professionals in Digital Fraud Management from a Computer Science Perspective

Recife

2025

RENATA FARIA GOMES

Connecting Technology and Professionals in Digital Fraud Management from a Computer Science Perspective

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

Área de Concentração: ENGENHARIA DE SOFTWARE E LINGUAGENS DE PROGRAMAÇÃO

Orientador: Prof. Dr. Vinícius Cardoso Garcia

Co-Orientadora:Profa. Dra. Daniela Soares Cruzes

Recife

2025

.Catalogação de Publicação na Fonte. UFPE - Biblioteca Central

Gomes, Renata Faria.
Connecting technology and professionals in digital fraud management from a computer science perspective / Renata Faria Gomes. - Recife, 2025.
131f.: il.

Dissertação (Mestrado)- Universidade Federal de Pernambuco, Centro de Informática, Programa de Pós-Graduação em Ciência da Computação, 2025.
Orientação: Prof. Dr. Vinícius Cardoso Garcia.
Coorientação: Profa. Dra. Daniela Soares Cruzes.

1. Fraud management; 2. Cybersecurity; 3. Computer science; 4. Risk management; 5. Digital fraud. I. Garcia, Vinícius Cardoso. II. Cruzes, Daniela Soares. III. Título.

UFPE-Biblioteca Central

Renata Faria Gomes

“Connecting Technology and Professionals in Digital Fraud Management from a Computer Science Perspective”

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação. Área de Concentração: Engenharia de Software e Linguagens de Programação

Aprovado em: 12/08/2025.

BANCA EXAMINADORA

_____

Prof. Dr. Divanilson Rodrigo Campelo
Centro de Informática / UFPE

_____

Prof. Dr. Kiev Santos da Gama
Centro de Informática /UFPE

_____

Prof. Dr. José Alonso Borba
Departamento de Contabilidade / UFSC

_____

Prof. Dr. Vinicius Cardoso Garcia
Centro de Informática / UFPE
(**orientador**)

ACKNOWLEDGEMENTS

Esta dissertação marca o encerramento de uma jornada de aprendizado, desafios e crescimento pessoal e profissional. Nenhuma etapa teria sido possível sem o apoio de pessoas muito especiais, a quem sou profundamente grata.

À minha mãe, Cláudia, por seu amor incondicional, força e exemplo de perseverança. Aos meus irmãos, Rodrigo e Rafael, por sempre estarem ao meu lado, mesmo nas entrelinhas da vida. À minha namorada, Izabella, que é também uma pesquisadora brilhante, por seu carinho, paciência e presença constante — estendo minha gratidão à sua família, que me acolheu com tanto afeto. À minha companheira de todas as horas, a Lua, cuja lealdade e amor me confortaram nos momentos mais difíceis. Ao meu padrasto Oscar, pelo suporte e incentivo contínuos.

Aos meus amigos queridos: Thamires, Alcides, Elton e Gabriela, por cada conversa, apoio e risada compartilhada. Também agradeço a todos os colegas da Apple Developer Academy e do BEPiD, com quem tive o privilégio de crescer e colaborar.

Expresso minha profunda gratidão ao professor Vinícius Cardoso Garcia, por sua orientação cuidadosa e confiança constante, e à professora Daniela Soares Cruzes, pela coorientação e pelo olhar sempre generoso. Ao professor Kiev, por seu apoio em momentos cruciais, e ao professor Fábio, por seus ensinamentos marcantes que influenciaram minha forma de pensar sobre ciência, ética e tecnologia.

Ao meu colega Ricardo, que esteve ao meu lado durante grande parte da caminhada do mestrado, dividindo ideias, inquietações e conquistas — minha sincera admiração e agradecimento.

E à minha líder Pamella, à minha parceira de Portal, Kamilla e aos colegas de trabalho, por todo o aprendizado compartilhado, especialmente em temas tão centrais como a fraude — que enriqueceram e aprofundaram ainda mais a minha perspectiva sobre o campo de estudo desta pesquisa.

A todas essas pessoas, minha mais sincera e afetuosa gratidão.

ABSTRACT

The escalating sophistication and volume of digital fraud demand robust, adaptive management. While academic insights exist on detection and tools, a persistent gap remains in comprehensively connecting these technologies with professionals and their practical contexts. **Purpose** – This dissertation addresses this gap by examining fraud management from a computer science perspective, focusing on software tools, relevant knowledge, and computing expertise. It seeks to answer key questions regarding current tool use and challenges, essential computer science knowledge and its application, and professionals' perception of collaboration with computing experts. **Methodology** – The study employs a mixed-methods approach, integrating a literature review, a software benchmark, and qualitative surveys conducted with Brazilian fraud professionals. **Findings** – Our findings indicate that technology is essential and multifunctional across all fraud management stages (deterrence to prosecution), but its effectiveness is often hindered by human factors, usability issues, and systemic fragmentation. Traditional frameworks struggle to capture real-world operational fluidity, and professionals encounter challenges like technical language barriers, limited integration, and bureaucratic inefficiencies, particularly in the public sector. **Recommendations** – To address these, the study advocates for integrated fraud resilience frameworks, improved technical communication to bridge human-technology gaps, legislative modernization for agile law enforcement, and responsible navigation of AI's ethical and security

Keywords: Fraud Management, Cybersecurity, Computer Science, Risk Management, Digital Fraud, Mixed-Methods, AI, Collaboration.

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

1 INTRODUCTION

The increasing sophistication of fraud, driven by the digitization of financial services and changing user behavior, has intensified the need for robust and adaptive fraud management practices. For instance, according to the latest Fraudscape report by CIFAS (CIFAS, 2025), fraud cases in the United Kingdom rose by 13% in 2025, setting a new record with over 46,000 cases (representing approximately 40% of all recorded crimes in the country) and resulting in 81 billion GBP in losses for public banks. This trend is not limited to the UK. In the United States, corporate fraud cases resolved in 2024 led to financial losses totaling approximately 2.3 billion USD (U.S. Department of Justice, 2025). In Brazil, 11,509,214 fraud attempts were recorded in 2024, with 2,361,409 incidents reported in just the first two months of 2025 (Serasa Experian, 2025). One major case of corporate fraud in the Brazilian public sector alone resulted in losses of 6 billion BRL to the population.

With the substantial increase in fraud cases, relying solely on manual analysis introduces significant vulnerabilities that can be exploited by opportunistic fraudsters. Consequently, the integration of technological tools is therefore essential to support fraud analysts in their daily activities (BEHDAD et al., 2012; CAVUSOGLU; RAGHUNATHAN, 2004). Given its importance, fraud has been widely examined in academic literature, which highlights a variety of tools and techniques such as data visualization (ZHOU et al., 2023), fraud detection systems (THAKUR et al., 2023), and the use of machine learning in risk management (SCARPINO, 2022).

Although the literature provides a broad overview of software tools, fraud management remains a complex challenge that cannot be fully addressed by technology alone. Recognizing the human dimension of this domain, several studies have investigated the professional practices and decision-making processes of key actors involved in fraud prevention and investigation, such as forensic accountants (OZILI, 2021), financial auditors (NAJAR et al., 2025), and governance and compliance professionals (FATRIZIA; PUTRA; HIDAYATI, 2025), underscoring the multidisciplinary nature of effective fraud management.

Hence, recognizing the complementary roles of manual analysis and technological tools, it is essential to understand how these elements interact to enhance fraud management efforts (BECKER; VOLINSKY; WILKS, 2010). Despite the richness of existing literature, a gap persists in connecting key dimensions—namely, the technologies, the professionals who use them, and the practical contexts in which they are applied. Bridging this gap may reveal underlying

challenges faced by professionals when engaging with technical tools, systems and colleagues, as suggested by our previous study (GOMES; JUNIOR; GARCIA, 2025).

1.1 OBJECTIVES

Given the aforementioned gap, this study explores the constraints and interactions within fraud management from a computer science perspective, emphasizing software tools, domain-relevant knowledge, and the role of professionals with computing expertise. The objective is to identify improvement points for both industry and academia, offering recommendations, proposing enhancements, and outlining future research directions. To achieve this, we adopt a mixed-methods approach that bridges multiple perspectives: academic literature, professional experience, and the technological tools currently available in the industry.

To guide our investigation, we define a set of three research questions, as follows:

1. What technological tools and software features are currently employed in fraud management, and what challenges are associated with their practical use?

2. What computer science knowledge is relevant to professionals working in fraud prevention and investigation, and how is this knowledge acquired or applied in practice?

3. How do fraud management professionals perceive collaboration with computer science experts?

These three research questions are designed to uncover insights that can help both academic and industry new discoveries and led to new practices in fraud management segment. Question 1 aims to identify the main software tools and features currently adopted in the field, along with the practical limitations faced by their users. Answering it will help uncover gaps, offering opportunities for future software development, research, and evaluation. Question 2 investigates which areas of computer science are most relevant to fraud professionals, and how this knowledge is acquired or lacking in current practice. Findings from this question are expected to inform educational programs, training initiatives, and interdisciplinary collaborations. The last question, number 3, seeks to understand how fraud management professionals perceive collaboration with computer science experts, with a focus on the challenges that hinder effective integration between technical and non-technical roles. Insights from this question will support the design of more inclusive systems, improve documentation and communication

practices, and foster more effective teamwork across disciplines. Together, the answers to these questions aim to promote a more integrated, practical, and human-centered approach to fraud management, while also identifying opportunities for innovation, training, and future research.

1.2 STRUCTURE

This study is structured to guide the reader through the complex landscape of fraud management from both technical and professional perspectives. It begins with the foundational background in Chapter 2, which establishes the key concepts and frameworks relevant to the field. Building on this foundation, Chapter 3 reviews prior work that informs and contextualizes our investigation. Chapter 4 then outlines the mixed-methods approach adopted in this research, integrating insights from literature, industry tools, and professional experience. The results of this investigation are presented in Chapter 5, followed by a critical discussion in Chapter 6 that connects the findings to the research questions. Finally, the study concludes with Chapter 7, where we offer final reflections, practical recommendations, and directions for future research.

2 BACKGROUND

As a prerequisite to understanding the complexities of fraud management discussed in the introduction, this chapter establishes a foundational overview of key concepts relevant to this research. It begins by addressing core aspects of fraud management and cybersecurity, followed by an examination of representative frameworks from both domains.

2.1 FRAUD MANAGEMENT

According to (CIMA, 2009), the definition of fraud has a variety of meanings. In general, it involves gaining an unfair advantage through the misrepresentation of facts. Examples of fraud include corruption, theft, money laundering, and extortion. While there are many forms of fraud, this work focuses on digital fraud — also known as e-crime or computer fraud. It occurs when technology is used to facilitate or commit criminal activities (CIMA, 2009; HUTCHINGS, 2013).

Some types of external and internal fraud are:

- **Asset Misappropriation** is a type of occupational fraud in which an individual (typically an employee) steals or misuses the organization's assets for personal gain. It is the most common category of fraud and often involves small but repeated thefts that can accumulate to significant losses over time (CIMA, 2009);
- **Fraudulent statements** refer to the intentional misrepresentation or omission of material information in financial reports, records, or communications with the aim of deceiving stakeholders and presenting a false picture of an organization's financial health or performance (CIMA, 2009);
- **Corruption** refers to the abuse of entrusted power for personal gain, typically involving a breach of duty by employees or officials in exchange for improper benefits. It is one of the three primary categories of occupational fraud, alongside asset misappropriation and fraudulent statements (CIMA, 2009);
- **Phishing** — A cyberattack method that involves tricking individuals into revealing sensitive information by impersonating trustworthy entities through deceptive emails, websites, or messages (STANIKZAI; SHAH, 2021).

- **Social Engineering** — A broader manipulation technique that exploits human psychology rather than technical vulnerabilities to gain unauthorized access to systems, data, or physical locations. It includes tactics like impersonation, pretexting, baiting, and tailgating Wang, Sun and Zhu (2020).

- **Account Takeover (ATO)** — A type of identity fraud in which an attacker gains unauthorized access to a user's online account, typically through credential theft or phishing. Once inside, the attacker can perform malicious activities such as changing account details, initiating transactions, or stealing data (HUTCHINGS, 2013).

- **Fake Account** — A fraudulent or artificially created user profile designed to impersonate a real individual or entity, or to operate under a fictitious identity. Fake accounts are commonly used in online platforms to carry out malicious activities such as spreading misinformation, conducting scams, manipulating public opinion, committing fraud, or bypassing platform restrictions. They may also be employed in conjunction with other attack vectors, such as social engineering or account takeovers(HUTCHINGS, 2013).

- **Mule Account** — A bank or digital account used to transfer illegally acquired funds, often operated by individuals (sometimes unknowingly) recruited by fraudsters. These accounts are used to obscure the origin of illicit money and facilitate money laundering schemes (HUTCHINGS, 2013).

While identifying these different types of fraud is essential, effective management also requires a deeper understanding of the psychological and contextual factors that lead individuals to commit them. To that end, we turn to Cressey (1953) Fraud Triangle, a foundational model for understanding these motivations.

2.1.1 The Fraud Triangle

To understand why individuals commit crimes, we turn to Cressey (1953) study, which identified three key motivating elements: pressure, opportunity, and rationalization, as illustrated in Figure 1. Pressure often stems from situations that destabilize individuals, consequently increasing their vulnerability to illegal acts. This can appear in various forms, such as urgent financial needs or overly ambitious corporate targets.

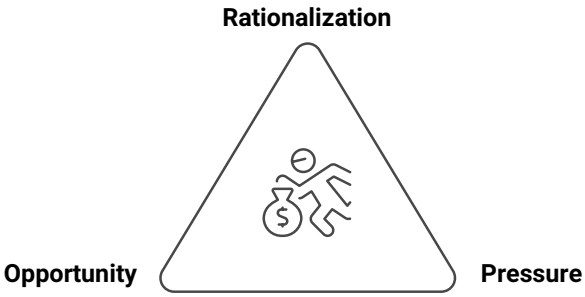


Figure 1 – Fraud triangle Cressey (1953)

Opportunity then presents itself when a pressured individual finds favorable conditions that allow them to act, such as security gaps or weak oversight. Lastly, rationalization serves as a psychological mechanism, enabling individuals to justify their actions and lessen any accompanying guilt. This might involve downplaying the impact of illicit behavior on large financial institutions or blaming unrealistic goals.

The "Fraud Triangle"model remains a fundamental framework for contemporary studies on organizational and ethical crimes, offering a systematic lens through which to understand underlying psychological and contextual dynamics. As fraud increasingly shifts to digital environments, understanding how to close the 'opportunity' gap, particularly through robust digital defenses, becomes paramount. This is where Cybersecurity plays a critical role.

2.2 CYBERSECURITY

Building upon the understanding of the motivations behind fraud provided by the Fraud Triangle, we now turn our attention to the critical field of cybersecurity. As a relevant area within Computer Science, it encompasses principles, technologies, and organizational practices aimed at protecting digital systems and networks from unauthorized access, misuse, and actions that conflict with the legitimate rights of data owners and users. It promotes the responsible and lawful use of digital resources in accordance with established legal and ethical frameworks (CRAIGEN; DIAKUN-THIBAULT; PURSE, 2014). Its relevance has become even more evident as fraud increasingly shifts to digital environments. In parallel, the widespread availability of AI tools has lowered the barrier for fraudsters to automate and enhance their methods, leading to more frequent and sophisticated attacks (CIFAS, 2025). The strong connection between this domain and fraud prevention is also emphasized in (TARIQ et al., 2024).

In this context, there is many types of cyberattacks that mainly affect the banking indus-

try, as well as it can also affect others sectors. Summarized by (STANIKZAI; SHAH, 2021) and illustrated in Figure 2, these attacks take multiple forms, each exploiting specific vulnerabilities to compromise systems and data. Malware and ransomware are used to hijack systems and demand ransom payments, often resulting in significant financial losses. Phishing attacks deceive users through fraudulent emails, frequently delivering malware via trusted platforms. Supply chain and third-party attacks exploit external dependencies by distributing malicious updates or components. Endpoint attacks target user devices connected to cloud services, leveraging the growing digital infrastructure. In man-in-the-middle attacks, attackers intercept communication between two parties to steal or manipulate information. Finally, DoS - Denial-of-Service attacks overwhelm systems with traffic, rendering them inaccessible to legitimate users.

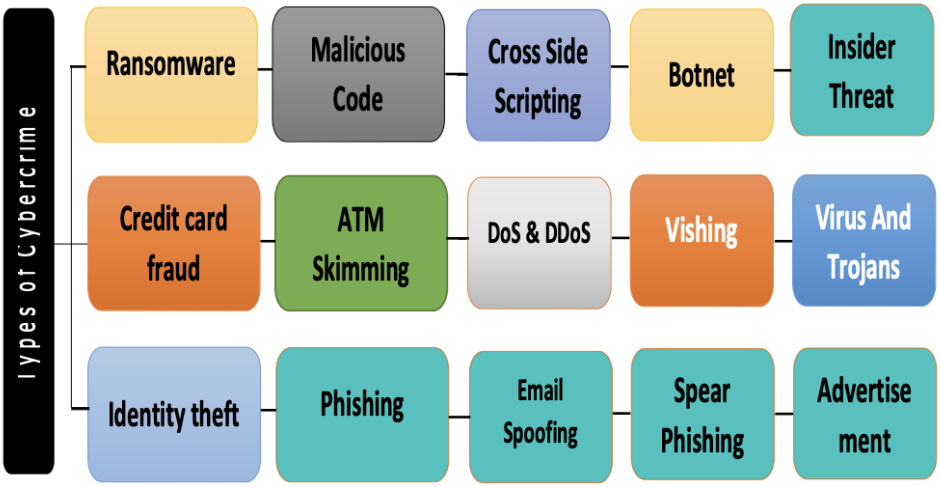


Figure 2 – Threats in Banking Systems by (STANIKZAI; SHAH, 2021)

However, effective Cybersecurity is not solely a technical endeavor; it is fundamentally guided by a robust legal and regulatory framework that mandates data protection and security practices.

2.3 LAWS, REGULATION AND STANDARDS FOR PRIVACY, SECURITY AND COMPLIANCE

Building on the importance of cybersecurity measures, this section delves into the key laws, regulations, and standards that define the legal and ethical boundaries for handling personal data, ensuring digital security, and maintaining compliance across both public and private sectors. It aims to provide a foundational understanding of the regulatory landscape that underpins fraud prevention, data protection, and information systems management. These

laws and standards were mentioned during the data collection phase of this research; therefore, it is important to provide an overview of their scope and relevance.

- **GDPR** – *General Data Protection Regulation* – Regulation by the European Union for data protection and privacy for individuals (The European Parliament and of the Council, 2016).
- **HIPAA** – *Health Insurance Portability and Accountability Act* -U.S. law that provides data privacy and security provisions for safeguarding medical information (U.S. Department of Health and Human Service, 2013).
- **FCPA** – *Foreign Corrupt Practices Act* – U.S. law prohibiting companies from bribing foreign government officials to gain business advantages (U.S. Department of Justice, 2025).
- **PSD2** – *Revised Payment Services Directive* – European regulation aimed at increasing competition and security in electronic payments (The European Parliament and of the Council, 2015).
- **PCI DSS** – *Payment Card Industry Data Security Standard* – A global standard for organizations that handle branded credit cards, designed to protect cardholder data (PCI, 2024).
- **ISO 27001** – *International Organization for Standardization - 27001* – An international standard for information security management systems (ISO, 2013).
- **eIDAS** – *Electronic Identification, Authentication and Trust Services.* – EU regulation establishing standards for electronic identification and trust services for electronic transactions (The European Parliament and of the Council, 2014).
- **SOX** – *Sarbanes-Oxley Act.* – U.S. federal law that sets requirements for public company boards, management, and public accounting firms, primarily related to financial reporting and internal controls (CIMA, 2009).
- **FinCEN** – *Financial Crimes Enforcement Network.* – A bureau of the U.S. Department of the Treasury that collects and analyzes financial transactions to combat money laundering, terrorist financing, and other financial crimes (U.S. Department of the Treasury, 2025).

- **LGDP** – *Lei Geral de Proteção de Dados Pessoais.*– The Brazilian data protection law was established to safeguard fundamental rights related to individual freedom, privacy, and personal development. It regulates the processing of personal data by both public and private entities. The law encompasses a broad range of data processing activities, which may be carried out through manual or digital means (Brasil, 2018).

To translate these requirements and the principles of cybersecurity into actionable, systematic practices, organizations often adopt frameworks, which provide practical guidance for implementation. It is these frameworks that will be explored in the subsequent section, providing a practical lens through which to understand the application of these legal and technical safeguards.

2.4 FRAMEWORKS FOR MANAGING RISK, FRAUD AND CYBERSECURITY

Following the overview of regulatory requirements in the previous section, this section presents a selection of frameworks related to managing risk, fraud, and cybersecurity. These frameworks vary in origin, with some developed by regulatory authorities and others by certification bodies and industry consortia. Our analysis is primarily structured around the framework proposed by Wilhelm (2004) to facilitate comparison with Soomro et al. (2019)'s approach. Additionally, other relevant frameworks, such as the National Institute of Standards (of U.S) (NIST) Cybersecurity Framework and the Cybersecurity Color Wheel, emerged during our data collection and offer complementary perspectives; it is therefore important to briefly introduce these before detailing our methodology and data.

2.4.1 The Wilhelm Fraud Management Cycle

The Wilhelm (2004) Fraud Management Cycle consists of eight fundamental stages. As Figure 3 illustrates, this cycle provides a overview of fraud management, specifically highlighting the integral support provided by technology and fraud-prevention specialists across its various phases. Each of these stages plays a distinct role in the ehensive fraud management process, beginning with Dissuasion.

Deterrence aims at discouraging fraudsters from developing the desire or intention to commit fraud. Within Cressey (1953)'s theory, this entails minimizing the 'opportunity for

fraud' within the company. One way to achieve dissuasion is by educating consumers about scams, training company employees and third parties about security, and increasing criminals' fear of the consequences of their actions (SPERDEA; ENESCU; ENESCU, 2011; DORMINEY et al., 2012; IJEOMA; ARONU, 2013).

Figure 3 – The Wilhelm (2004) Fraud Management Cycle

Following dissuasion, the cycle proceeds to the **Prevention** stage, which focuses on creating initial barriers to prevent fraudsters from carrying out illegal transactions. These barriers can be technological, such as multi-factor authentication, encryption, and real-time blocking systems, or organizational, like robust internal controls and segregation of duties (DEVOS; PIPAN, 2009). The third stage in the cycle is **Detection**, which takes place after a fraud has been initiated—once prevention measures have failed to deter it. Various mechanisms can be employed to detect fraud; however, Becker, Volinsky and Wilks (2010) underscores the importance of cooperation between advanced technologies and the expertise of qualified professionals in analyzing suspicious transactions.

Once an irregularity has been identified, the process moves to the **Mitigation** stage, aiming to stop the fraud and/or reduce the resulting damage Wilhelm (2004). It is significant that harm extends beyond financial losses; a fraud can also damage a company's reputation and weaken customer trust. Examples of mitigation methods include blocking or canceling the suspicious transaction, requesting additional personal documents, and making calls to verify the customer's identity, among other measures (SOOMRO et al., 2019). Following the Mitigation stage, the cycle moves to the **Analysis** phase. Here, problems and potential improvements to processes and tools are examined, a stage Wilhelm (2004) identifies as key for preventing repeated incidents and enhancing the effectiveness of anti-fraud operations. Data analysis tools are valuable allies during this process (MIRI-LAVASSANI et al., 2009).

Following the Analysis stage, the cycle advances to **Policy** implementation, which involves establishing the standards a company adopts to prevent fraud and protect both itself and its employees. A lack of anti-corruption and compliance policies can lead to serious issues

(VERDON, 2006). Notably, the anti-fraud policy should be continuously reviewed and updated as new cases arise.

Finally, the **Investigation** and **Prosecution** stages are sequential: during investigation, evidence is gathered that may be used to convict perpetrators in the prosecution phase. In both stages, it is possible to identify opportunities to improve the overall process.

2.4.2 The NIST Cybersecurity Framework

Having detailed the Wilhelm cycle's process-oriented approach to fraud management, we now turn to the NIST Cybersecurity Framework. As one of the additional frameworks identified during our research, it offers a different perspective centered on continuous Cybersecurity functions rather than the sequential stages of a fraud incident. This framework is particularly significant due to its widespread adoption by companies and government organizations in the United States.

The National Institute of Standards and Technology, or NIST, is a U.S. government organization. This institute is responsible for various important activities, including the development of standards. One of its key contributions is the Cybersecurity Framework , an important standard, as it is adopted by many American companies and government organizations (National Institute of Standards and Technology, 2024). Additionally, it offers accessible communication for non-technical teams and supports multiple languages for international reach.

The NIST Cybersecurity Framework is structured around what it calls 'core functions': Govern, Identify, Protect, Detect, Respond, and Recover. These functions are organized in a wheel, as shown in Figure 4, and serves to connect them into a single strategy for a company. Beyond these core functions, the framework further specifies categories that define the specific steps each function should follow to accomplish its objectives. A closer examination of these functions follows.

The framework begins with the **GOVERN** function, which leads enterprise risk management by defining the company's strategy, including roles, responsibilities, and, significantly, policies. Once this strategy is established, the organization's assets must be identified and mapped—a task for the **IDENTIFY** function. During this step, risks are uncovered and prioritized according to the security guidelines defined in the first function. Opportunities for improvement in policies, documents, and procedures may also be identified, further strengthening the company's safety. Following identification, the **PROTECT** function is responsible

Figure 4 – National Institute of Standards and Technology (2024) framework

for the action plan to prevent or avoid exposures. To achieve these goals, the company should adopt security mechanisms such as identity management and access control.

The subsequent function is **DETECT**, aiming to accelerate the discovery and analysis of problems through the use of metrics, dashboards, alarms, and other tools. Following detection, the framework concludes with the **RESPOND** function, focused on taking action to stop incidents, and the **RECOVER** function, dedicated to restoring services and minimizing negative effects.

2.4.3 The Cybersecurity Color Wheel

Having explored the NIST Cybersecurity Framework's functional approach to managing digital risks, it is also important to consider frameworks that emphasize the human and collaborative dimensions of cybersecurity. The Cybersecurity Color Wheel, introduced by Wright (2017), is widely adopted in the industry to bridge the gap between security teams and software developers. This framework addresses the common challenges where developers often prioritize functionality and delivery over security aspects in the software they build. To address these challenges, the framework proposes a set of specialized roles, each with a distinct function. As depicted in Figure 5, these roles are further explored in the subsequent discussion.

- **Blue Team** focuses primarily on defensive measures, including important activities such as incident response, threat detection, operational security, and digital forensics. As

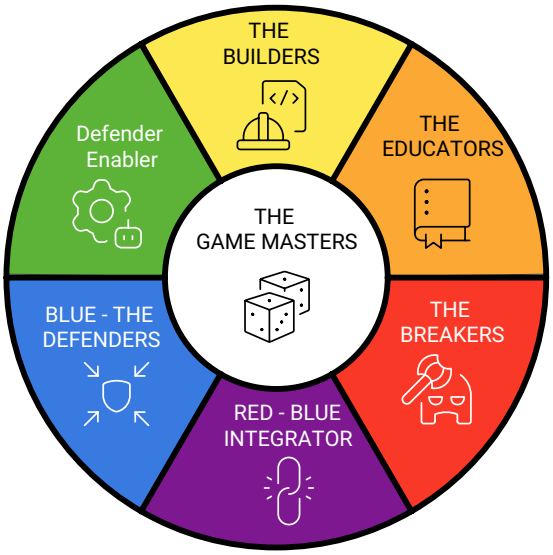


Figure 5 – The Cybersecurity Color Wheel. **Source**: Author's adaptation from Wright (2017).

'The Defenders,' these professionals diligently work to protect, detect, and recover from attacks.

- Complementing the Blue Team's defensive efforts, the **Red Team** specializes in offensive security operations. Simulating attacks through activities like penetration testing, black-box testing, social engineering, and vulnerability scanning, these professionals primarily aim to identify weaknesses in systems and applications. Dubbed 'The Breakers,' they emulate adversaries, challenging the resilience of security defenses established by the Blue Team.

- Serving as the 'Red-Blue integrator,' the **Purple Team** directly bridges offensive and defensive strategies. Aiming to maximize the value of Red Team exercises, they utilize results to strengthen Blue Team defenses. This team actively works to dismantle disconnected teams between attack and defense roles, thereby enhancing overall organizational security maturity.

- The **Yellow Team** comprises the 'builders', software developers, architects, and programmers, representing traditional software engineering practices. Focused primarily on building functional, correct, and efficient software, their development mindset often overlooks integrated security. This creates a gap that the framework aims to address through

collaboration with other teams.

- Known as 'The Educators,' the **Orange Team** operates at the intersection of the Red and Yellow teams. They primarily educate developers (Yellow Team) using offensive findings (from Red Team activities). Beyond merely patching vulnerabilities, their objective is to explain how and why these issues occur, empowering developers to internalize security within their acceptance criteria for software.

- The **Green Team** integrates the Yellow and Blue teams by enhancing code-level defenses. They achieve this by directly embedding logging, monitoring, forensics capabilities, and incident response readiness into the software. This integration enables developers (Yellow Team), informed by defenders (Blue Team), to adjust and improve systems for more effective detection and investigation efforts.

- The **White Team**, serving as 'The Game Masters,' functions as a neutral coordinator for all other teams. Their direct role involves establishing clear parameters for team interactions and activities (known as rules of engagement), organizing operations, and monitoring overall team dynamics. Comprised of members such as compliance officers, managers, and analysts, this team ensures structured and productive collaboration across the entire framework

2.4.4 The CIMA Risk Management Framework

Having explored frameworks that detail specific cybersecurity functions and team roles, it is also important to consider models that provide a broader, organizational perspective on risk management. The CIMA Risk Management Framework offers such a strategic view, outlining a systematic approach to identifying, assessing, and responding to risks across an entire enterprise.

CIMA stands for the Chartered Institute of Management Accountants, a global organization that offers training and qualification for accountants worldwide. As a trusted organization, CIMA in 2009 developed a framework with several key steps for risk management , as visualized in figure 6 (CIMA, 2009).

This framework's process begins with forming a risk management group responsible for coordinating efforts and aligning strategic goals based on the organization's context. This

group typically includes senior figures such as the Chief Risk Officer, finance and audit leaders, and HR representatives. Following this, the framework guides the identification of risk areas across the organization. This involves using methods such as workshops, interviews, process mapping, and peer market census to identify potential vulnerabilities. Once identified, risks are assessed considering their potential financial, reputational, and operational consequences, in terms of both impact and likelihood (i.e., probability of occurrence). This assessment evaluates risk at two levels: gross risk (before any controls or mitigation are applied) and net risk (after controls and mitigation strategies have been implemented). Guided by their defined risk appetite and operational conditions, organizations develop response strategies such as risk avoidance, reduction, retention, or transfer.

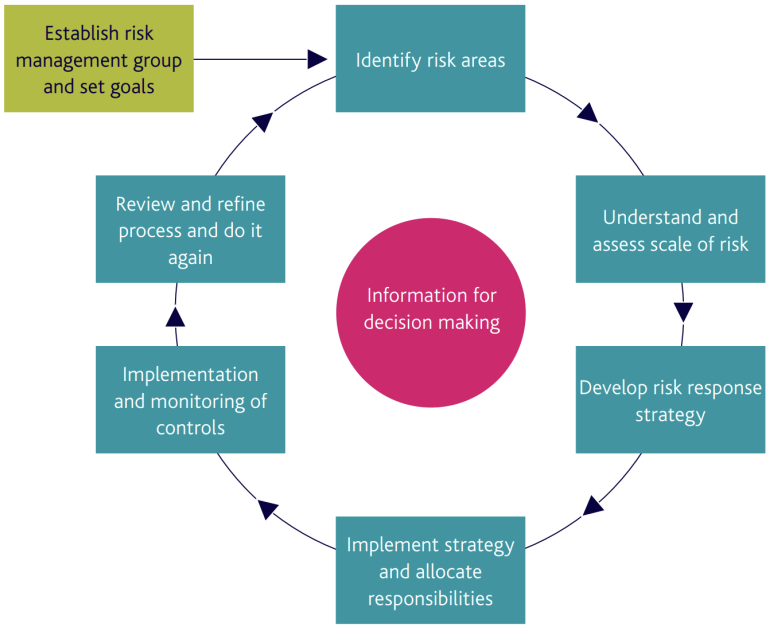


Figure 6 – CIMA Risk Management Framework

The next stage focuses on implementing the chosen risk strategies and assigning well-defined responsibilities for their execution, with defined timelines and clear lines of accountability. Such effective execution requires strong engagement across all organizational levels, particularly from senior leadership. To ensure ongoing relevance, organizations must continuously monitor and evaluate controls, adjusting them in response to evolving internal or external conditions; this can be achieved through various mechanisms, including reviews, assessments, or structured feedback tools. The process concludes with a review and refinement phase, which contributes to its ongoing improvement. By incorporating lessons learned, organizations

strengthen subsequent cycles and embed the discipline of risk management as a sustained, organization-wide practice that enhances resilience and strategic alignment.

2.4.5 Discussion

Having detailed the individual characteristics of various risk, fraud, and cybersecurity management frameworks, we will now proceed with a comparative discussion of their distinctions and complementarities.

In this subsection, we begin discussing the frameworks examined throughout this study. Our analysis began with the framework proposed by Wilhelm (2004), which initially appeared to be the most complete. However, despite its broad scope, it lacks specific details that are addressed more effectively by other frameworks. These complementary aspects are summarized in Table 1. Specifically, the table's first column presents each stage of the Wilhelm (2004) framework, while the second lists complementary frameworks along with a justification of how each contributes to or enhances the corresponding stage.

This analysis reveals both distinctions and complementarities among the frameworks, highlighting the potential benefits of a hybrid approach that combines their respective strengths. Our analysis began with the framework proposed by Wilhelm (2004), which initially appeared to be the most complete. This 2004 framework emphasizes fraud-specific operational workflows, presenting a pragmatic sequence of stages. It is highly applied and transaction-focused, commonly adopted in financial and compliance settings. However, it is important to note that Wilhelm (2004)'s framework predates the widespread influence of digital technologies on fraud, which may limit its direct applicability to contemporary e-crime without adaptation. In contrast, the NIST Cybersecurity Framework (CSF) offers a broader and more technically oriented structure for managing cybersecurity risks, organized around five continuous functions. The CSF's primary strength lies in guiding organizational resilience through policy formulation and technical safeguards; however, it lacks detailed guidance for fraud investigation and legal procedures.

Moving further into the comparative analysis, the Cybersecurity Color Wheel takes a unique approach, structuring the landscape around collaborative roles and responsibilities. Rather than focusing on stages or controls, it emphasizes the people and interactions that ensure security coverage by bridging cultural and operational gaps between security teams and development teams. The CIMA, finally, is rooted in enterprise governance and strategic alignment. It follows

Wilhelm stage	Connected Frameworks	Connection Points
Deterrance	Color Wheel	The Color Wheel's Orange Team promotes deterrence through educating individuals and fostering security awareness,
	CIMA	whereas CIMA's risk strategies aim for prevention at a broader, management-level to mitigate various fraud types.
Prevention	Color Wheel	Color Wheel teams (Green, Red, Blue, Purple) contribute to fraud prevention through role-specific actions and collaboration,
	NIST	while NIST's framework emphasizes uncovering and managing risks proactively before incidents occur.
Detection	Color Wheel	While the Green and Blue teams assist in detection and mitigation through human expertise and integrated code-level defenses,
	NIST	NIST's DETECT function primarily emphasizes leveraging technological and analytical capabilities for problem discovery.
Mitigation	Color Wheel	Green and Blue teams facilitate mitigation through team-driven response and integrated defenses,
	NIST	whereas NIST's RESPOND and RECOVER functions encompass a broader focus on immediate reaction, recovery after incidents, and service restoration.
Analysis	NIST	NIST accelerates risk and fraud analysis through technical tools under its DETECT function,
	CIMA	while CIMA's analysis is geared towards strategic policy refinement to reduce overall risk exposure.
Policy	Color Wheel	The Color Wheel's White Team focuses on team-specific policy protection and enforcement,
	NIST	whereas NIST's GOVERN function defines overall organizational risk appetite, roles, and high-level policies.
	CIMA	CIMA, conversely, frames policy as a strategic goal for reducing risk exposure.
Investigation	–	No direct mapping identified in the frameworks.
Prosecution	–	No direct mapping identified in the frameworks.

Table 1 – Integrating Fraud Management with Security and Risk Frameworks

a cyclical logic emphasizing top-down management of organizational risk appetite and policy enforcement, rather than operational detection or response.

Despite their differing perspectives, all frameworks acknowledge the cyclical nature of risk and security. Wilhelm (2004), NIST, and CIMA explicitly organize their stages in loops of continuous improvement. NIST and CIMA both prioritize the role of governance and policy, while Wilhelm (2004) and NIST include detection and mitigation stages. All four frameworks implicitly or explicitly emphasize the need for cross-disciplinary collaboration, which is the core principle of the Color Wheel. Why not create a hybrid framework?

2.5 ENDING OF CHAPTER

In conclusion, this chapter has demonstrated that the domains of fraud prevention and cybersecurity, while distinct in scope and methodology, exhibit significant complementarities

that underscore the need for an integrated and multidimensional approach. The frameworks analyzed, spanning operational, managerial, and technical paradigms, contribute unique perspectives to the understanding and mitigation of digital threats. Wilhelm (2004)'s procedural model emphasizes investigative workflows, while CIMA and the NIST Cybersecurity Framework introduce strategic and technical governance mechanisms. Additionally, the Cybersecurity Color Wheel (WRIGHT, 2017) enriches this landscape by delineating specialized team roles that foster cross-functional collaboration. Taken together, these frameworks not only reveal the complexity of contemporary fraud and security challenges but also highlight the potential for hybrid models capable of addressing these issues in a holistic, adaptive, and context-sensitive manner.

The following chapter reviews related works that inform and contextualize this study.

3 RELATED WORK

This chapter reviews the literature foundational to our study. We first detail the systematic methods employed to identify relevant works, then present a curated selection, highlighting their points of comparison and contrast with our research. We subsequently introduce two comprehensive literature reviews that emerged during our search, which further shape our methodological approach. The chapter concludes by contextualizing these works within our broader research objectives.

3.1 SEARCHING RELATED WORKS

We initiated our research with an exploratory literature analysis aimed at identifying relevant terminology to better understand the context of our study. Building upon this initial phase, we adopted the **PICOC** methodology to systematically structure our keyword selection (WOHLIN et al., 2012).

For the **Population**, we selected terms such as *expert, specialist, practitioner, investigator, analyst, consultant, auditor, examiner, detective, professional, career, and analyst*, reflecting the diverse professional profiles involved in fraud-related activities. For the **Intervention**, keywords included *computer science, computer-based, technology, software, computer, electronic, digital, and automated*, emphasizing the technological dimension of the solutions under investigation. In the **Comparison** category, we incorporated terms such as *deterrence, prevention, detection, mitigation, analysis, policy, investigation, and prosecution*, aligning with the (WILHELM, 2004) framework. The **Outcome** dimension focused on interactional and perceptual results, using terms like *perception, relationship, interaction, and collaboration*. Lastly, for **Context**, we selected domain-specific terms such as *fraud, audit, compliance, and diligence*, ensuring that the search remained grounded in the relevant thematic scope.

Subsequently, we conducted a literature search using the selected keywords on Google Scholar[1], with the primary objective of identifying prior research studies that could be related to ours. Table 2 presents a structured overview of selected studies on fraud, organized into five columns that together capture the key elements of each investigation.

[1] <https://scholar.google.com.br/> accessed on 24th May 2025

Work	Topic	Area	Method	Goal	Use of Technology
(CLEMENTS; KNUDSTRUP, 2016)	Fraud investigation procedures (general)	Forensic accounting, internal auditing	Research (survey with participants from continuing professional education meetings and national fraud conference).	Identify a set of common procedures, the most frequent ones, and those performed in (almost) all fraud investigations.	Not specified (focus on human and manual procedures).
(ZHOU et al., 2023)	Collusive fraud in health insurance	Health insurance	Visual Analytics (three-stage approach), case studies, expert feedback.	Assist health insurance audit experts in identifying suspicious groups, investigating suspect patient behavior, and validating collusive fraud outcomes.	Co-visit network, enhanced community detection algorithm, prototype system (FraudAuditor), time-scale-adapted visualizations.
(SILVA et al., 2021)	Bot Attack, Account Takeover (ATO)	Unspecified (online transactions)	User testing, real use case scenario.	Assist fraud analysts in making informed decisions and increasing effectiveness in fraud detection.	Visualization tool with three visualization models, Machine Learning (ML) for decision support.
(AL-SAYYED et al., 2024)	Mobile money transaction fraud	Mobile money services	Case study (using the PAYSIM dataset), visual and numerical analysis.	Demonstrate the importance of data visualization for initial dataset assessments, validating suitability and detecting unexpected patterns.	Multiple visualization schemes, data analysis (anomaly detection), Machine Learning (ML) for automated fraud detection.
(LEITE et al., 2018)	Anomalous event detection, financial fraud	Banks, stock markets, telecommunications, insurance companies, internal fraud	Survey (systematic review of existing approaches).	Classify different tasks and solutions, identify and propose future research opportunities in visual fraud detection.	Visual Analytics (VA) techniques, visualization techniques (heatmaps, circular representations, charts), data mining techniques.
(WEBGA; LU, 2015)	Rating fraud	E-commerce (online stores)	Real-time Visual Analytics system, case studies (simulated and real fraud scenarios).	Uncover small-scale anomalous activities in large volumes of data and detect fraud in time-critical online rating streams.	Custom streaming system (server and visual analytics interface), Singular Value Decomposition (SVD), co-mapped SVD diagram, reordered matrix representation, temporal visualization.
(CARMINATI et al., 2015)	Information stealing, Transaction hijacking, Stealthy fraud, Mixed frauds, Repeated fraud over time	Banking (online banking)	Evaluation on real data (fraud scenarios constructed with domain experts), data mining, statistical and mathematical techniques.	Analyze and investigate online banking fraud, rank transactions based on the risk of being fraudulent.	Decision support system (BANKSEALER), Histogram Based Outlier Score (HBOS), DBSCAN (Density-Based Spatial Clustering of Applications with Noise), exponential decay function.
(HOYER et al., 2012)	Insider fraud, internal threats	Auditing (accounting information systems, SAP ERP)	Design Science (generic architectural model, prototype implemented in SAP ERP test environment).	Unify classical fraud auditing with human behavior by considering the fraud triangle to improve fraud detection and prevention.	Quantitative analysis of business transactions, email text mining
(SCARPINO, 2022)	Biases, discrimination, and privacy in risk management (implications of AI and ML)	Risk management (general, applicable across industries)	Exploratory qualitative study (phenomenological approach, interviews with industry experts).	Explore issues such as biases, discrimination, privacy, risk boundaries, and moral decision-making in the implementation of AI and ML in risk management.	Artificial Intelligence (AI), Machine Learning (ML).

Table 2 – Related works found

The first column, **Topic**, identifies the specific type of fraud being examined, such as insider threats, account takeovers, rating manipulation, or ethical concerns involving artificial intelligence. Closely related, the **Area** column situates each topic within its real-world context by indicating the sector or domain in which the fraud occurs. These areas include banking, health insurance, e-commerce, cybersecurity, and general risk management. The third column, **Method**, outlines the research approach used in each case. These approaches include surveys, case studies, user testing, Design Science, and qualitative interviews. The method chosen often reflects the nature of the problem and the type of data available, with some studies drawing on real-world datasets or involving direct collaboration with domain experts.

Based on these methods, the **Goal** column describes what each study aims to achieve. Objectives range from improving fraud detection and supporting analysts in decision-making to validating the effectiveness of visualization tools or integrating behavioral theories, such as the fraud triangle, into auditing practices. Some studies also address broader concerns, including privacy, bias, and decision-making ethics in the use of artificial intelligence and machine learning for risk management. The final column, **Use of Technology**, presents the tools and techniques applied to meet these goals. These include machine learning algorithms, data mining, visual analytics systems, clustering techniques, real-time data platforms, and in some cases, manual investigative procedures. Together, the five columns offer a comprehensive view of how different types of fraud are being investigated, in which contexts, with what objectives, and using which technological and methodological resources.

3.2 ANALYSIS OF STUDIES

Starting the analysis, the studies reviewed differ significantly in scope and focus, with the notable exception of technological adoption. Only Clements and Knudstrup (2016) centers its approach on manual processes, while the others reflect a strong interdisciplinary effort to address fraud through the integration of domain expertise, methodological diversity, and technological innovation. Most investigations concentrate on financial fraud, particularly within banking, insurance, and e-commerce, while also extending into areas such as cybersecurity and ethical concerns related to the use of AI in risk management. Case studies and surveys are the most frequently employed methods, often supported by real or simulated datasets and expert input. Across the studies, the goals commonly include improving fraud detection, supporting analyst decision-making, and validating the role of visual and analytical tools.

From a technological standpoint, there is widespread use of machine learning, visual analytics, clustering algorithms, and data mining, although some approaches still incorporate human-centered or manual processes. Overall, the results suggest a clear trend toward combining automated techniques with contextual understanding to enhance fraud detection, investigation, and prevention.

Unlike our broad study, many reviewed works concentrate on specific technical solutions, surveys of current practices, or targeted aspects of fraud management. For instance, Leite et al. (2018) presents a survey of visualization techniques applied to fraud detection, classifying them by application domain, visualization method, interaction type, and analytical approach. Similarly, Clements and Knudstrup (2016) conducts an exploratory study to identify the most common procedures carried out by fraud investigators. While both studies share an analytical perspective similar to ours, their more constrained goals and scope highlight a key distinction.

On the other hand, several works emphasize system implementation and technical solutions. For example, Carminati et al. (2015) describes a decision support system for analyzing online banking fraud, employing user profiling and statistical analysis to generate interpretable outputs for analysts, while also addressing challenges such as limited data availability. In a related vein, Silva et al. (2021) introduces a tool composed of three visualization modules, designed to support fraud analysts in identifying cases of Bot Attacks (BA) and ATO. Likewise, Webga and Lu (2015) presents a real-time visual analytics system for detecting rating fraud in e-commerce, combining server-side algorithmic processing with client-side interactive analysis using diagrams, reordered matrices, and temporal views.

Several studies also highlight human factors and interdisciplinary collaboration, aligning with our third research question, which focuses on how professionals perceive collaboration with computer science experts. In this context, Zhou et al. (2023) proposes a visual analytics approach for fraud in health insurance, integrating expert knowledge into a three-stage detection system with tailored visualizations. A similar perspective is found in Al-Sayyed et al. (2024), which emphasizes the role of data visualization in the early assessment of mobile money fraud datasets, helping analysts uncover unexpected patterns before conducting deeper investigations. Finally, Hoyer et al. (2012) explicitly calls for the integration of human behavioral factors into automated audit systems. It proposes a generic architectural model that unifies traditional auditing with the analysis of user-related data such as event logs, network activity, and email content.

In summary, this study serves as a broad research initiative aimed at understanding and

advancing the current landscape of risk and fraud management by bridging academic, professional, and technological perspectives. The reviewed literature offers concrete examples, technical solutions, survey findings, and critical discussions on human factors and interdisciplinary collaboration, all of which provide valuable context and support for addressing the research questions outlined in the introduction.

3.3 LITERATURE REVIEW PAPERS

In addition to the previously mentioned studies, we identified two literature reviews that stand out for their comprehensive scope: Soomro et al. (2019) and Soltani, Kythreotis and Roshanpoor (2023). Both reviews are particularly relevant as they cover more than a decade of research and address multiple dimensions of the fraud detection field, including technological, organizational, and procedural aspects. Due to their methodological depth and broad coverage, we decided to incorporate them as part of our methodological foundation rather than treat them solely as related works. Their frameworks and findings serve as important references for shaping our analytical approach. A detailed examination of their methods and results will be presented in Chapter 4 and further discussed in the context of our findings in Chapter 5.

3.4 FINAL OF CHAPTER

This chapter provided an overview of the literature that informs and contextualizes our research. Through a systematic search process, we identified a diverse set of studies that address the fraud thematic from multiple perspectives, including technical, procedural, and human-centered approaches. The analysis highlighted both similarities and contrasts with our own study, especially in terms of goals, methods, and the use of technology. Additionally, two comprehensive literature reviews were introduced, which will serve as methodological references throughout our work. Taken together, these contributions illustrate the complexity and multidimensionality of fraud management, reinforcing the need for integrated approaches that combine domain expertise, data-driven techniques, and collaborative practices. In the next chapter, we build on these insights to present the methodological framework adopted in our study, detailing how the literature guided the design of our research questions, data collection, and analysis strategies.

4 METHOD

To achieve our objective, the practical experience of Brazilian professionals played a significant role in meeting our goals. However, relying solely on a qualitative approach could introduce biases. To address this, we incorporated a literature review to understand the academic foundation and conducted a software market census to explore practical activities in the fraud management domain. By utilizing these three data sources, we triangulated the collected data to provide stronger evidence for our findings as showed on Figure 7.

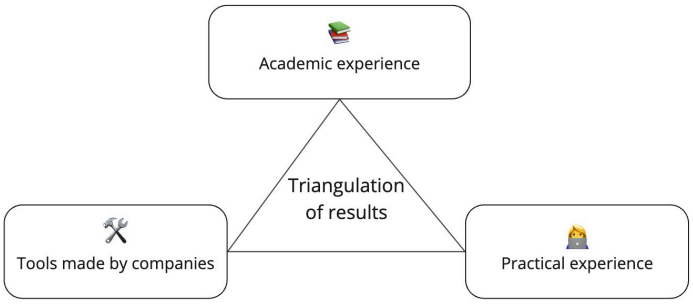


Figure 7 – Results triangulation

The next sections will describe in details the three chosen methods to compose the data collection.

4.1 LITERATURE REVIEW

For achieving the aimed goal, we based the literature analysis in the two reviews previous mentioned in chapter 3. The first work, Soomro et al. (2019), adopted the framework proposed by Wilhelm (2004) to organize their findings, aligning with the same structure employed in our market census. While the second, Soltani, Kythreotis and Roshanpoor (2023), categorized their results into four thematic groups: fraud detection techniques, causes and deterrence of Financial Statement Fraud (FSF), computer and online transaction fraud, and auditors' fraud-related responsibilities. These studies were utilized in two complementary ways: first, to examine their interpretations and thematic analyses of the existing literature; and second, to identify potentially related works aligned with our methodological approach. Both the reviewed studies and our own analysis will be examined in greater detail in the Results and Related Works sections.

4.2 SOFTWARE FEATURES MARKET CENSUS

The main objective of this phase was to examine the global software market for fraud management. Rather than focusing solely on identifying the most commonly used tools, the priority was to spotlight the functionalities that appear most frequently among them. By concentrating on these recurring functionalities, the findings can be compared more effectively with the data collected in subsequent steps.

4.2.1 Research Setting

The strategy employed was a repository mining to gather insights from industry. We chose this approach to contrast the academic experience, getting a comprehensively result. We began the process locating a trustworthy and authoritative source to collect information about the relevant software options. After careful deliberation, we chose Gartner Peer Insights[1] as our primary resource. Gartner is a reputable and specialized organization in the field of software reviews, relied upon by numerous large enterprises worldwide for its comprehensive evaluations. One of its key advantages is that it caters directly to enterprise-level concerns, offering insights that go beyond basic functionality — such as details on scalability, integration, and the availability of long-term support. By leveraging this platform, we ensured that the information gathered was both credible and highly applicable to our analysis. Despite the need of feedback to fully ensure the reliability of our findings, the use of a trusted platforms to extract the information can provide a high quality data.

With the data source, we defined the criteria we would use to select the categories, software and services.

1. Is it useful in any category of the Fraud Management Cycle?
2. Could it be somehow be employed by Cybersecurity, compliance or fraud management teams?
3. Are the software's or service's website available ?

Then, we employed a systematic approach to identify and categorize the available software solutions and services. We started by filtering through every relevant enterprise software

[1] <https://www.gartner.com/peer-insights>. Accessed on 24th May 2025.

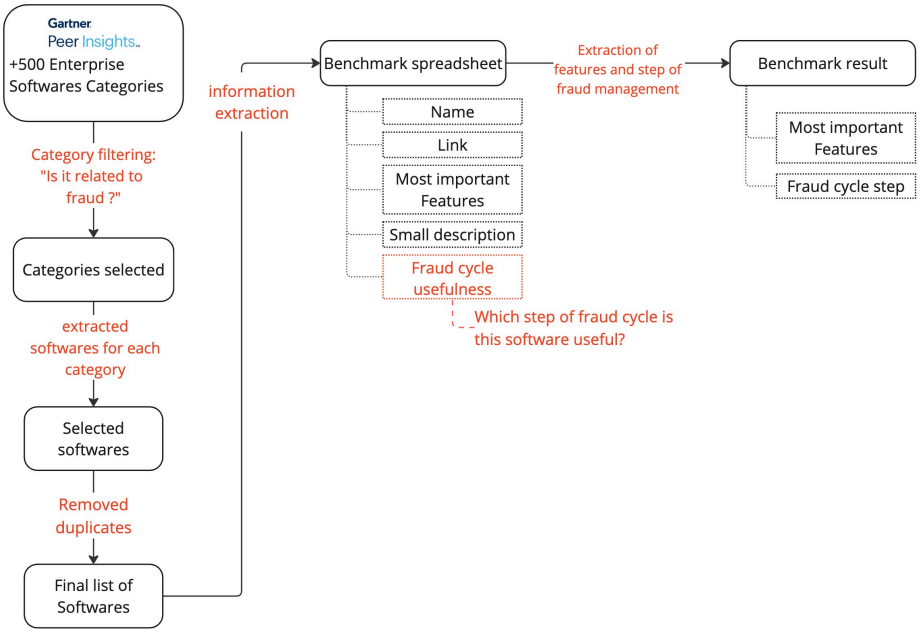


Figure 8 – Market census strategy

category that could potentially connect with fraud management, ultimately honing in on 61 distinct categories. From each category we then gathered the first twenty software, and then, removed any duplicates to prevent overlap and the ones with empty description. At the end of this work, we had the list of categories with 903 selected items, at appendix 8.

Using the help of Chat GPT[2], we retrieved the functionality of each software with the prompt shown in 3. We had done the first ten software's functionality and services list manually to compare the results with the GPT, concluding the results were very near, we continued to retrieve the other. Manually, we spent 10 minutes to retrieve one software, thus, the GPT help was crucial for this research. We reviewed the results and adjusted some of them (something about 20 items; less than 0.3% of the total).

Go to <software> website and return the main functionality of it.

Table 3 – Prompt used to return the functions information

In the next step, we joined all functionalities and services by its category, creating a list of features per categories. Then, we manually reviewed excluding the duplicates. Finally, we step into the results, understanding their fraud management step usability.

During the whole process, annotation were taken by the researchers and will be present in results' section.

[2] <https://chat.openai.com/>. Accessed on 24th May 2025.

4.3 SURVEY WITH PROFESSIONALS

For this step, the study employed a basic qualitative approach, using synchronous online interviews as the primary method for collecting empirical data from participants. It is important to note that the research was submitted to an ethics committee and received approval prior to conducting any interviews. Data were gathered online, according to each participant's preference. The two main software options offered were Google Meets[3] and WhatsApp[4], along with conventional mobile phone calls over the internet.

4.3.1 Sample of Participants

In this research, we chose not to use representativeness saturation due to certain limitations, which will be detailed in the Limitations Section. Due to the nature of this theme (Fraud), the interest of people to be interviewed was also followed by mistrusting (even presenting the documents of the University and Ethics Committee). This fact limited the number of participants who accepted to be interviewed about their routines. Even so, we still could capture some important information to contrast and compare with the other methods' data.

Thus, our strategy was to select a limited number of specific professionals to cover all stages outlined by (WILHELM, 2004) from various perspectives. Figure 9 illustrates how each step is covered. We conducted six interviews in total, distributed as follows:

- 2 Professionals that work in companies as Fraud Managers
- 2 Professionals that work in companies as Policy & Compliance Auditors
- 2 Professionals that work in the Police as Fraud investigators

It is important to note that are some intersections between them; e.g.: Fraud Managers and Police investigators have some complementary activities or even similar, acting in the same stages but with different roles. We also introduced exclusion criteria to ensure that participants could provide meaningful insights. The following were excluded:

- Professionals without relevant experience (fewer than six months)

[3] <https://meet.google.com/>. Accessed on 24th May 2025.
[4] <https://www.whatsapp.com/>. Accessed on 24th May 2025.

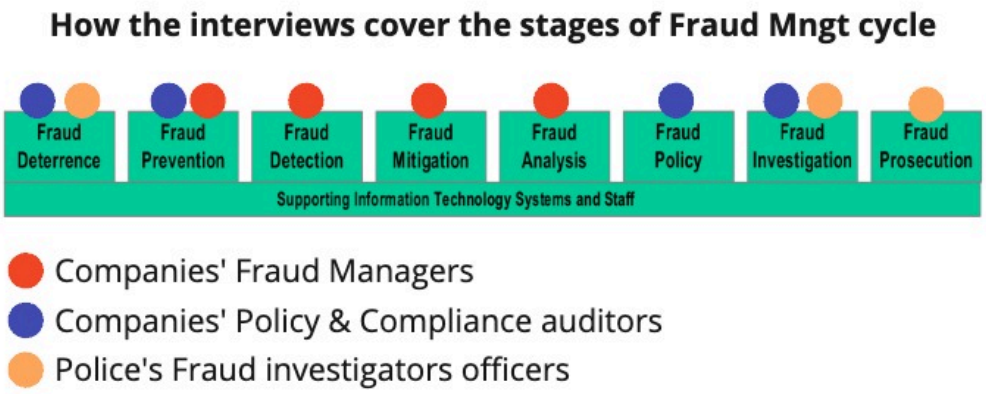


Figure 9 – Interview Coverage. **Source**: Authors

- Professionals who only supported fraud specialists but did not work directly in the area (e.g., software developers)
- Individuals who did not speak Portuguese fluently
- Those who did not have at least six months of relevant fraud experience in Brazil
- Minors under 18 years old

4.3.2 Recruitment of Participants

Invitations were distributed through text messages on *WhatsApp*, *Instagram*[5], *LinkedIn*[6]. *Accessed on 24th May 2025.*, and email. Additionally, the researchers maintained connections with professional communities in the field and requested permission to share the invitation there. Interested individuals sent a message to one of the researchers' contacts, where they received detailed instructions about the study. It was essential to emphasize that interested individuals only became volunteers after they accepted the terms of free and informed consent. Subsequently, an interview was scheduled according to the time and platform chosen by each volunteer.

[5] <https://www.instagram.com/>. Accessed on 24th May 2025.
[6] <https://www.linkedin.com/>

4.3.3 Data Collection Instruments and Procedures

Before data collection, participants were informed about the terms of the study (which can be located on appendix B) and were given the opportunity to clarify any doubts. Our interview script was made based on our objectives and restrictively following the ethics committee instructions, the full script is available at appendix C, Portuguese only. If recording was authorized, a recording app on a device dedicated to the research was used. Data were transcribed using Google's artificial intelligence service[7], and the audio files were deleted from the cloud as soon as the transcription was saved locally on the analysis computer. The transcription was then reviewed, and the data were anonymized as follows:

1. Removal of any personal information from the transcripts, including participants' and third parties' names.

2. Substitution of direct references to individuals, companies, platforms, or other entities with generic terms, such as "mentioned company."

3. Exclusion of excerpts that, even after removing names, could lead to the identification of individuals, companies, or platforms.

4. Use of additional measures, if necessary, to ensure the complete anonymization of data and protect the privacy of participants and any third parties involved.

4.3.4 Analysis

The interview, once transcribed and anonymized, was collaboratively coded by pairs of researchers to minimize bias. Initially, an open coding process was conducted, where the text was read repeatedly to identify key elements. These open codes were then reviewed and discussed among the researchers, organized into broader categories, and further refined into main groups repeatedly until making them ready for triangulation analysis.

[7] <https://console.cloud.google.com/speech/transcriptions/>. Accessed on 24th May 2025.

4.4 DATA TRIANGULATION

To ensure the robustness and credibility of the findings, this study adopted a methodological triangulation strategy that integrated data from three distinct sources: a literature review, a software feature market census, and semi-structured interviews with professionals. Each source was first analyzed independently to extract relevant themes related to fraud management and the role of computing, including technology usage, human expertise, training, data analysis, compliance, and workflow integration. Subsequently, the results were cross-compared using these emergent thematic axes to identify convergences, contrasts, and gaps. This comparative process allowed for the validation of consistent findings across sources—such as the relevance of identity verification and the need for cross-functional integration, while also highlighting critical mismatches; such as the availability of advanced automated tools in the market versus their limited practical use. By aligning theoretical, technical, and experiential perspectives, the triangulation enhanced the comprehensiveness and contextual sensitivity of the analysis.

4.5 ENDING OF CHAPTER

This chapter presented the data collection process, which was conducted through three complementary approaches: academic knowledge (via the literature review), market knowledge (through software analysis), and the practical experience of professionals from diverse specialties (through interviews). This combination aims to provide a 360-degree perspective that, despite its limitations, offers an initial overview of both the systems in use and the multidisciplinary skills required by these professionals. Additionally, it highlights key challenges from three different viewpoints, pointing to areas where we, in the field of computing, need to improve. The results of this data collection, as well as the triangulation process, will be detailed in the following chapter. It is important to note that the limitations of this methodology, along with the threats to validity, will be discussed in the final chapter of this dissertation.

5 RESULTS

This section presents the results of our study as a foundation for the subsequent discussion. We begin by examining each set of results individually to establish a clear understanding of their distinct contributions. Following this, we explore the integrated findings, highlighting the connections, divergences, and complementarities among them.

5.1 ISOLATED RESULT

In the following pages, we present the isolated results obtained from each of the three data collection methods employed in this study: the literature review, software analysis, and professional interviews. Each subsection details the data gathered, the analytical approach used, and the specific findings derived from that method. By examining each source independently, we aim to preserve the unique contributions and contextual nuances that each perspective offers. This segmented analysis not only highlights the strengths and limitations inherent to each method but also provides a solid foundation for the integrated discussion that follows in Section 5.2. Understanding the individual insights in isolation is essential before drawing connections across datasets, enabling a more comprehensive and coherent interpretation of the multidisciplinary aspects involved in fraud prevention, cybersecurity, and risk analysis.

5.1.1 Literature review

To support the triangulation process and enrich our analysis, we selected two literature reviews to compare with the other data collection methods used in this study. The first review, conducted by Soomro et al. (2019) is focused on fraud management and structured its findings using the framework proposed by Wilhelm (2004), which is the same organizational approach adopted in our market census. We begin by presenting their data and discussing the implications raised by their analysis. Subsequently, we examine the study by Soltani, Kythreotis and Roshanpoor (2023), which organized its results using a distinct thematic structure. Since both studies categorize their findings into analytical groupings, they offer a valuable basis for comparison in the triangulation phase of our research.

5.1.1.1 *Literature by Soomro et al. (2019)*

In this literature review, the authors focus on the online retail context with the aim of identifying fraud management practices and presenting a comprehensive set of strategies tailored to the e-tail sector. It is important to note that the study places particular emphasis on identity-related fraud, with a primary focus on external threats. This includes customer transactions and risks originating outside the organization, rather than internal processes or employee-related misconduct. In the following discussion, we direct our attention to the findings most aligned with the objectives of our study

The authors begin by noting that the existing literature tends to place greater emphasis on the phenomenon of fraud itself rather than on the processes involved in its management. Within their review, they identify three primary frameworks used to structure fraud management practices: the foundational model proposed by Wilhelm (2004), along with two subsequent adaptations, one by Shah and Okeke (2011) and another by Jamieson, Winchester and Smith (2007), both of which build upon Wilhelm's original framework. The authors proceed to structure their analysis by categorizing the findings according to the different stages of the fraud management process. Although the majority of the reviewed studies addressed more than one stage, none of them encompassed the entire process comprehensively. This observation highlights a fragmentation in the literature, where integrated approaches to fraud management remain limited. The table 4 summarizes the Soomro et al. (2019)'s research findings.

The literature on **Deterrence** emphasizes two main approaches: raising customer awareness (through actions such as educating users about risks and encouraging them to regularly review their bank statements) and fostering a fear of punishment after fraudulent acts.

Building on deterrence strategies, the literature on **Prevention** expands the scope of analysis across various industries—including healthcare, banking, and credit card services—making it the stage with the highest number of contributions. Unlike deterrence, the literature on prevention addresses both external and internal fraud. A common trend among these studies is a stronger focus on technological solutions rather than organizational practices. Key recommendations include maintaining up-to-date systems, regularly reassessing risks, particularly those related to identity theft, and providing employee training as a means to enhance fraud prevention effectiveness.

As a continuation of prevention efforts, the **Detection** phase introduces more technology-intensive approaches to identifying fraudulent behavior. Here, technology plays a central role

Stage	Key Points
Deterrence	Raising customer awareness Fostering a fear of punishment
Prevention	Keep up-to-date protection systems Reassess risks regularly (e.g., identity theft) Training fraud-related employees
Detection	Use of fraud detection systems and behavioral analysis Device and pattern recognition (e.g., demographics, history) Combine automated systems with professional insights
Mitigation	Use real-time detection systems (e.g., IP verification) Manual review triggered by automated flags Align mitigation with business processes and policies
Analysis	Identify and correct system vulnerabilities Leverage collected fraud data to identify new patterns Share data across organizations to enhance security Evaluate tools, policies, and staff performance regularly
Policy	Policies should align with business strategy Policies often focus only on InfoSec (limitation) Policies influence training, detection, and awareness
Investigation	Collaboration between internal and external investigators
Prosecution	Limited IT-related studies, but supports accountability

Table 4 – Resume of Soomro et al. (2019) literature review findings

in verifying user identity. The literature highlights the use of various tools such as fraud detection systems, behavioral analysis, device recognition, and the automated verification of identity-related patterns and factors, including demographic information, shopping history, product types, devices used, and associated addresses. Some authors emphasize the importance of integrating insights from trained professionals with automated detection systems, arguing that such collaboration can enhance accuracy and improve the overall effectiveness of fraud detection mechanisms.

Detection mechanisms feed directly into the **Mitigation** phase, where immediate action is required once suspicious activity is flagged. The literature highlights a combination of manual and automated actions. For instance, real-time detection systems (IP address verification, for example) are used to flag unusual patterns, which then trigger manual interventions such as contacting the customer and requesting additional evidence. These systems help filter transactions, allowing human reviewers to concentrate on truly suspicious cases. This approach is especially important given the high volume of online transactions and the need for rapid response. Accordingly, several studies emphasize the role of well-designed business processes and the importance of aligning mitigation strategies with organizational policies.

To ensure that all prior stages remain effective and aligned, the **Analysis** phase serves as a complementary function across the entire fraud management lifecycle. Its goal is to uncover system inefficiencies and support continuous improvement. This step often involves multiple processes, teams, and professionals. For example, risk assessments must be conducted regularly and based on emerging fraud trends. The IT department plays a critical role in identifying and correcting vulnerabilities, while organizations are encouraged to leverage their data—especially in confirmed fraud cases—to identify new fraud patterns and improve system performance. Sharing data across organizations is also recommended to foster a more secure environment and reduce operational costs. Additionally, recurring evaluation of tools, processes, and staff performance helps identify opportunities for improvement.

Guiding all these stages is the **Policy** component, which provides the foundational structure for effective fraud management. Policies are expected to align with overall business strategy; however, the literature often shows a limited focus on Information Security, which may not encompass the broader strategic objectives of a company. Well-developed policies influence several other areas of fraud management, including awareness training, detection, and prevention. Despite this, few studies mention specific software tools associated with policy enforcement.

Once policies are in place and operational activities are underway, the process advances to **Investigation**. This stage can be conducted by both law enforcement professionals and internal corporate investigators, though the literature highlights the enhanced effectiveness of collaboration between the two. The main objective is to collect and analyze evidence—a process that Soomro et al. (2019) notes can be improved through data analysis tools and techniques.

In the subsequent phase, **Prosecution**, the collected evidence is used to hold fraudsters accountable. Despite its importance, there is limited literature on IT-driven practices in this stage. One hypothesis to explain this phenomena may be the law-related theme, less explored by computer science literature.

Finally, we observed that Soomro et al. (2019) focused on identity fraud in the e-tail sector and, despite adopting one of the most comprehensive frameworks, the analysis yielded limited results. This limitation also reflects a broader challenge in classifying studies using the framework proposed by Wilhelm (2004). This highlights the framework's inherent rigidity in capturing the multi-functional and iterative nature of modern fraud tools and practices, which often transcend sequential stages. We will explore this issue further in the final results section.

5.1.1.2 *Literature by Soltani, Kythreotis and Roshanpoor (2023)*

This study provides a comprehensive review of financial FSF detection literature from 2001 to 2021, employing a hybrid approach that combines bibliometric analysis and machine learning. The authors collected 1,076 peer-reviewed articles from Scopus[1] and analyzed them through co-word analysis, frequency metrics, and Latent Dirichlet Allocation (LDA) topic modeling. The authors identified the most frequently used keywords in the literature on FSF, revealing key areas of focus within the field. Notably, anomaly detection emerged as the most prominent term, with a frequency more than twice that of the second most common keyword—a trend that has shown a marked increase since 2015. To further explore these thematic directions, the authors grouped the keywords into four clusters based on shared conceptual and methodological characteristics.

The first cluster, **Fraud Detection Techniques**, includes a variety of computational and analytical methods such as classification algorithms, artificial intelligence, time series analysis, graph mining, and visual analytics, with commonly cited techniques like random forest, decision trees, k-means, and fuzzy logic. The second context, **Causes and Deterrence of FSF**, explores the underlying motivations and models of fraudulent behavior, emphasizing concepts such as earnings management, corporate governance, the fraud triangle, and the fraud diamond. The third context, **Computer and Online Transaction Fraud**, focuses on cyber-related threats and includes terms such as digital forensics, network security, Malware, DoS - Denial-of-Service attacks, cloud computing, and online transaction risks. Lastly, the fourth context, **Auditors' Fraud-Related Responsibilities**, encompasses auditing processes and tools, including audit risk planning, analytics, standards, software, and auditor experience, with attention to the effectiveness and independence of audit committees.

We examined two major literature reviews (Soomro et al. (2019) and (SOLTANI; KYTHREOTIS; ROSHANPOOR, 2023) that provide distinct perspectives on identity fraud and its management. These reviews help frame the scope, structure, and limitations of existing research and allow for a critical comparison with our own approach. In this section, we analyze the frameworks adopted by each study, the depth of their thematic categorization, and their relevance to the broader objectives of fraud detection and prevention, particularly in the context of identity-related crimes.

The literature review conducted by Soomro et al. (2019) illustrates a recurring challenge

[1] <https://www.scopus.com/home.uri>

in fraud research: the difficulty of clearly separating stages such as detection and mitigation, as well as prevention and analysis, which often overlap in practice. The study follows all the layers proposed by the Wilhelm (2004) framework and applies it within a fraud-specific context. However, despite its methodological rigor, the analysis is highly focused on identity fraud in the e-commerce sector, which narrows its generalizability. In contrast, the second review adopts a broader and more flexible perspective, with less reliance on formal frameworks. While this allows for a wider thematic range, the discussion on fraud tends to remain superficial, listing relevant aspects without delving deeply into their mechanisms or implications. As a result, each study offers complementary contributions: one through structured depth with limited scope, and the other through thematic breadth with reduced analytical detail. These observations underscore a the gap in the literature that our mixed-methods approach aims to address, providing a more integrated perspective on fraud management by triangulating academic insights with practical and technological realities

Having concluded the discussion of the literature review, we now turn to the next stage of data analysis in our research.

5.1.2 Software feature market census

A total of 61 categories and 903 software tools and services were identified and systematically organized according to the framework proposed by (WILHELM, 2004). A summary of the results is presented in Table 5. In our analysis, we notice that Software and Services have always more than one capability, as consequence, the most part of them could be applied in more than one step from the framework. Not only with them this occurs, but also with some features as well. This supports our observation the frameworks may be too diverse to fit into Wilhelm (2004) framework. The full results are available in appendix E.

5.1.2.1 Deterrance

In the deterrence category, tools emphasized user awareness, policy compliance, and access restrictions.

Beginning with training, the software tools and services addressed a broad range of topics, including cybersecurity, protection against social engineering attacks, and best practices for data usage and protection. Policy awareness was also a recurring theme, with employees

Category	Key Functionalities & Services Summary
Deterrence	Employee education, simulations, access restrictions.
Prevention	Encryption, network protection, security testing. Integration with security services.
Detection	Alerts, AI-based detection, biometrics, anomaly patterns, application and network security.
Mitigation	Incident response, automated blocking, fixes, SOC - Security Operations Center, alerts, and financial support.
Analysis	Reports, dashboards, risk and security insights, visualizations, auditing.
Policies	Regulatory compliance (GDPR, LGPD etc.), internal policies, automation, auditing and governance.
Investigation	Sensitive data protection, evidence collection and analysis, reports, integrations.
Prosecution	Automation of reports and takedowns, AI/NLP, integration with regulatory systems.

Table 5 – Overview of Security Functionalities and Services

participating in certification programs such as SAT - Security Awareness Training, designed to reinforce organizational compliance and individual accountability. In addition, organizations implemented simulated phishing emails and other social engineering scenarios to assess employee responses, identify high-risk individuals, and monitor their progress over time. Another set of deterrence-oriented features involved the enforcement of technical barriers and restrictions to prevent suspicious actions or inadvertent errors. These included setting expiration dates for credentials and assets, limiting time-bound or consumption-based access, filtering internal network traffic, blocking non-work-related websites, and restricting software downloads and installations to authorized applications only.

It is important to highlight that the identified features were primarily designed for work-related environments. This observation raises a relevant question: why, and to what extent, is it possible to develop and implement deterrence-focused software features aimed at protecting individuals beyond the workplace context? This gap suggests potential challenges related to privacy, user adoption, or a perceived lack of market demand for such individual-focused solutions.

5.1.2.2 Prevention

We classified the identified prevention features and services into three main groups based on their scope. Internal features are applied within organizations, targeting infrastructure, systems, and personnel. External features are designed for third parties, such as partners or vendors. Mixed features apply to both internal and external contexts, including customers and general users, reflecting their broader applicability.

For internal features (Figure 10), we identified four categories. The technical dimension includes core infrastructure protections, third-party integrations, and hybrid mechanisms forming a multilayered defense. This involves designing prevention plans and defending against threats like SQL Injection, formjacking, and DoS - Denial-of-Service. Common strategies include Code Obfuscation, encryption, and Anti-tampering across API - Application Programming Interface, data, and code. Infrastructure defenses cover endpoints, networks, and cloud environments, while secure access is enabled via IPsec - Internet Protocol Security,SSL - Secure Sockets Layer, HTTPS, DNS, VPN - Virtual Private Network and ZTNA - Zero Trust Network Access solutions.

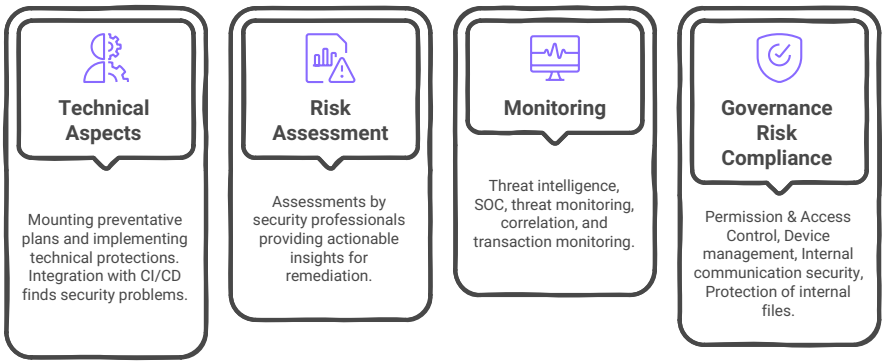


Figure 10 – Internal prevention tolls and features

Automated mechanisms complement core defenses by preventing payment data leakage and maintaining service continuity through PoPs. Integration with CI/CD - Continuous Integration / Continuous Deployment pipelines enables early vulnerability detection, while connections to systems like SIEM - Security Information and Event Management, ITSM - IT Service Management, IAM - Identity and Access Management, SOAR - Security Orchestration, Automation, and Response, and Governance, Risk, and Compliance (GRC) tools support a cohesive security

environment. Risk assessment relies on expert reviews and automated tools such as SAST - Static Application Security Testing, DAST - Dynamic Application Security Testing, Penetration Testing, RASP and vulnerability scans. These are paired with risk scoring, API - Application Programming Interface verification, and Malware scanning to strengthen pre-deployment security. Continuous monitoring ensures ongoing protection through 24/7 endpoint oversight, detection of security debt, and real-time analytics. AI-driven tools support predictive maintenance and infrastructure visibility.

These capabilities feed into threat intelligence, generating alerts for misconfigurations and suspicious activity. Insights are enriched by monitoring social media, the Dark Web, and network traffic, with SOC - Security Operations Center providing round-the-clock supervision.

5.1.2.3 Detection

Detection refers to the prompt identification of issues as early as possible. During the process of classifying security features using the framework proposed by (WILHELM, 2004), we encountered challenges in clearly distinguishing between prevention and detection mechanisms. For instance, the request for a second authentication factor may be considered a preventive measure, as it serves as a barrier against automated attacks. However, it could also be interpreted as a detection mechanism, particularly in scenarios where an attack has already been initiated—such as through password theft—but is ultimately thwarted due to the absence of second-factor confirmation. This ambiguity will be further addressed in the discussion section. For now, we return to our analysis.

Prior to a fraudulent action, specific features are important for strengthening security. These include tools primarily designed for monitoring activities, as well as those focused on verifying the identity of potential attackers to inform the most appropriate response.. A wide range of elements can be monitored with the aim of detecting anomalies. Within the code, it is possible to identify attack patterns such as SQL Injection, DoS - Denial-of-Service, API scraping, XSS, and brute-force attempts. Additionally, systems may track indicators of data leaks, compromised passwords, host intrusions, and abnormal network traffic.

On the other hand, checking possible irregularities during the use of systems is as important as code-level. For example, check the presence of malicious app inside the device which had done some transactions, as well as check if could be automatized bots. One of the most frequently employed security strategies involves user identity verification. In the market census,

we found various methods: biometric systems for face, voice, and behavior; liveness detection (biometrics with video); AI checks to detect deepfakes in biometrics; analysis of buying history details (such as average order value, preferred credit card, and others); MFA; KYC; document validation with OCR; and device fingerprinting. Some of these features can be packaged together to protect against money laundering, ATO, mule accounts, and other types of fraud.

5.1.2.4 Mitigation

The next phase addressed is **Mitigation**, which focuses on halting fraud or attacks as quickly as possible to minimize damage. As in the previous subsections, the findings were organized into thematic groups to enhance clarity and facilitate synthesis. The main categories that emerged from the analysis were arranged according to their response time, from the most immediate actions to longer-term strategic measures, as illustrated in Image 11. In the following paragraphs, we examine each of these categories in detail.

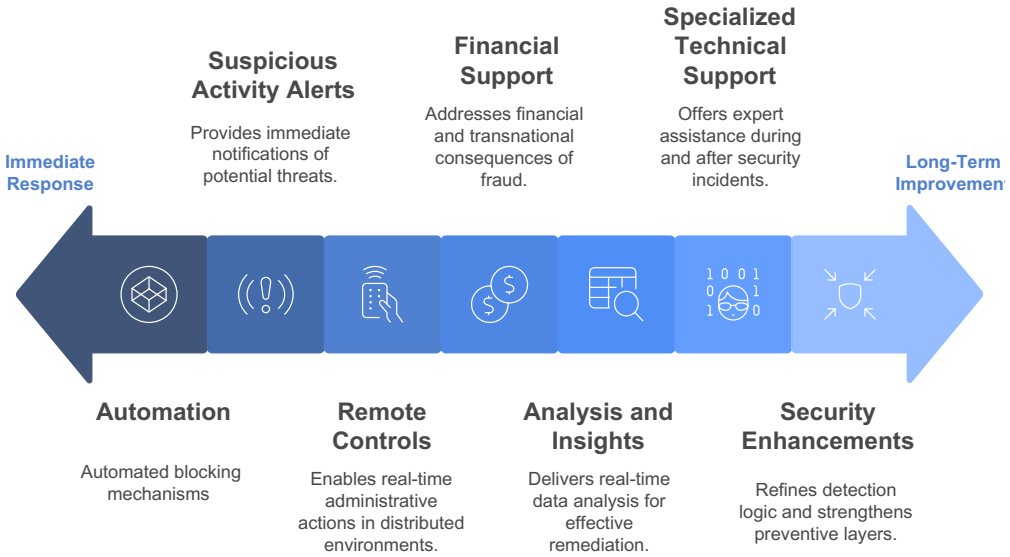


Figure 11 – Mitigation: from immediate response to long-term improvements. **Source**: Authors.

Starting with the fastest category for immediate response, **Automation** emerges as a central theme in mitigation, aiming to reduce response time and minimize human error. One of its primary areas of focus is incident response, with tools that offer automated investigation, containment, and remediation workflows. These systems are capable of addressing known

attack patterns, enforcing predefined security rules, and initiating appropriate responses upon threat detection. In addition to response automation, automated blocking mechanisms are frequently highlighted. These include blocking suspicious access, URL - Uniform Resource Locator s, or network traffic; isolating infected devices; halting malicious application execution; and leveraging artificial intelligence for real-time threat mitigation. Automated systems also contribute to system resilience by redirecting or isolating non-compliant endpoints, blocking phishing emails, and maintaining email availability during service disruptions. Furthermore, automation supports routine corrective actions, such as guiding users through security updates or initiating the take down of fraudulent websites.

If automation fails to stop a threat, is not properly configured, or is unavailable, another rapid-response mechanism is the use of **Suspicious Activity Alerts**. These alerts enable prompt manual intervention, allowing security teams to respond as quickly as possible to mitigate potential damage. It is important to note, however, that alerts are not limited to scenarios where automation is absent or ineffective. Even in automated environments, alerts play a critical role in keeping the organization informed of ongoing incidents, thereby supporting oversight, situational awareness, and potential escalation when necessary. The tools examined in our market census provide real-time alerts enriched with contextual data from threat intelligence platforms, reputation services, and breach feeds. These alerts notify teams about leaked credentials, unusual data access patterns, or emerging vulnerabilities, and in some cases, trigger automated remediation workflows to accelerate incident response. In such alert-driven scenarios, **Remote Control** capabilities also become essential to enable rapid and effective mitigation. These tools support the remote issuance and revocation of credentials, remote access to devices within the network, and real-time tracking of mitigation efforts. Such features are particularly relevant in distributed work environments and high-risk operational contexts, where immediate administrative intervention is critical to containing threats and ensuring business continuity.

To help discover what happened, the **Analysis and Insights** category help the mitigation tools by increasingly incorporate real-time data analysis and machine learning to identify potential policy violations or security breaches. These systems often include dashboards that support security management by providing visualizations and actionable insights. Key features include real-time antivirus analysis, incident tracking, and disaster recovery planning. Detailed reporting on attack vectors and methods enables more effective remediation, while real-time alerts and analytical outputs facilitate rapid decision-making and continuous improvement of

the overall security posture.

Certain platforms also offer mitigation support that goes beyond technical aspects, addressing financial and transnational consequences of fraud, the **Financial and Cross-Border Support**. These include features for recovering improperly transferred funds, expediting the collection of unpaid transactions, managing cases, and detecting post-fraud financial anomalies through AI. Additionally, tools for automating account reconciliation help streamline recovery and reduce operational disruption after a financial incident.

Besides the tools, the companies could also ask help to **Specialized Technical Support** services. This services provide resources and actions designed to assist organizations before, during, and after security incidents. Pre-incident strategies involve operational planning to reduce recovery time in the event of a breach. A significant focus is placed on training, which equips security teams with the knowledge needed to investigate and respond to incidents effectively. These initiatives include documenting remediation actions, proposing mitigation plans, and supporting the development of response strategies. During incidents, the literature emphasizes tools that guide response actions, offer real-time remediation support, and help mitigate risks such as Phishing, Malware, and data leakage. Forensic analysis capabilities are also highlighted as essential for rapid resolution of Data Loss Prevention (DLP) events. Additionally, SOC - Security Operations Center are presented as a critical structure for real-time threat detection and response, providing centralized monitoring and incident handling.

Lastly, some mitigation tools contribute to long-term **Security Enhancements**. These include refining detection logic based on learned application behavior, reducing false positives, and improving the accuracy of threat identification. Identity analytics, for instance, leverage artificial intelligence to support access control decisions and automate compliance processes, thereby reinforcing both preventive and mitigative layers of defense. In this context, the **Analysis** phase plays a crucial role in identifying areas for improvement and informing strategies to enhance the overall effectiveness of the mitigation process.

5.1.2.5 Analysis

The next step is **Analysis**, which is highly important as it contributes to the entire fraud management process. The tools examined provide functionalities that directly impact what is analyzed, why such analysis is performed, how it is conducted, and when it takes place. In Figure 12, we summarized the main points of the analyzed tools.

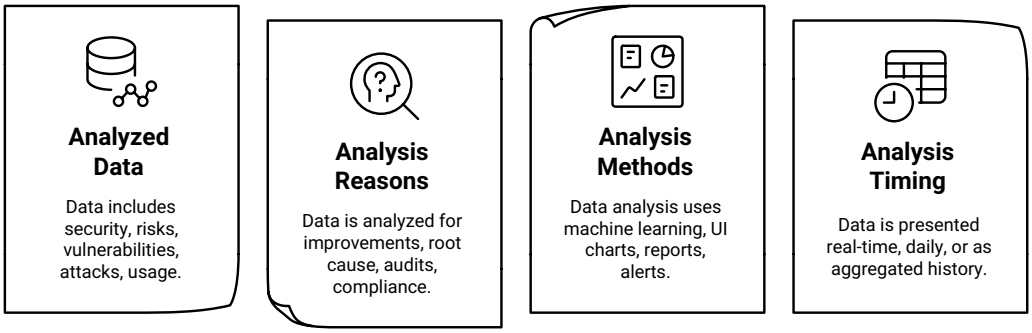


Figure 12 – Summary of Analysis' tools and services. **Source**: Authors.

In terms of **what** these tools analyze, they cover a wide spectrum of indicators relevant to organizational security. This includes the overall security posture, identification of risks, and detection of vulnerabilities. Tools often monitor records of past and potential attacks, analyze usage patterns, and verify compliance with established standards. Additionally, they capture events such as unauthorized internal transactions, failed authentication attempts, and policy violations. Many tools also support audit process visibility, generate diverse performance metrics (including quality, financial, and compliance data), and track payments made and pending. Together, these elements build a comprehensive foundation for understanding an organization's exposure and operational behavior.

The purpose of this analysis (why it matters) emerges clearly in practice. Tools assist in generating suggestions for improvement, enabling organizations to evolve based on empirical evidence. They help uncover the root causes of attacks, facilitating a deeper understanding of incidents beyond surface-level symptoms. Analysis also supports internal and external audits, ensures policy compliance, and enables organizations to prioritize investigations and actions based on risk level. Some tools integrate with financial systems, contributing to financial reporting and aligning fraud management with broader business goals.

As for **how** this analysis is performed, tools employ a range of techniques. Many leverage machine learning to identify anomalies, patterns, or suspicious behaviors in large datasets. They provide user-friendly dashboards with interactive visualizations, allowing diverse stakeholders to interpret the data effectively. Features such as customizable reports, metric-based configurable alerts, and detailed logs enhance the analytical capabilities, offering flexibility and precision in how insights are extracted and communicated.

Finally, the analysis provided by these tools varies according to when the data is processed. Real-time analysis is particularly valuable during active attacks, supporting immediate detection and response. Short-term analysis—typically using data from the past few days—offers greater depth for incident diagnosis. Aggregated historical analysis enables audit preparation, long-term evaluation, and strategic planning by revealing patterns and trends over time.

In summary, the analysis functionalities embedded in the tools reviewed demonstrate a robust alignment with the needs of fraud management. By addressing the what, why, how, and when of analysis, these tools not only enhance operational effectiveness but also empower organizations to make informed, data-driven decisions in a rapidly evolving threat landscape.

5.1.2.6 Policies

Another key component uncovered through the analysis of fraud and risk management tools is the domain of policy compliance and governance. Tools in this area are designed not only to enforce adherence to internal and external regulations but also to support strategic governance practices that ensure organizational integrity and accountability. The analysis revealed three main dimensions in which these tools operate: external policy compliance, internal policy enforcement, and governance-specific capabilities.

Starting with external policy compliance, many tools support organizations in meeting the demands of regulators and auditors. These solutions often provide pre-built templates that facilitate the creation and submission of documents for audits, reducing the manual burden on compliance teams. In some cases, they offer consulting features or access to professionals who specialize in external regulatory frameworks. Furthermore, many tools include the automated generation of compliance reports, offering evidence of adherence to regulatory standards. A recurring feature is the identification of non-compliance points, helping teams proactively address gaps. Complementary capabilities such as cloud-based evidence storage, metadata cataloging, and support for audit planning and execution further streamline the compliance workflow and increase transparency.

Regarding internal policy enforcement, the tools examined offer robust mechanisms to operationalize and monitor corporate rules and procedures. Core features include risk mapping, which helps visualize areas of concern, and automation of compliance processes, which ensures that internal controls are applied consistently. Some tools analyze device usage policies, ensuring that hardware and software practices align with internal standards. Others are capable of

applying contextual rules to sensitive data—such as Personally Identifiable Information (PII), financial records, or intellectual property—tracking their usage and modifications over time. Additionally, several platforms allow for the automation of internal policy lifecycle management, including their creation, approval, and dissemination. These platforms can detect policy violations, centralize compliance reporting, and even assess the policies of third-party partners, ensuring the organization's internal standards extend across its ecosystem.

The third dimension focuses on governance-specific features, which play a crucial role in maintaining long-term organizational resilience. Tools in this category support the implementation of advanced security models such as Zero Trust architectures and the principle of least privilege, reducing unnecessary access and minimizing risk exposure. They also contribute to employee training and awareness, helping staff understand and follow internal policies. Capabilities such as monitoring for unsigned or expired contracts, detecting unauthorized privilege changes, and enhancing asset visibility reinforce a governance model based on accountability and traceability. Moreover, these tools offer controls for authentication methods, ensuring that login mechanisms are secure and auditable. Features like data cataloging, impact analysis of system changes, and identity management across devices further expand the governance toolkit. Notably, automated auditing of vendors enables organizations to maintain oversight and compliance even across their supply chains.

In summary, the policy-related functionalities found in the analyzed tools reveal a sophisticated ecosystem supporting external compliance, internal standardization, and strategic governance. By automating, centralizing, and enhancing visibility into policies and their execution, these tools allow organizations not only to meet regulatory demands but also to strengthen operational integrity and risk management at scale.

5.1.2.7 Investigation

Investigation begins once suspicious activity is identified and requires a detailed, secure, and structured approach to evidence collection, forensic analysis, documentation, and collaboration. The tools analyzed offer a diverse range of functionalities that support this stage, enabling both internal and external stakeholders—such as compliance teams, forensic experts, and law enforcement—to operate effectively across complex investigative workflows.

One foundational aspect of these tools is ensuring security in the investigation process. Platforms offer dedicated features for securely storing case-related data while preserving pri-

vacy, confidentiality, and data integrity. This includes the use of secure communication channels tailored for investigators, which reduce the risk of information leakage during ongoing inquiries. Access logs are also maintained to track how and when sensitive resources are used, contributing to traceability and audit readiness. A common capability among several tools is the provision of a centralized and searchable repository for all case-related materials, allowing investigators to manage large volumes of information efficiently and securely.

The second area of emphasis is digital forensics, where tools demonstrate a high degree of specialization. Many systems support the automated identification of attack origins and the generation of forensic reports on past incidents. Some platforms allow for the outsourcing of forensic analysis to specialized professionals, while others integrate artificial intelligence to detect anomalies and irregular patterns within structured and unstructured data. AI functionalities also enable the extraction of insights from multimedia sources such as videos, images, and documents, as well as the recovery of deleted or hidden files. Tools further support data normalization and correlation, facilitating pattern detection across disparate data sources. The use of forensic telemetry and case-linking capabilities allows for a broader understanding of how incidents are connected, helping investigators map relationships between entities. Some platforms also aggregate and visualize data from multiple systems, providing tailored insights to internal investigators, external consultants, and police agencies. Additional features include suspect identification mechanisms and AI-assisted mapping of evidence to case narratives, strengthening the overall investigative output.

Complementing the forensic layer is a suite of features dedicated to documentation and data management. Tools in this category help investigators draft formal reports, track incidents, and extract key data throughout the case lifecycle. They also organize digital documents, interview records, and collected evidence to ensure quick retrieval and structured archiving. Several systems generate legal and forensic-ready documentation, facilitating submission in judicial or audit contexts. Many of these capabilities are enhanced through integration with external platforms, enabling the automatic capture of evidence, system changes, and contextual information relevant to the investigation.

Lastly, effective investigation increasingly relies on collaborative work environments, and many tools are designed with this in mind. These platforms facilitate the segmentation and assignment of investigative tasks, ensure documentation is properly maintained, and allow team members to contribute across various stages of the case in a cohesive and transparent manner. Such features help coordinate multidisciplinary teams, streamline operations, and

reduce miscommunication across complex investigations.

In sum, the investigation capabilities offered by modern tools encompass secure data handling, advanced forensic functionality, efficient documentation workflows, and collaborative coordination. Together, these features create a robust infrastructure for conducting comprehensive, compliant, and high-impact investigations across organizational and jurisdictional boundaries.

5.1.2.8 Prosecution

The Prosecution phase is a critical step in the fraud response process, focused on transforming investigative findings into actionable legal documentation. Tools supporting this phase streamline operations through automation, AI, and system integrations.

Automation features include the removal of fraudulent websites, generation of forensic reports, and creation of supporting documents such as spreadsheets and legal forms. Many tools offer predefined templates to standardize procedures and accelerate document preparation.

The use of AI and NLP enhances this process by enabling intelligent data collection to identify suspects and by assisting in the review of investigative reports, ensuring accuracy and completeness in the materials used for formal accusations.

Finally, strong integration capabilities with government, regulatory, and investigative systems ensure a smooth transition from investigation to prosecution, allowing data to flow securely and efficiently across institutional boundaries.

In sum, the accusation phase is increasingly supported by digital tools that improve speed, consistency, and legal robustness in building cases against fraud actors.

5.1.2.9 Comments of the census

While applying Wilhelm (2004)'s framework to classify the functionalities of current tools and services, several limitations and ambiguities emerged. In practice, the boundaries between categories such as prevention, detection, and mitigation appear significantly blurred. Many tools serve all three purposes simultaneously, suggesting that these phases may not be as sequential or discrete as the framework implies. Similarly, the distinction between analysis and investigation was difficult to maintain, as analysis often triggers and overlaps with investigative tasks, especially in systems that aggregate, visualize, and correlate data.

The category of deterrence posed further challenges. Few tools could be clearly assigned to this stage, and its conceptual boundaries were difficult to define. For instance, blocking access to unauthorized websites could be interpreted as either deterrence or prevention, depending on perspective. This ambiguity highlights a broader issue: many features are multifunctional and do not fit neatly into a single category, raising questions about the applicability of rigid frameworks in dynamic, real-world environments.

Moreover, policy management revealed strong ties to governance, especially through functionalities related to access control, audit automation, and regulatory compliance. This suggests the need to reconsider how governance is represented in fraud-related models, moving towards a more integrated view that recognizes its pervasive influence across all fraud management activities, from strategic planning to daily operations. Several tools also addressed global regulations, but appeared heavily tailored to European and U.S. standards, which may limit their effectiveness in contexts governed by local laws such as Brazil's LGPD.

Finally, the analysis indicated that many tools are increasingly no-code, modular, and integrated with external systems, blurring the line between software and service. This evolving technological landscape points toward the necessity of adapting or extending existing frameworks—possibly moving toward a more flexible, function-based or capability-centered approach.

5.1.3 Interview with professionals

The professionals participating in this study represented a diverse yet highly specialized set of roles across fraud prevention, cybersecurity, legal compliance, and criminal investigation. Their respective occupations and the specific domains each interview aimed to represent are outlined in Table 6. The collected data were then coded through an axial strategy, leading to their organization into five main categories, detailed in the subsequent paragraphs. The full squeme can be found on Appendix D.

5.1.3.1 Knowledge

The analysis reveals a diverse range of educational backgrounds among professionals in digital security and investigation fields, with a strong emphasis on practical experience, continuous learning, and specialized knowledge. While law degrees are common, particularly in

Interviewee	Occupation	Related Area
INT01	Police Investigator	Fraud Investigator
INT02	Police Investigator and the Police Academy Professor	
INT03	CEO of a company specialized in Fraud Analysis and Professor of Risk,Compliance and Fraud at more than one institution	Fraud Analysis and Management
INT04	Fraud Analyst at a Private Bank	
INT05	Governance, Risk, and Compliance (GRC) Analyst at a Large Retail Company	Policy & Compliance
INT06	Data Protection Officer at a Cybersecurity Company	

Table 6 – Interviewees' profiles

Data Protection Officer (DPO) and GRC roles, there is a clear shift towards requiring technical expertise and a growing recognition of the value of professionals from non-IT fields. Certifications are highly valued, not as mandatory requirements, but as indicators of specialized knowledge and a competitive advantage. *"Certifications are not strictly mandated by the authority; however, it is widely recognized within the market that they serve as an external validation. Possessing such certifications can provide a significant advantage over other individuals."* – INT06.

"If professionals possess these certifications, their resumes will have significantly greater value in a competitive job market." –INT03

The importance of soft skills, data literacy, and adaptability in the face of evolving threats and technologies is consistently highlighted across different roles.

5.1.3.2 Systems

In the context of daily operations, professionals of fraud investigation, compliance, and risk management utilize a diverse array of information systems to support their activities. Ranging from biometric verification and document analysis to case management and auditing systems. While many of these tools are regarded as essential for streamlining procedures, conducting complex analyses, and improving the compilation and correlation of data, several challenges

were also reported. These include data fragmentation across multiple platforms, limited access to relevant information—particularly across jurisdictions—issues related to software acquisition and renewal, usability difficulties for non-technical users, and demands for integration and functional enhancements. Furthermore, discussions around the use of artificial intelligence highlighted both its potential to accelerate workflows and the ongoing concerns regarding bias and the importance of proper contextualization. To illustrate some of the answers, we designed the mind-map in Figure 15 using napkin[2]. The next paragraphs, we detailed more the experiences described by the inteviewees.

Fraud Analysts rely on a range of systems aimed at detecting and validating fraudulent activity, including biometric and liveness verification, facial recognition, metadata inspection, and behavioral monitoring. They navigate multiple platforms for cross-referencing, perform high-accuracy systemic analyses, and leverage visual analytics tools like Power BI, while managing parallel workflows across various specialized programs.

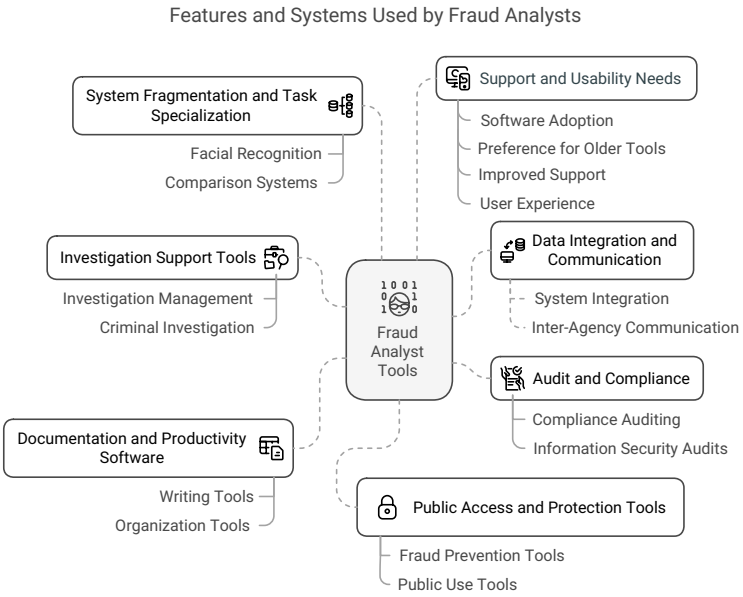


Figure 13 – Tools Fraud Analysts use in daily work. **Source**: Authors.

DPOs and GRCs operate within complementary domains of organizational governance, with overlapping reliance on structured systems to ensure compliance and mitigate risk. GRC specialists focus on managing operational risks, monitoring controls, and maintaining audit readiness through platforms that support asset tracking, workflow management, and automated

[2] https://app.napkin.ai/

reporting. In parallel, DPOs emphasize legal compliance and data protection, utilizing tools for request handling, risk assessment, and data mapping—often supported by centralized repositories and spreadsheet-based visualization. Both roles increasingly explore automation and AI, particularly for anomaly detection, policy generation, and procedural documentation, yet they also face common challenges related to data discovery, system integration, and regulatory alignment.

In contrast, law enforcement professionals adopt a broad suite of investigative and forensic technologies, spanning national police databases, document and facial recognition tools, forensic extraction software, and cross-referencing systems. Despite access to diverse governmental and open-source tools, challenges persist regarding system integration, access restrictions across jurisdictions, and the bureaucratic overhead required for data extraction. There is growing demand for AI-driven facial recognition, automated transcription, and streamlined multi-system search capabilities.

"An individual registers (in this systems) for access to property, water, and electricity services in their home (...) We face a challenge in compiling this essential information due to a lack of formal agreements that would grant us access to these records." –INT01

"We had a great system (...) we spent three years developing it alongside the company. However, when it comes time for renewal, either the company demands an excessively high price, (...) or a new police administrator decides the system is no longer essential or that a different one is needed. Consequently, we face significant difficulties in this regard." – INT02.

5.1.3.3 Processes

The interviews reveal that although professionals from GRC, DPO, law enforcement, and fraud analysis operate in distinct domains, they share overlapping responsibilities related to risk management, data handling, and procedural compliance. Each role exhibits specific operational focuses: GRC emphasizes proactive risk governance and policy adherence; DPO are central to data privacy compliance and incident response; police investigators manage criminal cases with limited prioritization mechanisms; and fraud analysts handle case-based detection through system-assisted triage.

The roles of GRC, DPO, law enforcement, and fraud analysts exhibit marked differences in how they approach analysis, fieldwork, and demand management, though shared challenges persist. In terms of analysis, GRC focuses on deficiencies, incidents, and business continu-

Profile	Type of Analysis	Approach	Demand & Prioritization
GRC	Analyzes deficiencies, incidents, and their impact	Focus on internal processes and systems	Receives demands for risk/incident monitoring and workflow support, acts as compliance hub
DPO	Assesses legal risks, classifies data by risk level, handles subject requests	Focus on legal assessment and compliance tasks	Responds to incidents and requests, prioritizes based on data risk classification
Police	Performs preliminary analysis of police reports, internal investigations, manual case grouping	Includes dynamic routines and field operations	Receives cases via police reports, prioritizes strictly by order of arrival (with life-risk exception)
Fraud Analyst	Manually reviews prefiltered cases, investigates suspicions, escalates and closes fraud cases	Desk-based investigation, suggests collaboration with developers	Handles prefiltered system alerts, prioritizes based on case escalation

Table 7 – Comparison of Profiles in Terms of Analysis, Approach Analysis, and Prioritization

ity risks; DPO assess legal violations, classify data by risk levels, and handle data subject requests—often hindered by manual information retrieval. Police investigators conduct preliminary analysis of police reports, manually group related cases, and face difficulties in user identification on social media due to legal and technical constraints. Fraud analysts examine system-prefiltered cases, investigate by learning process flows, escalate suspicious activity, and terminate fraudulent accounts—expressing interest in closer collaboration with system developers.

Fieldwork is a distinguishing feature of law enforcement professionals, whose activities involve dynamic routines and direct engagement in on-site operations. In contrast, GRC practitioners concentrate on internal governance workflows and system-based process management; DPOs engage primarily in legal assessment, data classification, and regulatory compliance; while fraud analysts conduct desk-based investigations guided by system-generated alerts and established procedural frameworks. Each role reflects a distinct operational mode aligned with its institutional mandate.

Demand and prioritization also vary. Police operate on a strict first-come, first-served basis, with exceptions for life-threatening cases, and face workload issues, particularly in smaller jurisdictions. DPOs respond to privacy incidents and data subject requests through dedicated channels, with implicit risk-based prioritization. GRC handles risk monitoring, incident management, and policy workflow, acting as a compliance hub. Fraud analysts receive filtered cases and prioritize according to the escalation level of suspected fraud.

5.1.3.4 Cybercrime

The interviewees spoke about the crimes they deal with and the risks they face in their daily work, revealing that fraud takes many different forms. The data highlights a wide variety of schemes, including transactional fraud—such as account takeovers, rented or sold accounts, and repeated scams—as well as document-based fraud involving manipulated images, identity fraud, and digitally native documents. Social engineering tactics, like password phishing, chat-focused scams, and fake websites, are also common. More advanced techniques involve technology-enabled fraud, including deepfakes, voice impersonation, and the use of multiple devices to avoid detection. Brand and identity impersonation is another major concern, with criminals creating fake mirror sites or taking over expired domains to steal personal information.

The data also reveals signs of organized criminal collaboration and a structured infrastructure behind many fraud schemes. Criminals often use social media platforms to facilitate the illegal exchange of accounts and personal data, while final negotiations and transactions typically occur through private communication channels. To avoid detection, they frequently rely on multiple phones, platforms, and identities. Police and fraud analysts report the use of infiltration tactics, extensive cross-referencing of banking data, and long-term operations—such as fake e-commerce site takedowns —highlighting the complexity and multi-stage nature of these investigations.

"If someone opens an (social media) account today to commit a crime and closes it tomorrow, it falls into a "limbo"." – INT01.

"On social media (...) where all kinds of current information is being sold or rent. In one of these groups, someone once posted, "Does anyone have an account for rent?"and many people responded." –INT03

Expanding on these findings, the persistence of fraud is closely linked to systemic vulnerabilities and organizational risk factors, as shown in Figure 14. A significant proportion of incidents originate from human error, such as employees falling victim to phishing schemes or failing to detect anomalous behavior. This highlights a persistent need for continuous security awareness and training programs. Furthermore, structural gaps in regulation—most notably the absence of legal prohibitions on practices like account rental—further facilitate fraudulent activity. This poses a significant legislative challenge that undermines prevention efforts and demands immediate policy reform.

Weaknesses in identity verification mechanisms, alongside a heightened risk appetite in

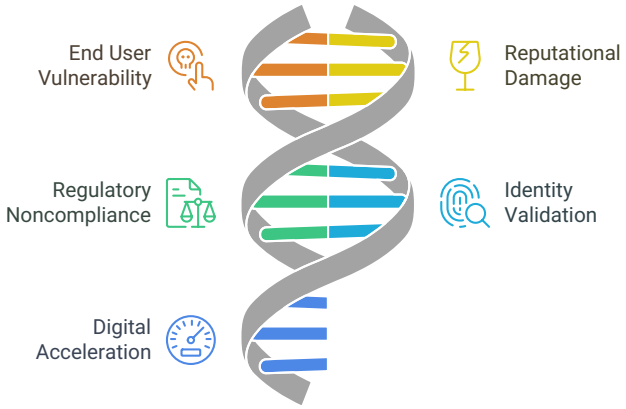


Figure 14 – Risks cited by interviewees. **Source**: Authors.

some organizations driven by the desire for rapid onboarding and operational efficiency, also exacerbate exposure to fraud. This creates an inherent tension between business agility and robust security, which organizations must critically balance. These issues are further compounded by regulatory and reputational risks, particularly highlighted by DPO and GRC professionals, who underscore the long-term consequences of inadequate safeguards and insufficient legal frameworks.

In response to these challenges, the data underscores the critical importance of cross-sector collaboration involving police forces, fraud analysts, GRC professionals, and DPOs. Effective fraud mitigation relies not only on technological tools, such as behavior monitoring systems and anomaly detection, but also on coordinated workflows, including ticketing systems and structured incident escalation. However, the findings also emphasize that technology alone is insufficient; in some cases, it introduces new vulnerabilities that require careful oversight. Moreover, several narratives reveal a disconnect between perception and reality. While the public often imagines cyberattacks as highly sophisticated operations, many successful incidents stem from simple tactics such as social engineering. Reputational risks are frequently underestimated, despite their significant impact on organizational trust. Importantly, professionals across domains acknowledge that criminal actors tend to evolve and adapt more rapidly than the institutions tasked with preventing them, reinforcing the need for continuous learning, shared intelligence, and adaptive strategies.

5.1.3.5 Collaboration among Fraud Professionals and Technical peers

Collaboration encompass both external and internal stakeholders, depending of both occupation and type of institution.

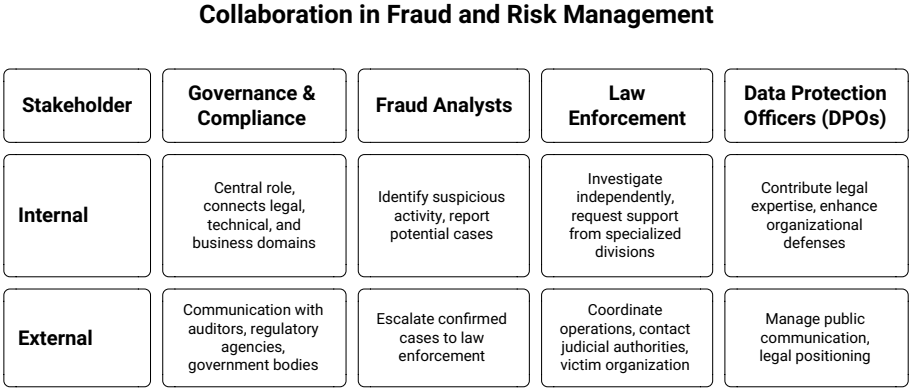


Figure 15 – Resume of collaboration results. **Source**: Authors.

Collaboration in fraud and risk management spans both internal and external stakeholders, shaped by institutional structure and occupational roles. As highlighted in the Cybersecurity Color Wheel framework, governance and compliance teams often occupy a central role, connecting legal, technical, and business domains. This is reflected in awareness initiatives, such as organization-wide security training, and in consultative interactions, where business professionals and project managers seek guidance on identifying risks in their projects and ensuring regulatory compliance. Governance actors also engage continuously in risk evaluation processes, while DPOs (Data Protection Officers) and GRC (Governance, Risk, and Compliance) professionals contribute not only with legal expertise during incidents but also by enhancing organizational defenses. Their role extends externally through active communication with auditors linked to investors, regulatory agencies, and government bodies, ensuring alignment with standards in data privacy, security, and risk management.

These collaborative dynamics are mirrored in operational contexts as well. Within companies, fraud analysts play a proactive role in identifying suspicious activity and reporting potential cases. When anomalies are detected, cases are often escalated to more senior analysts who validate the information and investigate further. Once confirmed, mitigation actions—such as account blocking or data access suspension—are carried out, and when necessary, detailed case

information is forwarded to law enforcement authorities. This interaction marks the beginning of a new layer of collaboration that extends beyond organizational boundaries and into public institutions.

In Brazil, the structure and specialization of police units vary significantly depending on the jurisdiction, available resources, and technical expertise. Some units focus on specific domains, such as computer forensics, ballistics, or financial crimes, while others operate more broadly. When a fraud report is submitted, the local unit typically begins the investigation independently, attempting to resolve the case with its own resources. However, if the case proves complex or requires expertise beyond the unit's scope, support may be requested from specialized divisions. In situations where multiple cases appear connected—particularly when there are signs of organized criminal activity—different units may join forces in what is formally known as an "operation." These coordinated efforts aim to uncover larger schemes by combining technical, legal, and investigative capacities across departments. Throughout the process, law enforcement remains in contact with judicial authorities and the victim organization, requesting additional evidence or legal authorization for deeper investigative procedures when necessary.

"The last major operation we conducted was against fake websites. (...) They (any employee of a private company) came to us because customers were contacting them, stating they had made purchases but hadn't received their items. (...) they realized they had been buying from fake websites. Also, on the technical side with public agencies, I've participated in investigations involving city halls and public tenders; we handle that aspect as well." – INT002

The conclusion of an investigation may result in the submission of a final report to the judiciary, which then determines the appropriate legal actions. Meanwhile, companies affected by fraud may also take internal measures to control reputational damage. In such cases, DPOs, internal controls, and brand protection teams work together to manage public communication, legal positioning, and preventive strategies. This final stage of collaboration highlights how interconnected internal and external actors must be, not only to resolve individual cases, but to build a resilient ecosystem capable of preventing and responding to fraud effectively.

5.1.3.6 Challenges

A persistent challenge in the domains of fraud prevention, cybersecurity, and compliance involves technical limitations and communication barriers. Professionals in police and antifraud

roles frequently lack programming expertise, while developers of antifraud systems often have limited understanding of core investigative concepts. This misalignment impairs collaboration and hinders the development of effective tools. Similar difficulties are observed among GRC professionals and Data Protection Officers (DPOs), who often face obstacles when engaging with technical systems, interpreting specialized reports, and navigating terminology—much of which is presented in English. These barriers contribute to a reliance on security teams, increased effort to interpret unfamiliar terms, and a steep learning curve, especially for early-career professionals. Even experienced practitioners report ongoing difficulties with technical language and tools, including programming languages such as Python.

Another set of recurrent challenges relates to resource constraints, system limitations, and bureaucratic hurdles. Police and investigators report a lack of adequate tools, including limited device access credentials and insufficient functionalities such as data correlation, discovery, and transcription systems. Access to external databases—such as those from public health services, utility providers, and interstate systems—is also restricted, impeding investigations. Existing infrastructure is often outdated, with obsolete equipment, limited storage, and insufficient processing power. Additional issues include discontinued software support, unintuitive interfaces for non-technical users, and imprecise liveness detection technologies. Data storage remains a critical concern, with full external drives and minimal internal capacity.

Human resources are equally constrained, resulting in excessive workloads, overtime, and psychological strain, while regulatory bodies lack sufficient personnel to ensure corporate compliance. Bureaucratic processes further delay operations, including slow licensing procedures, the need for judicial authorization to access data, and reliance on manual workflows. Social media presents unique challenges due to the proliferation of anonymous accounts, rapid information spread, user anonymity, and perceived gaps in legislation—demanding swift police response despite procedural constraints.

5.1.3.7 Comments for this section

The last sections of the survey highlight the complexity and interdisciplinary nature of roles involved in fraud prevention, compliance, and risk governance. As observed, Governance, Risk, and Compliance (GRC) professionals operate at the intersection of legal mandates and technological implementation—an alignment consistent with regulatory frameworks such as the Sarbanes-Oxley Act (SOX), which mandates robust audit mechanisms and oversight to

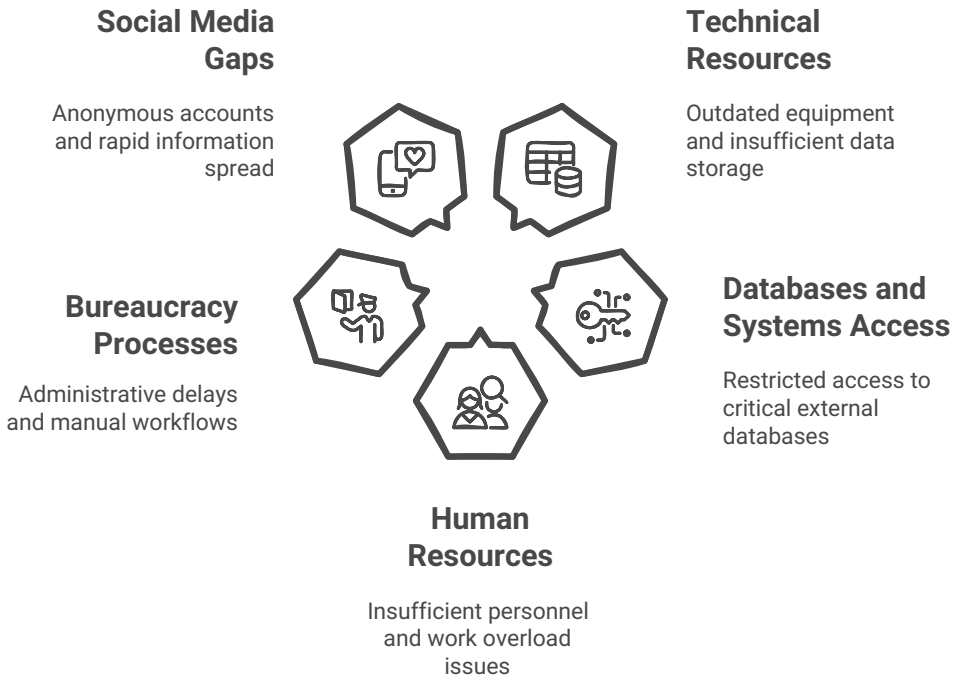


Figure 16 – Challenges faced by professionals of fraud management. **Source**: Authors.

ensure transparency and fraud mitigation. The document further reinforces this through the portrayal of GRC as a compliance hub, responsible for developing mitigation plans and reacting swiftly to incidents such as fraudulent website takedowns. This aligns with the notion that GRC is not only operational but also strategic, often supported by specialized certifications like CISA and GRCP, and regulatory instruments such as ROPA under the LGPD framework.

The discussion also acknowledges that technological advancement, while central to modern investigative and compliance practices, can introduce new vulnerabilities. Echoing concerns raised in the analysis, artificial intelligence, though useful for anomaly detection and automation, may inadvertently expand the capabilities of fraud actors—demonstrating that technology alone is insufficient for robust fraud prevention. This dual role of technology underscores the importance of integrating normative frameworks and collaborative operational models. The document contrasts models like the NIST Cybersecurity Framework—which offers structured, policy-oriented guidance—with the InfoSec color wheel, which promotes interdisciplinary team collaboration. As highlighted in the final sections, effective cybersecurity and risk manage-

ment demand both structural standards and dynamic interaction across legal, technical, and organizational domains.

5.2 FINAL RESULTS AND DISCUSSION

Having all the isolated results in hand, we started the comparison between them. For this, we used our questions as guides, but not excluding another emergent topics that appeared. It is important to note that this section's aim is not yet to answer the research questions, but rather to provide material for further discussion in the next chapter. The following sections will present the emergent topics from combining the results; Figure 17 shows the summarized information of these subsections.

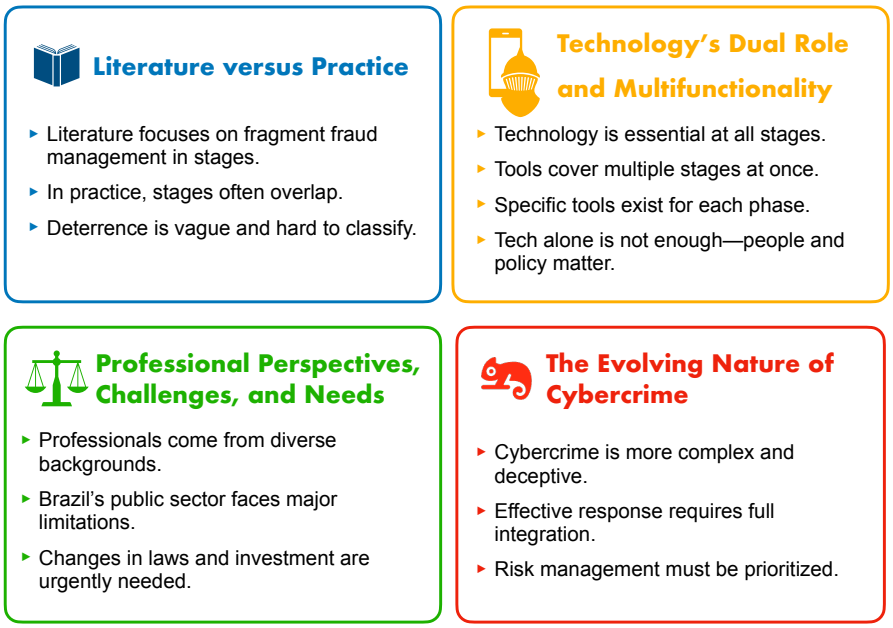


Figure 17 – Summary of Final Results. **Source**: Authors.

5.2.1 Literature versus Practice

The literature review highlights a fragmentation in academic discussions on fraud management, with integrated and comprehensive approaches remaining relatively scarce. Most studies tend to focus on isolated stages or specific types of fraud, offering limited applicability across broader contexts. For instance, Soomro et al. (2019) adopt a detailed framework but narrow their focus to identity fraud within e-commerce settings, which constrains the generalization

of their findings in other sectors.

In contrast, insights from the software market census and interviews with professionals indicate that, in real-world applications, the boundaries between traditional fraud management stages (Deterrence, Prevention, Detection, Mitigation, Analysis, Policy, Investigation, and Prosecution) are often indistinct. Many tools and operational practices support multiple phases simultaneously, challenging the notion of a linear or modular approach to fraud management. In particular, distinctions among Prevention, Detection, and Mitigation proved especially difficult to maintain, as numerous technologies and strategies function across all three areas concurrently. Likewise, the separation between Analysis and Investigation is frequently blurred, given that analytical outputs often serve as the foundation for initiating investigative actions. These overlaps suggest that the fraud management process is more iterative and interconnected.

Furthermore, the Deterrence category proved particularly ambiguous, presenting consistent difficulties in classifying relevant tools. This persistent ambiguity challenges the adequacy of current conceptualizations regarding its precise role and operationalization within fraud management systems. Collectively, these findings from our investigation critically underscore the limitations of rigid, stage-based frameworks in effectively capturing the fluid and dynamic nature of contemporary fraud prevention and response efforts, thereby highlighting an urgent need for more adaptable and context-sensitive models that can comprehensively guide future research and practice.

5.2.2 Technology's Dual Role and Multifunctionality

Technology emerged as a central enabler across all stages of fraud management. From biometric verification and AI-driven anomaly detection to automated incident response mechanisms, technological tools play a pivotal role in strengthening detection and mitigation efforts. These systems allow for faster reaction times, improved accuracy, and scalable interventions, helping organizations proactively address potential threats.

Beyond specific functionalities, a notable trend observed in the market census is the multifunctionality of software tools. Many platforms support several stages of fraud management simultaneously, such as combining detection, prevention, and mitigation within a single solution. This convergence challenges traditional linear frameworks and suggests a shift toward more integrated and holistic fraud management strategies that reflect the operational complexity of real-world scenarios.

The analysis identified a wide range of technologies (and specialized services) being applied at various points in the fraud lifecycle. In early stages such as deterrence and prevention, companies leverage tools like user awareness training, policy compliance systems, access control mechanisms, encryption, security testing, and risk assessment methods such as DAST - Dynamic Application Security Testing, SAST - Static Application Security Testing, and Penetration Testing.

In detection, AI-based systems monitor for anomalies, biometrics verify user identity, and device or behavioral patterns are tracked in real time. As threats escalate, mitigation strategies rely heavily on automation—responding to incidents with real-time blocking, activating SOCs, and even supporting financial restoration.

The analysis phase is enhanced through the use of dashboards, detailed reports, audit logs, and machine learning models that extract actionable insights from historical and real-time data. Other essential aspects include the role of policy enforcement tools that automate lifecycle management and support compliance with regulatory frameworks. In investigation and prosecution, technologies such as digital forensics, anomaly classification, automated reporting, and integration with legal systems help document evidence and initiate corrective or punitive actions.

Despite these advances, the findings also highlight important limitations. The study emphasizes that technological dependence must be balanced with human oversight. While AI enhances efficiency and scalability, it may also inadvertently empower fraud actors by enabling more sophisticated forms of attack. Moreover, as discussed in the survey results, usability challenges and the persistent human factor mean that even the most advanced tools are ineffective without proper training and integration into human workflows. Therefore, a purely technical approach is insufficient. To be effective, fraud management must integrate technology with organizational governance, policy, and human expertise, forming a multi-layered defense capable of adapting to evolving risks.

5.2.3 Professional Perspectives, Challenges, and Needs

Professionals working in fraud prevention and investigation come from diverse disciplinary backgrounds, including law, information technology, and other fields, reflecting the inherently multidisciplinary nature of the domain. This diversity underscores the need for collaborative approaches and cross-functional understanding. Practical experience and continuous learning are

particularly valued, given the rapidly evolving threat landscape and the constant advancement of technology.

Despite their experience, persistent challenges hinder operational effectiveness. A key issue is system fragmentation—fraud analysts often need to navigate multiple platforms for cross-referencing, while law enforcement faces integration issues and jurisdictional access barriers. These challenges are further compounded by limited access to external databases and critical information, particularly across institutional or regional boundaries. Additionally, usability issues affect both technical and non-technical professionals, with many tools presenting steep learning curves or requiring specialized knowledge that is not universally accessible.

In Brazil, law enforcement agencies face even greater obstacles due to the bureaucratic constraints associated with public resource management. These include a lack of adequate tools, outdated infrastructure, insufficient storage capacity, limited processing power, and severe human resource shortages, all of which contribute to excessive workloads. Given the growing volume and complexity of cybercrimes, waiting an entire year for software licensing approvals becomes untenable.

In conclusion, while the expertise and commitment of professionals remain strong, systemic and structural challenges—ranging from technological fragmentation to bureaucratic inefficiencies—significantly limit the effectiveness of fraud prevention and investigation. Addressing these issues requires not only better tools and integration, but also institutional reforms that policymakers and organizational leadership must drive to support agility, cross-sector collaboration, and continuous capacity-building.

5.2.4 The Evolving Nature of Cybercrime

Cybercrime is not only expanding in scale but also becoming increasingly sophisticated and technologically advanced. The evidence presented in this study (mainly on the interview study) shows the worry of complex techniques such as deepfake media, synthetic voice generation, and deceptive social engineering tactics; in one case, there was already a case of creation of fraudulent websites and the simulation of trusted individuals by using many devices. These developments reflect a growing trend in which criminals exploit both technological tools and human vulnerabilities to execute their schemes.

Given this reality, effective fraud prevention relies on a coordinated blend of advanced technological solutions, well-defined operational processes, professional expertise, and public

awareness. However, this combination alone is not sufficient. As the findings suggest, success also hinges on the maturity of risk management practices. Organizations must adopt a more conservative approach to refining their risk appetite and strengthening controls to create a more hostile environment for criminal activity. Achieving this requires cross-sector collaboration, ongoing investment in security infrastructure, and a continuous commitment to adapt strategies in response to the evolving threat landscape.

5.3 ENDING OF THIS CHAPTER

In this chapter, we presented the findings of the research, structured into two main segments: isolated results (Section 5.1) and integrated analysis (Section 5.2). The first section disaggregates findings from the three methodological components—literature review, software market census, and professional interviews—to preserve the specificity and context of each source. The literature review contrasts two key studies: Soomro et al. (2019), structured around the Wilhelm (2004) fraud management cycle, and Soltani, Kythreotis and Roshanpoor (2023), which applies machine learning to categorize research clusters in financial statement fraud. These studies reveal both thematic fragmentation and methodological divergences, particularly regarding identity fraud and audit responsibilities.

The software market census categorizes 903 tools across 61 domains, aligned with Wilhelm (2004)'s framework. Results expose feature overlaps and ambiguities between stages like detection and prevention, underscoring the multifunctionality of technologies. Features range from deterrence (e.g., awareness training) to prosecution (e.g., regulatory automation). Notably, prevention tools dominate in variety and technical depth.The professional interviews add a grounded layer, revealing practical limitations and unmet needs. Respondents cite issues like system fragmentation, skill gaps, and difficulty communicating technical requirements. These testimonies illustrate the human and organizational challenges faced by fraud professionals, which often hinder tool effectiveness.

In the final section, integrated findings are triangulated, revealing key themes: the discrepancy between literature and practice, the dual/multifunctional nature of technologies, professional constraints, and the increasing sophistication of cybercrime. Thus, chapter 5.1, through its triangulation of disparate data sources and identification of practical challenges, serves as a pivotal bridge between theoretical frameworks and real-world application, preparing the ground for the final considerations and implications discussed in Chapter 6.

6 DISCUSSION

Building on the key discussion points outlined in the previous chapter, this final chapter delves deeper into the research objectives. We critically analyze the findings to present our proposed recommendations and outline future work. The chapter is structured around the three main objectives established at the outset, culminating in an integrative discussion.

6.1 TECHNOLOGY AND CHALLENGES

Fraud management is a diverse and complex domain that involves numerous actors and workflows. The tools used in this context are equally varied, many are highly specialized, while others serve multiple purposes simultaneously. Our Benchmark and academic literature have explored this landscape in rich detail, mapping a wide range of technologies and emphasizing their potential for integration. However, a different picture emerges when we listen to professionals working on the front lines of fraud management. While they occasionally express a desire for additional functionalities, the lack of specific features is rarely seen as the core issue. Instead, a recurring pattern of difficulties appears across distinct areas of fraud management. These challenges are less about missing tools and more about how technology fits, or fails to fit, into real-world workflows. The most pressing problems are consistently linked to human factors, usability limitations, and organizational processes.

While research continues to advance in the direction of more sophisticated, feature-rich tools, the people who use these systems daily are more concerned with barriers that prevent effective use. This suggests a disconnect between the academic and commercial focus on technical capabilities and the actual needs in practice. It also points to an important opportunity: to realign the future of computer science in fraud management toward approaches that prioritize usability, integration, and organizational context. One of the most cited challenges is the language barrier. Many users, especially those without technical backgrounds, struggle with systems that rely on complex terminology, rigid workflows, and interfaces that assume a high level of digital fluency. Tools may offer advanced functionalities such as AI-based anomaly detection, behavioral analysis, biometrics, and interactive dashboards, yet these are often underutilized due to a lack of accessibility for non-specialists. This suggests that the design and deployment of such tools must account for diverse user profiles, emphasizing user-centered

design principles and comprehensive training programs to unlock their full potential.

Integration also remains a persistent issue. Although the market census lists over 900 tools and describes numerous integration scenarios, professionals still report the need for manual cross-referencing between systems. This indicates that the tools may exist in theory, but a cohesive and functional ecosystem is still out of reach in practice. Implementation is often hampered by cost, complexity, legacy infrastructure, or simply the absence of a clear integration strategy. Compounding these technical and design issues are bureaucratic and infrastructure-related limitations. Many teams face restricted access to the data they need, either because of internal policies or regulatory concerns. Others operate with outdated equipment, limited storage, or insufficient processing power. In such environments, even the most capable software struggles to deliver value.

Finally, while bureaucracy in law enforcement plays an important role in maintaining fairness and structure, it often slows the response to modern fraud. Criminals today leverage sophisticated digital technologies, operate across borders, and continuously adapt their methods. In contrast, many police procedures still rely on slow approvals, rigid protocols, and disconnected systems that hinder information sharing. This makes it difficult for teams to act quickly and effectively. To keep pace, Brazilian lawmakers should recognize these challenges and work to accelerate the processes for acquiring new hardware and software for law enforcement professionals. These changes are not just beneficial, they are essential to staying ahead of rapidly evolving criminal activity.

Directly addressing the question: **"What technological tools and software features are currently employed in fraud management, and what challenges are associated with their practical use?"**

- The tools used in fraud management span a wide range of categories, including cybersecurity solutions for preventing both internal and external threats; data-driven and automated systems for detection and mitigation; and analytical platforms that generate real-time insights to support investigation and decision-making, often incorporating collaborative features. Additionally, automation tools aligned with legal and regulatory standards assist in policy enforcement and prosecution. Many of these tools also facilitate collaboration between teams and organizations, which is particularly valuable in multi-case investigations involving organized criminal groups.

- The main challenges are more closely related to human factors than to a lack of available

tools. Usability issues and the prevalence of highly technical language hinder effortless use, particularly for non-technical professionals. In the public sector, law enforcement agencies face additional barriers such as bureaucratic delays in acquiring licenses, limited access to advanced software, and in some cases, insufficient hardware resources. Furthermore, access to necessary data is often restricted or requires disproportionate effort, making efficient management more difficult.

Beyond tools, fraud and risk management can be strengthened by a set of skills rooted in the field of computer science. We will explore this topic in the following section.

6.2 COMPUTER SCIENCES KNOWLEDGE IN FRAUD MANAGEMENT

Computer Science encompasses a broad set of knowledge areas, many of which can significantly improve the productivity, efficiency, and effectiveness of professionals working in fraud and risk management. To explore how this potential can be applied in practice, we analyzed insights from interviewees, summarized key tools and services identified in our market census study, highlighted relevant findings from the literature, and contrasted them with the challenges discussed in previous sections.

One recurring challenge mentioned by all interviewees was the difficulty of understanding technical concepts, particularly during work meetings and when using software interfaces. This raises an important question: how can computer science help bridge this gap? Learning to program is not necessarily the answer. For example, one participant who had studied the Python programming language still experienced the same difficulties as others. This reflects a broader issue in professional environments, where many non-technical individuals frequently collaborate with technical teams without formal training in computer science. These professionals, often referred to as conversational programmers, may benefit more from education tailored to the specific needs and objectives of their roles in fraud management, as suggested by Cunningham et al. (2021).

In addition, legal and regulatory requirements in fraud and risk management increasingly demand at least a basic understanding of computer science. Frameworks such as PCI DSS and ISO 27001 are not merely procedural documents. They include technical elements related to encryption, access control, data retention, and system architecture. Understanding these aspects can significantly improve both compliance auditing and practical implementa-

tion. Furthermore, knowledge of core information security concepts, such as how networks are exposed to threats, helps professionals anticipate and reduce the risks posed by digital attacks, and supports their participation in discussions about policies and strategies.

Last but not least, data analysis plays a central role in the entire fraud and risk management process. Therefore, understanding how databases operate, how data is processed and compiled, and how to uncover hidden patterns, trends, or anomalies is essential. Developing these analytical skills is highly valuable for professionals across all areas of fraud and risk management. One of the key enablers for leveraging data is the use of AI, which can act as a supportive peer across a wide range of tasks. Given that fraudsters are already using AI to enhance their scams, it becomes a strategic imperative to leverage the same technology for defense. While interviewees expressed interest in adopting AI-based solutions, they also shared concerns about data leakage and the lack of trust in the security of available platforms. For this reason, future research must carefully consider the ethical implications of using data and AI, particularly in high-stakes domains such as fraud prevention and risk management, to ensure responsible and effective implementation.

To conclude this section, we address the question: **"What computer science knowledge is relevant to professionals working in fraud prevention and investigation, and how is this knowledge acquired or applied in practice?"**.

- **Technical communication skills**, particularly the ability to engage effectively with technical peers while remaining focused on the goals of fraud and risk management professionals (CUNNINGHAM et al., 2021); Beyond the C.S. boundaries, how should C.S. education be offered for other professionals, as part of their future jobs? As clearly applicable, courses of Law should start adding C.S. courses into their program?

- **Foundational principles of information security,** including how systems and networks can be exposed to threats and how to mitigate them; It seems the practical knowledge came from experience, but why not teach network principles and other subjects for professionals in this area? These skills are important for their daily routine as Law knowledge is.

- **Database management and data analysis**, which are essential for identifying patterns, anomalies, and supporting investigative efforts; The professionals (especially in law enforcement) are usually overload with cases that may be the same, sometimes need

a big number of different documents. The knowledge of data strategy, data analysis, data extraction and other data skills would increase their productivity, decreasing their overload of information.

- **The use of AI**, which can enhance knowledge and automate certain tasks, though broader adoption depends on building trust in the security and ethical use of these technologies. As data knowledge could decrease the overload of information, AI would decrease the manual work that sometimes need to be done. For example: analysis of similarities of images, voice transcription, information gathering and much other tasks that need their attention today.

Beyond tools and technical knowledge, the fight against cybercrime increasingly takes place within a more collaborative environment, while essential, also brings new challenges. In the next section, we will explore these subject in greater detail.

6.3 COLLABORATION

Initially, research question 3 aimed to explore collaboration with technology experts. As the research progressed, however, it became clear that this interaction is part of a broader and more dynamic cooperative landscape within Fraud and Risk Management. In this section, we examine the characteristics of this environment, outline its key benefits, and reflect on the main challenges that still need to be addressed.

In this context, it is important to note a convergence in our data regarding collaboration. For instance, law enforcement officers expressed a desire for greater visibility into cases their peers were handling; a feature that was indeed found in the software. Similarly, GRC professionals highlighted the importance of documentation for maintaining consistent procedures. Our benchmark also identified tools that monitor when procedures are updated, subsequently checking compliance and alerting the respective owners. The literature similarly revealed this pattern, evident, for example, in discussions about employee awareness and the critical collaboration between internal (company) and external (police) investigators. This consistent finding across disparate data sources validates collaboration as a critical, pervasive aspect of effective fraud management, underscoring its foundational role in addressing complex digital threats and highlighting a key area for future strategic development.

Despite these efforts to support collaboration, not all related challenges are fully resolved.

One example involves attempts to improve technical communication through dashboards that visualize data, making complex information more accessible to non-technical stakeholders. While such visual tools can aid in conveying specific metrics or trends, they fall short of addressing the deeper issues at play. As discussed in previous sections of this chapter, the core challenges go beyond interface design and include gaps in contextual understanding, interpretive capacity, and cross-functional alignment—factors that remain central to achieving effective collaboration in practice.

6.3.1 Collaboration with Tech Experts

Another interesting fact is how Computer Sciences specialists had cooperate with fraud analysts for more than one reason, more than one specialty of topic and even how was this interaction. Professionals working in Governance, Risk, and Compliance (GRC), along with Data Protection Officers (DPOs), frequently communicate with security teams to address policy concerns and assess potential threats—yet these teams typically operate outside the scope of software development. When it comes to interacting with development teams, the dialogue is usually restricted to strategic matters and occurs mainly with leadership roles, such as Tech Leads or Project Managers. Direct contact with developers involved in day-to-day coding tasks does not seems to happen very often.

On the other hand, fraud analysts are more likely to interact directly with software development teams when they hold senior positions; otherwise, such collaboration tends to be indirect or mediated through other roles. The nature of this engagement differs from that of governance or compliance professionals: rather than focusing on policy or regulatory alignment, analysts are primarily concerned with enhancing the tools they use for prevention, detection, and mitigation. Their contributions are typically more tactical than strategic, drawing on practical experience to inform system improvements. By leveraging their operational knowledge, these professionals can increase the effectiveness of technical solutions, often proposing customizations that address specific threats and vulnerabilities unique to the company's context.

When it comes to authorities, collaboration with technology professionals follows no single pattern. In some cases, technical peers work closely with investigators on a daily basis, especially when internal teams are directly involved in developing software solutions. In other situations, however, the organization outsources development to external software companies, which shifts the interaction primarily toward Product Owners or project managers, rather than

developers themselves. Additionally, authorities may rely on internal technology experts for a wide range of support—from navigating complex software systems to extracting information from digital hardware. Although these specialists are embedded within the organization, their involvement is typically demand-driven and mobilized when specific expertise is required.

In addition to the forms of collaboration discussed earlier, both the benchmark analysis and the literature point to a relevant dimension that received less attention in the interviews: the role of third-party service providers. Many organizations enhance their cybersecurity efforts by outsourcing specialized services, such as SOC - Security Operations Center and threat intelligence. Similarly, software vendors often provide technical support to help companies adapt and integrate tools more effectively into their existing systems. This reliance on external expertise also extends to training, where fraud and risk specialists are contracted to strengthen the skills of internal teams, including fraud analysts and, in some cases, police investigators. These forms of collaboration highlight the importance of external partnerships in expanding internal capabilities and addressing complex challenges that require domain-specific knowledge.

Finally, to address the research question directly— **"How do fraud management professionals perceive collaboration with computer science experts?"**. The findings suggest the following:

- There is a clear convergence across the three data sources used in this study. The features identified in the software market census align closely with the needs and challenges raised during the interviews, particularly in relation to collaboration.
- The nature of collaboration between fraud and risk professionals and IT experts varies depending on contextual factors. This interaction differs in terms of roles, objectives, and the degree of proximity or integration between the parties involved.
- Third-party services and tools also play a significant role in shaping these collaborations and must be considered when analyzing professional dynamics in this context.

6.4 END OF CHAPTER

This chapter has explored the three core dimensions of this research: the technological landscape of fraud management, the relevance and application of computer science knowledge in professional practice, and the dynamics of collaboration between fraud management professi-

onals and technical experts. A key insight is that while technological advancement continues to enrich the tools available for fraud management, many of the most pressing challenges lie not in the absence of features, but in their accessibility, usability, and integration within real-world workflows. Similarly, although computer science knowledge is increasingly necessary in this domain, effective learning must be contextualized and practical rather than purely theoretical or programming-focused. Furthermore, collaboration remains a cornerstone of effective fraud prevention and investigation. Yet, as shown, these interactions are shaped by organizational structures, role definitions, and external dependencies. From internal development teams to third-party service providers, successful collaboration depends on mutual understanding, clear communication, and adaptable processes.

In sum, this study underscores the critical importance of aligning technological tools, human expertise, and organizational processes. It is through this alignment that institutions can build resilient and adaptive systems capable of responding to the complexity and velocity of contemporary fraud. The following and final chapter builds on this discussion to present practical recommendations and outline potential directions for future research.

7 FINAL CONSIDERATIONS

For the final considerations, we will discuss the threats to validity and the limitations of our study, followed by our conclusion and directions for future work. Finally, the lessons learned throughout the research process and our recommendations.

7.1 CONCLUSION

This study embarked on a comprehensive exploration of fraud management from a computer science perspective, emphasizing the intricate interplay between software tools, domain-relevant knowledge, and the crucial role of professionals with computing expertise. By adopting a mixed-methods approach that triangulated insights from academic literature, a market software market census, and direct interviews with professionals, we aimed to identify critical improvement points for both industry and academia.

Our findings reveal that technological tools are essential across all stages of fraud management, from deterrence to prosecution. Modern software systems exhibit high multifunctionality, often blurring the traditional boundaries between prevention, detection, and mitigation efforts. These tools leverage advanced capabilities such as AI-driven anomaly detection, biometrics, automated incident response, digital forensics, and integration with regulatory systems.

However, the research underscored that the most significant challenges in practical fraud management are less about the absence of features and more about human factors, usability, and systemic integration. Professionals frequently struggle with complex technical language, fragmented systems requiring manual cross-referencing, and limited access to critical data. Particularly in the public sector, limitations are exacerbated by bureaucratic hurdles, outdated infrastructure, and severe human resource shortages. This highlights a disconnect between the sophisticated tools available and their effective adoption and utilization in real-world contexts.

Regarding relevant computer science knowledge, the study found that technical communication skills, foundational information security principles, database management, and data analysis are paramount for fraud professionals. While AI is seen as a valuable asset, its broader adoption is contingent on building trust in its security and ethical implications. The acquisition of this knowledge often occurs informally, pointing to a need for more tailored educational programs for non-technical professionals.

Collaboration emerged as a consistently important theme across all data sources, indicating a clear convergence on its necessity. The nature of collaboration with technology experts varies significantly based on roles and organizational context, often involving third-party service providers and indirect interactions with development teams. Despite efforts to facilitate collaboration, challenges remain in achieving deep contextual understanding and seamless cross-functional alignment.

In essence, the study confirms that while technology is a powerful enabler, effective fraud management requires a delicate balance among robust tools, proficient human expertise, and well-structured organizational processes. The increasing sophistication of cybercrime demands not only continuous technological advancement but also an evolving understanding of risk management, cross-sector collaboration, and adaptable strategies.

7.2 RECOMMENDATIONS FOR ADVANCING FRAUD MANAGEMENT

The evolving landscape of digital fraud necessitates a proactive and integrated approach, moving beyond traditional silos to cultivate a resilient and adaptive defense. Our findings illuminate areas where strategic intervention can significantly enhance the effectiveness of fraud management, bridging the gap between theoretical models and practical realities.

7.2.1 Proposing an Integrated Fraud Resilience Framework

The current array of fraud management frameworks, while individually valuable, often present a fragmented view, failing to fully capture the dynamic and interconnected nature of real-world operations. As highlighted by the comparative analysis in Table 1, the strengths of frameworks like Wilhelm (2004), NIST Cybersecurity Framework , and CIMA Risk Management Framework lie in their distinct emphases: operational workflows, technical governance, and enterprise risk management, respectively. This could be a theme of a future study, extending the discussion of chapter 2 section 2.4.5.

Yet, their individual limitations become apparent when confronted with the multidimensionality and iterative demands of contemporary fraud challenges. The path forward demands a hybrid framework that transcends rigid, sequential stages. This new structure must inherently acknowledge the multifunctionality and iterative demands of contemporary fraud challenges, where prevention, detection, and mitigation capabilities often operate in concert. Such an inte-

grated framework would offer a more realistic and adaptable guide for organizations, reflecting modern defensive strategies.

7.2.2 Bridging Communication Gaps for Enhanced Collaboration

Moving from the conceptual to the collaborative, effective teamwork is fundamental to robust fraud management, yet it is hindered by persistent technical language barriers. Professionals often struggle with complex terminology and system interfaces, impeding seamless interaction with technical teams. To foster deeper collaboration, focused research into solutions for technical communication is crucial. Increasing digital literacy, understanding security foundations, and developing data analysis skills are essential starting points. Empowering all stakeholders with accessible understanding will significantly enhance cross-functional dialogue and strengthen collective defense.

7.2.3 Legislative Modernization for Agile Law Enforcement

Because of the multidisciplinary aspect of this study, we found improvements for another areas outside Computer Sciences, in the case of this subsection, Law and Public Policies. As we consider the broader operational environment, combating cybercrime requires agile responses from law enforcement. However, current legislative and bureaucratic frameworks often impede police efficiency in solving crimes. Slow approvals, rigid protocols, and limited access to critical external databases (such as public health services and utility providers) hinder investigations. Outdated equipment and year-long delays in software acquisition further prevent police from keeping pace with evolving criminal tactics. Legislative changes are urgently needed to streamline processes, ensuring timely access to advanced digital tools, forensic capabilities, and fostering efficient data sharing agreements for effective crime resolution.

7.2.4 Navigating the AI Frontier: Ethics, Secrecy, and Trust

Finally, looking to the future of capabilities, Artificial Intelligence profoundly impacts fraud, offering defensive opportunities while creating new challenges as fraudsters leverage AI for scams. Professionals are interested in AI but express concerns about data leakage and platform security. The dual role of AI necessitates careful governance to prevent empowering malicious

behavior. Achieving AI's full potential requires robust data governance, explainable AI, security by design, and clear ethical guidelines to address biases. Investing in secure collaboration platforms will build confidence and responsibly harness AI's power against digital fraud.

7.3 THREATS TO VALIDITY AND LIMITATIONS

This study employed a multi-methodological design, integrating a literature review, a software feature market census, and semi-structured interviews with professionals. This approach aimed to corroborate, complement, and expand our research findings by triangulating data from academic, industry, and practical perspectives. However, as with any research, several limitations and potential threats to validity must be acknowledged.

7.3.1 Author Expertise on Fraud Management Bias

The main author had experience with Fraud Management which could affect in parts the results of the research. To limit this bias, we invite another researcher with zero prior experience on Fraud to join the methodology decisions, data gathering and analysis and discussion of results. Is also important to say the Supervisor Professor was also unexperienced with these concepts. Lastly, this research was presented in a student event before sending for Ethical Approve, which was evaluated for some Professors, which had some changes in order to increase its relevance, impact and reliability.

7.3.2 Multi-Methodology and Integration Challenges

A significant limitation emerged from the use of (WILHELM, 2004)'s Fraud Management Cycle as the primary framework for classifying functionalities and findings. Although initially appearing comprehensive, its application revealed ambiguities and overlaps between stages such as deterrence, prevention, detection, and mitigation. Similarly, maintaining a clear distinction between *analysis* and *investigation* proved difficult, as analytical outputs often serve as the foundation for investigative actions. The "*Deterrence*" stage, in particular, was conceptually vague and challenging to apply consistently. The integration of findings highlighted these blurred boundaries, suggesting that the fraud management process is more iterative and interconnected than the framework implies. This points to a potential 'integration failure'

antipattern, where the chosen framework proves inadequate in fully capturing the multifaceted nature of empirical data, leading to fragmented understanding and potentially ineffective strategic guidance.

7.3.3 Market census Limitations

Our market census assessed enterprise software based on the breadth and quality of their security and fraud management features. *Gartner* was selected as the primary source due to its authority in enterprise software evaluations, particularly with regard to scalability, integration, and long-term support. The market census focused on identifying the presence and scope of fraud-related functionalities as advertised on vendor websites, rather than conducting empirical performance testing.

This approach entails limitations. It lacks automated, repeatable procedures under controlled workloads, which are common in traditional market census. Instead, we performed a structured inventory of publicly available feature descriptions, which does not constitute a replicable experimental setup. To enhance construct validity, identified features were mapped to Wilhelm (2004)'s framework and validated through expert feedback. Although this method does not support performance claims or replication, it serves as a useful feature-oriented market census.

7.3.4 Qualitative Survey Limitations

We conducted semi-structured, synchronous online interviews with six professionals occupying key roles in fraud management, including Fraud Managers, Compliance Auditors, and Police Investigators. Interviews were guided by open-ended questions, recorded, transcribed, anonymized, and analyzed using open coding into thematic categories (e.g., "Knowledge," "Systems," "Processes," "Cybercrime").

Our sampling strategy prioritized in-depth insights from diverse roles across (WILHELM, 2004)'s fraud management cycle, rather than aiming for data saturation. While this approach limits broad generalizability, it provided rich, nuanced perspectives critical for understanding the complexities of the Brazilian context, particularly within the public sector. The findings, though requiring caution in transferability, offer valuable qualitative depth as a foundation for future, larger-scale studies.

Despite these threats and limitations, the study offers valuable insights. They also highlight important opportunities for future work and inform the lessons learned that guide the next steps in this research.

7.4 LESSONS LEARNED

The research journey offered several valuable lessons, both in terms of methodological execution and in deepening our understanding of the complex, multidisciplinary nature of fraud management.

One of the first key experiences was navigating the ethical review process. This marked the researchers' initial formal submission to an ethics committee, introducing important considerations related to consent, data privacy, and participant protection. Recruiting suitable professionals for interviews also proved more difficult than anticipated, underscoring the challenge of engaging busy experts in academic research, especially in sensitive domains like fraud and compliance.

Methodologically, the deliberate choice to adopt a multi-method approach (combining literature review, software market census, and qualitative interviews) proved essential in mitigating threats to validity. This triangulation enriched the study by enabling a holistic view across academic, technical, and operational perspectives. However, integrating these data sources was not without challenges, particularly when attempting to classify findings using already existed frameworks. (WILHELM, 2004)'s Fraud Management Cycle, while initially promising, revealed limitations when applied to empirical data, especially due to conceptual overlaps and unclear boundaries between categories such as prevention, detection, and mitigation.

The execution of a feature-oriented software market census was a novel undertaking for the researchers, providing practical insight into evaluating enterprise tools systematically. This process was further enhanced by the integration of generative AI, that was used for the first time in this research, assisting data extraction and processing. While helpful, AI involvement required careful post-processing to ensure accuracy and resolve occasional misinterpretations, emphasizing the necessity of human oversight in AI-augmented workflows.

Perhaps one of the most important lessons concerned the nature of fraud management itself. The domain's vastness and interdisciplinary demanded a steep learning curve, combining elements of law enforcement, Cybersecurity, risk governance, and human behavior. A critical takeaway is that technology alone is insufficient: effective fraud mitigation strategies must

combine technical tools with human judgment, adaptive organizational processes, and ethical considerations. AI systems, while powerful, can inadvertently enable malicious behavior if not carefully governed, highlighting the need for responsible design and implementation.

Ultimately, the study demonstrated the importance of cross-disciplinary collaboration, continuous learning, and flexible methodologies to navigate and respond to the evolving threat landscape in fraud management. These lessons not only shaped the present research but will also guide future efforts toward more integrated, human-centered solutions.

To build upon the lessons learned and address the identified threats and limitations, the following section outlines potential directions for future research.

7.5 FUTURE WORKS

This study highlights several directions for future research that can address its limitations and contribute to advancements in fraud management. One key opportunity involves refining existing conceptual frameworks. The application of Wilhelm's Fraud Management Cycle revealed limitations such as overlapping categories and rigid distinctions that did not fully reflect the iterative and interconnected nature of real-world practices. Future work should aim to develop models that better represent the dynamic interaction between technology, human expertise, and organizational processes. In addition, the empirical validation of fraud-related software functionalities remains an open area. While this study examined publicly advertised features, future research could evaluate system performance in practical settings through user studies or hands-on testing, offering more concrete evidence of effectiveness.

Another important direction involves expanding the qualitative component. Including a broader and more diverse group of professionals across different sectors, geographic regions, and organizational levels would strengthen the generalizability of findings. Comparative studies could also explore how fraud management strategies vary between public and private institutions or across distinct regulatory environments. This research also introduced generative artificial intelligence for data extraction, suggesting new possibilities for integrating AI into fraud detection and investigation workflows. Future studies could examine how AI can be applied in a responsible and effective manner, considering not only accuracy and efficiency but also explainability, ethical implications, and user trust. It is also important to investigate how professionals interact with AI tools in practice, identifying patterns of collaboration that enhance decision-making.

Finally, the study reveals the need for focused educational initiatives and improved usability in fraud management tools. Future work could include the development of training programs aimed at enhancing digital literacy among non-technical professionals, such as auditors and investigators, while also helping technical teams understand legal and investigative processes. Research should also explore participatory design and usability testing to ensure that tools meet the needs of different user groups and organizational contexts. These combined efforts can promote more integrated and human-centered approaches to fraud management, capable of responding to the evolving challenges of the field.

BIBLIOGRAPHY

AL-SAYYED, R.; ALHENAWI, E.; ALAZZAM, H.; WRIKAT, A.; SULEIMAN, D. Mobile money fraud detection using data analysis and visualization techniques. *Multimedia Tools and Applications*, Springer, v. 83, n. 6, p. 17093–17108, 2024.

BECKER, R. A.; VOLINSKY, C.; WILKS, A. R. Fraud detection in telecommunications: History and lessons learned. *Technometrics*, Taylor & Francis, v. 52, n. 1, p. 20–33, 2010.

BEHDAD, M.; BARONE, L.; BENNAMOUN, M.; FRENCH, T. Nature-inspired techniques in the context of fraud detection. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, IEEE, v. 42, n. 6, p. 1273–1290, 2012.

Brasil. *Lei Geral de Proteção de Dados Pessoais*. 2018. <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Accessed on June 3, 2025.

CARMINATI, M.; CARON, R.; MAGGI, F.; EPIFANI, I.; ZANERO, S. Banksealer: A decision support system for online banking fraud analysis and investigation. *computers & security*, Elsevier, v. 53, p. 175–186, 2015.

CAVUSOGLU, H.; RAGHUNATHAN, S. Configuration of detection software: A comparison of decision and game theory approaches. *Decision Analysis*, Informs, v. 1, n. 3, p. 131–148, 2004.

CIFAS. *Fraudscape 2025: Fighting Fraud and Financial Crime Together*. 2025. <https://www.fraudscape.co.uk/>. Accessed: 2025-05-15.

CIMA. *Fraud risk management: A guide to good practice*. [S.l.]: Chartered Institute of Management Accountants, 2009.

CLEMENTS, L. H.; KNUDSTRUP, M. Which fraud investigation procedures are most often performed? an exploratory study. *Journal of Forensic & Investigative Accounting*, v. 8, n. 2, p. 168–178, 2016.

CRAIGEN, D.; DIAKUN-THIBAULT, N.; PURSE, R. Defining cybersecurity. *Technology innovation management review*, v. 4, n. 10, 2014.

CRESSEY, D. R. Other people's money; a study of the social psychology of embezzlement. Free press, 1953.

CUNNINGHAM, K.; ERICSON, B. J.; BEJARANO, R. A.; GUZDIAL, M. Avoiding the turing tarpit: Learning conversational programming by starting from code's purpose. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. [S.l.: s.n.], 2021. p. 1–15.

DEVOS, J.; PIPAN, I. The role of it/is in combating fraud in the payment card industry. In: *International conference on eCommerce, ePayments and Applications (ICeP'09)*. [S.l.: s.n.], 2009. v. 14, n. 3.

DORMINEY, J.; FLEMING, A. S.; KRANACHER, M.-J.; JR, R. A. R. The evolution of fraud theory. *Issues in accounting education*, American Accounting Assocation, v. 27, n. 2, p. 555–579, 2012.

FATRIZIA, S.; PUTRA, I. N. N. A.; HIDAYATI, S. A. Role of good corporate governance in preventing financial statement fraud and money laundering. *Journal of Accounting and Finance in Emerging Economies*, v. 11, n. 1, p. 25–36, 2025.

GOMES, R. F.; JUNIOR, R. F. D. S.; GARCIA, V. C. Exploring non-cs learners' experience in brazil. In: SBC. *Simpósio Brasileiro de Educação em Computação (EDUCOMP)*. [S.l.], 2025. p. 15–26.

HOYER, S.; ZAKHARIYA, H.; SANDNER, T.; BREITNER, M. H. Fraud prediction and the human factor: An approach to include human behavior in an automated fraud audit. In: IEEE. *2012 45th Hawaii International Conference on System Sciences*. [S.l.], 2012. p. 2382–2391.

HUTCHINGS, A. Hacking and fraud. *Global Criminology: Crime and Victimization in a Globalized Era (2013)*, p. 93–114, 2013.

IJEOMA, N.; ARONU, C. The impact of fraud management on organizational survival in nigeria. *American Journal of Economics*, v. 3, n. 6, p. 268–272, 2013.

ISO. *Information technology — Security techniques — Information security management systems — Requirements*. Switzerland, 2013. v. 2013.

JAMIESON, R.; WINCHESTER, D.; SMITH, S. Development of a conceptual framework for managing identity fraud. In: IEEE. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. [S.l.], 2007. p. 157c–157c.

LEITE, R. A.; GSCHWANDTNER, T.; MIKSCH, S.; GSTREIN, E.; KUNTNER, J. Visual analytics for event detection: Focusing on fraud. *Visual informatics*, Elsevier, v. 2, n. 4, p. 198–212, 2018.

MIRI-LAVASSANI, K.; KUMAR, V.; MOVAHEDI, B.; KUMAR, U. Developing an identity fraud measurement model: a factor analysis approach. *Journal of Financial crime*, Emerald Group Publishing Limited, v. 16, n. 4, p. 364–386, 2009.

NAJAR, A. V.; ALIZAMANI, L.; ZARQI, M.; HOOSHMAND, E. A global scoping review on the patterns of medical fraud and abuse: integrating data-driven detection, prevention, and legal responses. *Archives of Public Health*, Springer, v. 83, n. 1, p. 43, 2025.

National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD, 2024. Https://doi.org/10.6028/NIST.CSWP.29.

OZILI, P. K. Forensic accounting research around the world. *Journal of Financial Reporting and Accounting*, Emerald Publishing Limited, v. 23, n. 1, p. 128–153, 2021.

PCI. *PCI Data Security Standard*. 2024. <https://www.pcisecuritystandards.org/standards/pci-dss/>. Accessed on June 2, 2025.

SCARPINO, J. P. *An Exploratory Study: Implications of Machine Learning and Artificial Intelligence in Risk Management*. Phd Thesis (PhD Thesis) — Marymount University, 2022.

Serasa Experian. *Indicadores Econômicos | Serasa Experian*. 2025. Accessed on June 1, 2025. Available at: <https://www.serasaexperian.com.br/conteudos/indicadores-economicos/>.

SHAH, M.; OKEKE, R. I. A framework for internal identity theft prevention in retail industry. In: IEEE. *2011 European Intelligence and Security Informatics Conference*. [S.l.], 2011. p. 366–371.

SILVA, P.; MAÇÃS, C.; POLISCIUC, E.; MACHADO, P. Visualisation tool to support fraud detection. In: IEEE. *2021 25th International Conference Information Visualisation (IV)*. [S.l.], 2021. p. 77–87.

SOLTANI, M.; KYTHREOTIS, A.; ROSHANPOOR, A. Two decades of financial statement fraud detection literature review; combination of bibliometric analysis and topic modeling approach. *Journal of Financial Crime*, Emerald Publishing Limited, v. 30, n. 5, p. 1367–1388, 2023.

SOOMRO, Z. A.; AHMED, J.; SHAH, M. H.; KHOUMBATI, K. Investigating identity fraud management practices in e-tail sector: a systematic review. *Journal of Enterprise Information Management*, Emerald Publishing Limited, v. 32, n. 2, p. 301–324, 2019.

SPERDEA, N. M.; ENESCU, M.; ENESCU, M. Challenges of managing e-commerce. *Economics, Management and Financial Markets*, Addleton Academic Publishers, v. 6, n. 2, p. 194, 2011.

STANIKZAI, A. Q.; SHAH, M. A. Evaluation of cyber security threats in banking systems. In: IEEE. *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*. [S.l.], 2021. p. 1–4.

TARIQ, E.; AKOUR, I.; AL-SHANABLEH, N.; ALQUQA, E. K.; ALZBOUN, N.; AL-HAWARY, S. I. S.; ALSHURIDEH, M. T. How cybersecurity influences fraud prevention: An empirical study on jordanian commercial banks. *International Journal of Data and Network Science*, Growing Science, v. 8, n. 1, p. 69–76, 2024.

THAKUR, K.; ALI, M. L.; OBAIDAT, M. A.; KAMRUZZAMAN, A. A systematic review on deep-learning-based phishing email detection. *Electronics*, MDPI, v. 12, n. 21, p. 4545, 2023.

The European Parliament and of the Council. *Directive (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market*. 2014. <https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng>. Accessed on June 3, 2025.

The European Parliament and of the Council. *Directive (EU) 2015/2366 on payment services in the internal market*. 2015. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015L2366-20250117>. Accessed on June 3, 2025.

The European Parliament and of the Council. *General Data Protection Regulation*. 2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Accessed on June 3, 2025.

U.S. Department of Health and Human Service. *Health Insurance Portability and Accountability Act of 1996*. 2013. <https://www.hhs.gov/regulations/index.html>. Accessed on June 3, 2025.

U.S. Department of Justice. *Fraud Section: Year In Review*. [S.l.], 2025. Accessed on June 1, 2025. Available at: <https://www.justice.gov/criminal/media/1385111/dl?inline>.

U.S. Department of the Treasury. *Financial Crimes Enforcement Network*. 2025. <https://www.fincen.gov/about>. Accessed on June 3, 2025.

VERDON, D. Security policies and the software developer. *IEEE Security & Privacy*, IEEE, v. 4, n. 4, p. 42–49, 2006.

WANG, Z.; SUN, L.; ZHU, H. Defining social engineering in cybersecurity. *IEEE Access*, v. 8, p. 85094–85115, 2020.

WEBGA, K.; LU, A. Discovery of rating fraud with real-time streaming visual analytics. In: IEEE. *2015 IEEE symposium on visualization for cyber security (VizSec)*. [S.l.], 2015. p. 1–8.

WILHELM, W. K. The fraud management lifecycle theory: A holistic approach to fraud management. *Journal of economic crime management*, v. 2, n. 2, p. 1–38, 2004.

WOHLIN, C.; RUNESON, P.; HÖST, M.; OHLSSON, M. C.; REGNELL, B.; WESSLÉN, A. et al. *Experimentation in software engineering*. [S.l.]: Springer, 2012.

WRIGHT, A. C. *Orange Is the New Purple*. 2017. White Paper, Black Hat USA. Accessed: 2025-05-15. Available at: <https://www.blackhat.com/docs/us-17/wednesday/us-17-Wright-Orange-Is-The-New-Purple-wp.pdf>.

ZHOU, J.; WANG, X.; WANG, J.; YE, H.; WANG, H.; ZHOU, Z.; HAN, D.; YING, H.; WU, J.; CHEN, W. Fraudauditor: A visual analytics approach for collusive fraud in health insurance. *IEEE Transactions on Visualization and Computer Graphics*, IEEE, 2023.

APPENDIX A – BENCHMARK - SELECTED ITEMS PER CATEGORY

Category list	Number of selected
Access Management	4
Accounts Payable (AP)	5
Anti-Money Laundering (AML) Software	11
API Protection	19
Application Security Posture Management (ASPM) Tools	18
Application Security Testing	20
Audit Management Solutions	15
Brand Protection Software	19
Cloud Security Posture Management Tools	20
Cloud Web Application and API Protection	13
CPS Protection Platforms (Cyber-Physical Systems)	19
Cyber Asset Attack Surface Management	18
Data and Analytics Governance Platforms	20
Data Loss Prevention	20
Data Masking	18
Data Security Platforms	8
DDoS Mitigation Solutions	14
Digital Commerce Payment Vendors	25
Digital Evidence Management Systems,	3
Digital Forensics and Incident Response Retainer Services	20
Digital Rights Management Software	12
DNS	8
Electronic Signature	19

This table continued from previous page

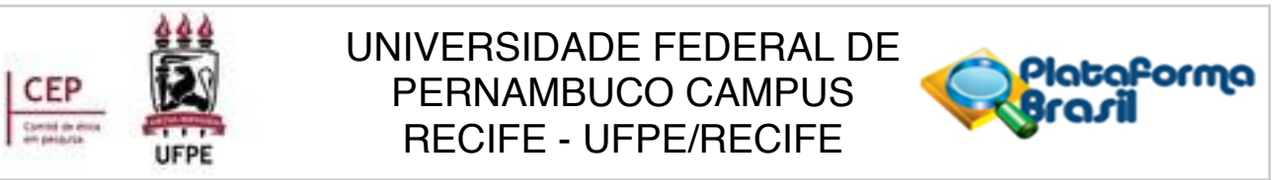
Email Security	18
Endpoint Protection Platforms	19
Error and Anomaly Detection in Finance	10
External Attack Surface Management	19
External Audit Services	11
Financial Close and Consolidation Solutions	17
Identity Governance Administration	18
Identity Verification	12
In-app Protection	14
Insider Risk Management Solutions	19
Instant Communications Security & Compliance	5
Integrated Risk Management	15
Intelligent Asset Management (IAM) Software	10
Internal Audit Services	6
Intrusion Prevention Systems	19
Investigation Management Software	6
IT Risk Management Solutions	12
IT Vendor Risk Management Solutions	17
Managed Security Services	18
Mobile Application Security Testing	14
Mobile Threat Defense	16
Network Access Control	16
Online Fraud Detection	16
Organization Security Certification Services	14
Password Management Tools	18

This table continued from previous page

Policing & Investigative Case Management Systems	11
Privileged Access Management	18
Risk Management Consulting (Worldwide)	16
Security Awareness Computer-Based Training	18
Security Information and Event Management	19
Security Orchestration	18
Security Service Edge	20
Security Threat Intelligence Products and Services	17
Third-Party Risk Management Solutions for Compliance	10
Tokenization Platform	15
User Authentication	17
Visitor Identification Software	3
Zero Trust Network Access	14
Total geral	**903**

Table 8 – List of categories and number of collected items

APPENDIX B – RESEARCH APPROVAL ON ETHICS COMMITTEE



PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: O PAPEL DA CIÊNCIA DA COMPUTAÇÃO NA GESTÃO DE FRAUDES NO CONTEXTO PRÁTICO BRASILEIRO

Pesquisador: RENATA FARIA GOMES

Área Temática:

Versão: 2

CAAE: 79945224.6.0000.5208

Instituição Proponente: CENTRO DE INFORMÁTICA

Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 7.022.897

Apresentação do Projeto:

O projeto apresenta um estudo qualitativo, baseado em entrevistas, focado em profissionais que trabalham com gestão de fraude e busca mapear ferramentas utilizadas, compreender as dificuldades enfrentadas pelos profissionais e investigar como eles percebem o papel da computação em suas rotinas de trabalho. A coleta de dados se dará de forma virtual. Os critérios de inclusão e exclusão estão claros, definindo o perfil do profissional que é alvo do estudo.

Objetivo da Pesquisa:

O projeto tem objetivo explorar a utilização de conhecimentos, tecnologias e processos de computação para a gestão de fraudes, com foco nas práticas e desafios enfrentados por profissionais brasileiros. A pesquisa adota uma abordagem qualitativa, utilizando como coleta de dados empíricos entrevistas feitas através de meio virtual (online) com profissionais que atuam em diferentes etapas do ciclo de gestão de fraudes.

Avaliação dos Riscos e Benefícios:

Riscos e benefícios estão adequados à metodologia proposta e são apresentados tanto no projeto detalhado como no TCLE e na plataforma Brasil.

Comentários e Considerações sobre a Pesquisa:

A metodologia da pesquisa está clara e traz preocupações éticas com os dados dos

participantes.

Considerações sobre os Termos de apresentação obrigatória:

Os documentos necessários estão anexados adequados às normas da CONEP.

- Folha de Rosto devidamente assinada
- Dispensa de carta de Anuência, por ser coleta virtual
- TCLE para maiores de 18 anos
- Currículo Lattes de todos os envolvidos na referida pesquisa
- Projeto detalhado no modelo do CEP, conforme normas da ABNT
- Termo de Confidencialidade
- Instrumento de Coleta de Dados (roteiro de entrevistas)
- Comprovante de matrícula/vínculo da mestranda

Recomendações:

Sem recomendações

Conclusões ou Pendências e Lista de Inadequações:

Pendências foram verificadas.

Considerações Finais a critério do CEP:

As exigências foram atendidas e o protocolo está APROVADO, sendo liberado para o início da coleta de dados. Conforme as instruções do Sistema CEP/CONEP, ao término desta pesquisa, o pesquisador tem o dever e a responsabilidade de garantir uma devolutiva acessível e compreensível acerca dos resultados encontrados por meio da coleta de dados a todos os voluntários que participaram deste estudo, uma vez que esses indivíduos têm o direito de tomar conhecimento sobre a aplicabilidade e o desfecho da pesquisa da qual participaram.

Informamos que a aprovação definitiva do projeto só será dada após o envio da NOTIFICAÇÃO COM O RELATÓRIO FINAL da pesquisa. O pesquisador deverá fazer o download do modelo de Relatório Final disponível em www.ufpe.br/cep para enviá-lo via Notificação de Relatório Final, pela Plataforma Brasil. Após apreciação desse relatório, o CEP emitirá novo Parecer Consubstanciado definitivo pelo sistema Plataforma Brasil.

Informamos, ainda, que o (a) pesquisador (a) deve desenvolver a pesquisa conforme delineada neste protocolo aprovado. Eventuais modificações nesta pesquisa devem ser solicitadas através de EMENDA ao projeto, identificando a parte do protocolo a ser modificada e suas justificativas.

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_2309580.pdf	08/08/2024 23:04:18		Aceito
Outros	RESPOSTAPENDENCIAS.pdf	08/08/2024 23:04:02	RENATA FARIA GOMES	Aceito
Outros	roteiro.pdf	08/08/2024 23:01:45	RENATA FARIA GOMES	Aceito
Outros	CartaAnuenciaPosAjuste.pdf	08/08/2024 22:59:40	RENATA FARIA GOMES	Aceito
Projeto Detalhado / Brochura Investigador	ProjetoPesquisaPosAjustes.pdf	08/08/2024 22:53:33	RENATA FARIA GOMES	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TCLEColetaVirtual.pdf	17/05/2024 17:51:36	RENATA FARIA GOMES	Aceito
Outros	confiassinado.pdf	26/03/2024 14:08:04	RENATA FARIA GOMES	Aceito
Outros	sigaa.pdf	26/03/2024 14:07:36	RENATA FARIA GOMES	Aceito
Outros	lattesvinicius.pdf	26/03/2024 14:03:17	RENATA FARIA GOMES	Aceito
Outros	lattesricardo.pdf	26/03/2024 14:02:20	RENATA FARIA GOMES	Aceito
Outros	lattes.pdf	26/03/2024 14:01:18	RENATA FARIA GOMES	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TCLE.pdf	26/03/2024 10:45:54	RENATA FARIA GOMES	Aceito
Folha de Rosto	folhaDeRosto.pdf	26/03/2024 10:43:58	RENATA FARIA GOMES	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

RECIFE, 22 de Agosto de 2024

Assinado por:
LUCIANO TAVARES MONTENEGRO
(Coordenador(a))

Endereço: Av. das Engenhasria, s/n, 1º andar, sala 4 - Prédio do Centro de Ciências da Saúde
Bairro: Cidade Universitária **CEP:** 50.740-600
UF: PE **Município:** RECIFE
Telefone: (81)2126-8588 **Fax:** (81)2126-3163 **E-mail:** cephumanos.ufpe@ufpe.br

APPENDIX C – INTERVIEW SCRIPT

UNIVERSIDADE FEDERAL DE PERNAMBUCO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO

Roteiro de entrevista

Renata Faria Gomes
PESQUISADORA RESPONSÁVEL
Mestranda em Ciência da Computação
Universidade Federal de Pernambuco
Contatos
[redacted]

Ricardo Ferreira
PESQUISADOR
Bacharel em Sistemas de Informação
Universidade Federal de Pernambuco
Contatos
[redacted]

Prof. Dr. Vinicius Garcia
PROFESSOR ORIENTADOR
Universidade Federal de Pernambuco
Contatos
[redacted]

Apresentação e Contexto

Olá [Nome do Entrevistado], meu nome é [Nome do entrevistador] gostaria de agradecer por participar desta entrevista.

- Antes de prosseguirmos com a entrevista, gostaria de me apresentar (se apresenta)

Objetivo da Pesquisa:

- Esta pesquisa visa preencher uma lacuna na literatura ao explorar a diversidade de ferramentas e conhecimentos na área da computação para profissionais de gestão de fraudes. O objetivo é contribuir para o conhecimento específico da comunidade científica e profissional.

Consentimento e Proteção dos Participantes:

- Esta pesquisa é exclusivamente acadêmica e não possui nenhum vínculo com instituições ou empresas além da UFPE.
- Medidas de mitigação estão em vigor para garantir seu conforto e segurança durante a entrevista. Se surgirem problemas técnicos ou desconfortos, faremos o possível para solucioná-los imediatamente.

Direitos e Benefícios da Participação:

- Você tem o direito de recusar participação ou retirar o consentimento a qualquer momento, sem qualquer prejuízo.
- Todas as informações fornecidas serão tratadas com total sigilo e anonimato, seguindo as diretrizes éticas e legais aplicáveis.
- Embora não haja benefícios diretos, sua participação irá contribuir para os conhecimentos da área, sendo um benefício indireto

Você possui alguma dúvida antes de iniciarmos ?

Informações gerais

1. Vamos iniciar essa entrevista conhecendo um pouco de você. Poderia me dizer seu nome e de que cidade você está falando?
2. Para nos situarmos melhor, poderia compartilhar um pouco sobre sua formação acadêmica?
3. Pode falar um pouco sobre sua trajetória profissional?
    a. Caso a formação seja relacionado a computação
        i. Como você vê a relação da sua formação acadêmica com sua carreira?
    b. Caso não tenha sido dito:
        i. Qual o nome do cargo em que você está atualmente?
        ii. Quanto tempo você faz que você está nessa área? (senioridade)
        iii. Qual o principal ramo da empresa que você atua hoje?
            1. Comércio online, banco, saúde, telecomunicações etc
4. Poderia compartilhar conosco quais os tipos de fraudes mais comuns que você enfrenta no seu dia a dia?

Integração da Computação na Gestão de Fraudes

5. Quais habilidades ou conhecimentos você considera essenciais para lidar com as demandas diárias da gestão de fraudes?
    a. Caso alguma habilidade/conhecimento esteja relacionado a computação
        i. Como você aprendeu isso?
    b. Caso não tenha sido citado:
        i. Em sua jornada profissional, houve algum conhecimento fora da sua área de especialização que você precisou aprender?
            1. Caso tenha relação com computação
                a. Como você aprendeu isso?
6. Olhando para o futuro, existe algum conhecimento que você acredita ser importante para progredir em sua carreira na área de gestão de fraudes?
    a. Caso tenha relação com computação
        i. Como você planeja aprender isso?

Explorando Ferramentas e Tecnologias

AVISAR A PESSOA QUE ESTAMOS ENTRANDO EM UMA SESSÃO DE FERRAMENTAS.

A pessoa pode ficar a vontade para citar ou omitir o nome da ferramenta. Avisar que saber o nome da ferramenta não é importante e que será um texto anonimizado na transcrição.
EX: no lugar de google docs, falar "editor de texto".

7. Quando você desempenha suas funções diárias na gestão de fraudes, quais são as principais atividades que realiza?

<< PARA CADA ATIVIDADE>>>

   a. Considerando essa <ATIVIDADE>, você utiliza alguma ferramenta para te auxiliar?
      i. Qual a função dessa ferramenta?
      ii. Quais os benefícios você enxerga ao utilizar ela?
      iii. Como você aprendeu a utilizá-la?
8. Além das ferramentas mencionadas, há outras que você usa regularmente em sua rotina de trabalho ou já usou em outras empresas?
9. Além das ferramentas que você já utiliza, existe alguma outra que você acredita ser útil no contexto de gestão de fraudes?

Contexto Profissional e Interação com profissionais

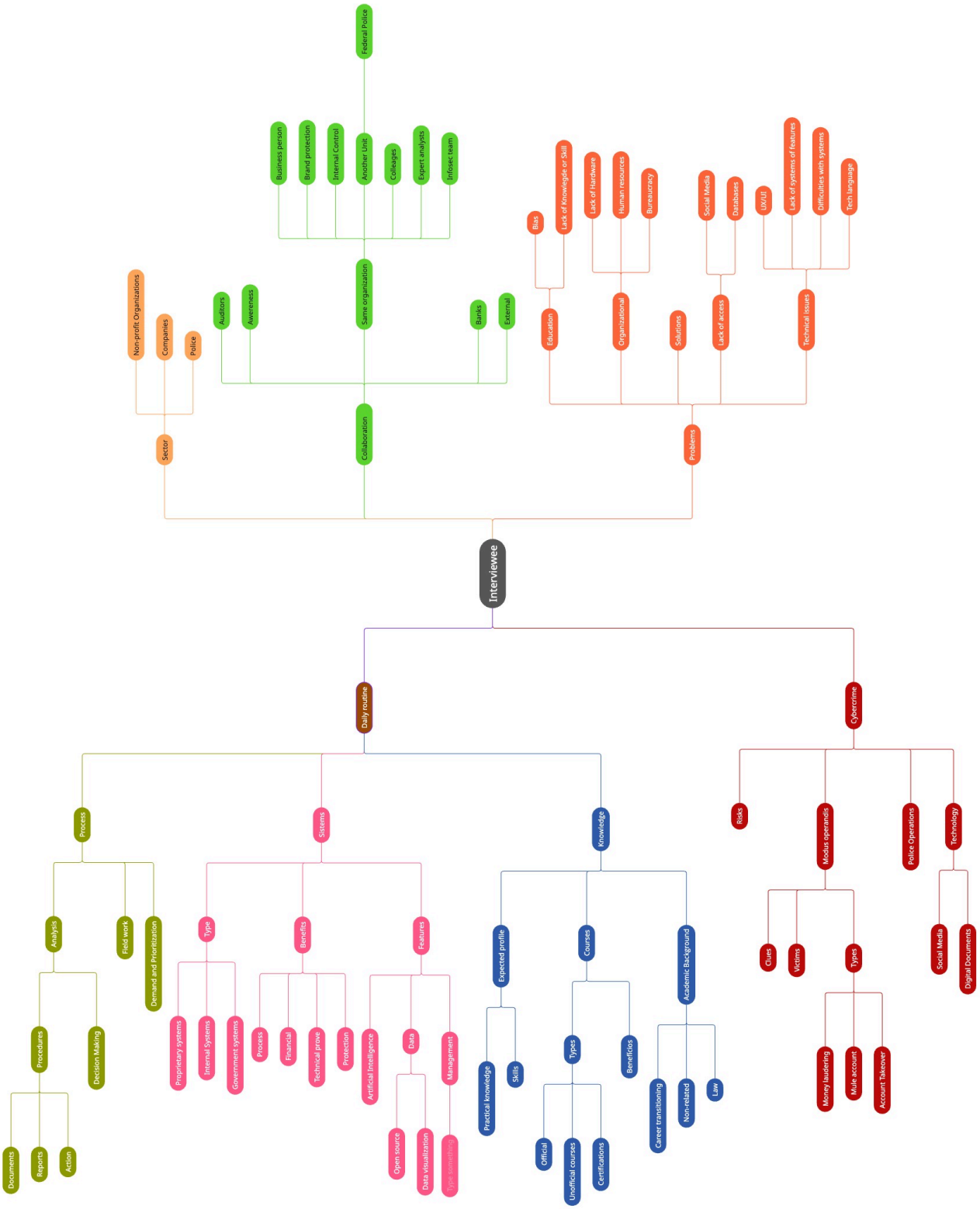
10. Quais profissionais compõem sua equipe atual ?
    a. Caso não seja citado:
       i. Qual o papel de cada pessoa do seu time?
    b. Caso tenham profissionais de TI:
       i. Como é a sua interação com esse profissional ?
11. Você costuma interagir com profissionais de outras áreas ?
    a. Caso seja com profissionais de TI:
       i. Pode falar com mais detalhes sobre essa interação? Vocês costumam conversar sobre quais tópicos?
    b. Caso não seja citado:
       i. Em experiências profissionais anteriores, você já teve a oportunidade de trabalhar com profissionais de outras áreas?
          a. Pode falar com mais detalhes sobre essa interação? Vocês costumam conversar sobre quais tópicos?

Encerramento

Mais uma vez, gostaria de expressar minha gratidão pela sua participação nesta entrevista. Suas perspectivas são valiosas e contribuem significativamente para o nosso entendimento sobre a interseção entre a gestão de fraudes e a computação.

12. Algum comentário final ou observação que gostaria de acrescentar antes de encerrarmos?

APPENDIX D – INTERVIEW CODE-MAP BY THEMATICS



APPENDIX E – RESULTS OF BENCHMARK (LIST OF EVERYTHING FOUND)

Dissuasão

Educação

- Educação de funcionários
    - Cibersegurança (phishing, social engineering, mobile security, and data protection).
    - Notifica os usuários sobre violações de políticas para promover a conscientização – security awareness training (SAT).
    - Treinamentos com certificações relacionadas às políticas empresariais
    - Possui treinamentos internos e simulações de ataques de engenharia social, de forma a preparar os funcionários da empresa
    - Identifies high-risk employees and tracks improvement.
    -
- Limitações e barreiras
    - Data de expiração de chaves e dispositivos
    - Licenças e logins com data de expiração para terceiros
    - Inspeciona e filtra os sites que serão abertos dentro da rede interna, bloqueando sites não autorizadas com base nas politicas.
    - Restringir o uso tanto da rede quanto do computador a aplicativos e sites autorizados, os demais são bloqueados
    - Controle por limite de tempo ou consumo utilizado;

Prevenção

- Interno
    - Técnico
        - Montagem de plano preventivo;
        - Proteções técnicas
            - Proteção contra ataques (SQL injection, magecart, formjacking; engenharia reversa, DDoS)
            - Proteção baseada em ofuscação / criptografia
                - Criptografia de APIs without exposing keys to applications directly.
                - Criptografia de dados
                - Ofuscação de código (proteção contra engenharia reversa)
                - Anti-tampering;
            - Proteções de rede
                - Protects endpoints, cloud workloads, and network traffic.
                - Prevents breaches, blocks malware at the point of entry.
                - Supports IPsec/SSL VPNs and Zero Trust Network Access to protect remote connections.
            - Proteções tanto baseadas em software quanto em hardware.
            - Mecanismos automatizados
                - Evitar vazamento de informações de pagamento;

        - Points of Presence (PoPs): para prevenir que o ataque derrube a operação.
- Integração
    - Integra com CI/CD de forma a encontrar problemas de segurança antes de novas versões de software;
    - Connects with SIEM, ITSM, IAM, VPN and ERP system;
    - Integração com SOAR
    - Works with threat intelligence tools.
    - Integration with GRC Tools.
- Avaliação de risco, testes e correção de problemas de segurança de softwares internos;
    - Provides assessments conducted by experienced security professionals, delivering actionable insights and remediation guidance.
    - Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST) – Simulates attacks by injecting data into web applications and analyzing responses to identify vulnerabilities;
    - Teste de penetração;
    - Performs regular scans and testing to identify potential weaknesses e vulnerabilidades;
    - Priorização de vulnerabilidades;
    - Automated Security Assessments before deployment.
    - Score de risco de vulnerabilidades;
    - Offers inspection and malware scanning for web and cloud traffic in real time.
    - Teste de vulnerabilidade, verificação inteligentes de API (se contém zero-days por ex), proteção para chaves de api
    - identify known and zero-day threats;
- Monitoria
    - Endpoint protection with 24x7 threat monitoring and management
    - Monitoramento de débitos de segurança, alertando quando existem muitos acumulados;
    - Permite detectar problemas de segurança durante fluxos de CI/CD;
    - Utilizes advanced analytics and AI models to anticipate failures and schedule proactive maintenance.
    - Real-time discovery of networks, assets, and vulnerabilities with an AI attribution engine and a large mapped risk dataset.
    - Continuously monitors and analyzes endpoint activity and behaviors.
    - Mecanismos para evitar que o serviço caia/ deixe de funcionar;
    - Monitoria de transações;

- Extends data security measures to AI applications, ensuring comprehensive protection.
- Provides deep inspection of web traffic to enforce security policies and protect against advanced threats.
- Alerts on exposures from misconfigurations, over-permissioned users, and compromised accounts.
- Threat intelligence (information about cyber threats that is analyzed and organized to help security teams prevent, detect, and mitigate cyberattacks)
    - Provides expert guidance to enhance overall security posture
    - Análise de redes sociais e Dark Web;
    - Monitors network traffic for anomalies.
    - SOC – é uma equipe interna ou terceirizada de profissionais de segurança de TI dedicada a monitorar toda a infraestrutura de TI de uma organização 24 horas por dia, 7 dias por semana.
    -
- Visibilidade da rede empresarial (e sobre sua segurança);
- Correlação entre análise de rede e threats que estejam afetando o mercado;
- Proteção granular de IPs e protocolos de rede;

- Governança, Risco e Conformidade (GRC)
    - Governança
        - Provides remote control and screen sharing features to securely access and view the screens of almost any computer, mobile device, or other endpoint.
        - Gestão de permissões & Controle de acesso;
            - Auxilia na gestão de permissões e identidades – Role-Based Access Control (RBAC);
            - Automates onboarding/offboarding processes to ensure correct access privileges;
            - Privileged Identity Management (PIM): Manages and limits admin access.
            - Zero Trust Network Access (ZTNA) – Provides secure access to applications and data based on user identity and device posture, replacing traditional VPNs with a more secure and scalable solution.
            - Granular control based on vendor ID, product ID, serial number and more.
            - Workflow Automation – Managed onboarding, offboarding, and lifecycle access requests;
            - Risk-Based Access Reviews – Prioritizes high-risk user accounts for audit.

    -
- Device management
    - Protects mobile devices across all attack vectors, including apps, files, network, and OS, zero-day exploits, ensuring corporate data remains safe.
    - Detects malware and risky applications.
- Comunicação interna
    - Email gateway
    - Ensures all communications, including messages, voice, and video calls, are securely encrypted protecting the confidentiality and integrity of messages.
    - Observa problemas relacionados aos padrões de email.
    - Uses machine learning to analyze email threats;
    - Utilizes advanced AI and machine learning to prevent sophisticated email-based attacks, including phishing and malware, before they reach end users.
    - Scans incoming and outgoing emails for malicious attachments, embedded links, and zero-day exploits.
    -
- Proteção de arquivos internos e sigilosos
    - Armazenamento seguro de arquivos;
    - Criptografia de documentos
    - Ofuscação de dados sensíveis utilizando tokens;
    - Delivers comprehensive visibility into IT assets, enabling organizations to monitor asset performance, utilization, and compliance status;
    - Near real-time asset discovery and mapping of internet-facing attack surfaces (exposed assets).
    - Build a complete inventory (domains, subdomains, IPs, cloud instances).
    - DRM – É uma tecnologia que protege conteúdos digitais contra acessos não autorizados e pirataria;
    - Uso de senhas para abrir arquivos
    - Manages and restricts the use of external devices to prevent unauthorized data transfers.
    - Data Loss Prevention (DLP): Prevents sensitive data leaks in cloud environments and prevents unauthorized data sharing.
    - Visibility and control over an organization’s data security posture.
    - Scans data assets for sensitive information (PII, financial, health data).
    - Applies real-time obfuscation and dynamic masking for sensitive data.

        - Real-time visibility into how data moves and is accessed, enabling the prevention of data exfiltration and the detection of risky behavior;
        - Monitors activities such as copy/paste, USB usage, and printing to prevent data leaks at the device level.
        - Ensures proper storage and deletion of business records.
        - Attachment Verification (Ensures that attachments are intended for the selected recipients, reducing the risk of sending sensitive information to unauthorized parties).
- Riscos – Enterprise Risk Management (ERM)
    - Risk-Based Audit Approach: Identifies financial risks and weaknesses.
    - Uso de IA para ter visibilidade da segurança de todos os ativos;
    - Informa possíveis brechas de configuração e brechas em compliance;
    - Assesses security risks across people, processes, and technology;
    - Develops risk frameworks for businesses.
    - Evaluates threats, vulnerabilities, and attack surfaces.
    - Helps organizations prevent fraud and financial crimes.
    - Identifies financial risks and weaknesses.
    - Identifies and assesses risks that could impact financial statements.
    - Continuously improves risk detection over time.
    - Provides quick analysis to expedite decision-making processes.
    - Helps organizations categorize, assess, and manage risks.
    - Analyzes how different risks are related and the potential cascading effects on the organization.
    - The platform automates the identification and remediation of data security risks.
    - Provides robust encryption and tokenization solutions to protect sensitive data at rest and in transit.
    - Streamlines the risk assessment process with automation, enabling healthcare delivery organizations (HDOs) to assess, manage, and mitigate risks across all vendors efficiently.
    - Autenticação segura
        - Autenticação com tokens
        - Internet and intranet protection – firewalls
        - Escaneamento contínuo de vulnerabilidades e de rede através de IA;
        - Utilização de dispositivos como fator de autenticação;
        - Método de autenticação por hardware (YubiKey)

            - Offers comprehensive DNS security solutions to protect against threats such as DNS tunneling and cache poisoning;
            - Authenticates users and devices continuously before granting access to applications, enforcing least-privilege principles.
            - Provides secure credential storage, automated password rotation, and detailed session auditing.
        - Validação de falsos positivos.
    - Conformidade
        - Identificar violações de políticas
        - Provides logging, reporting, and access review workflows to meet regulatory requirements.
        - Extends DLP policies (defines how your organization shares and protects data without exposing it to unauthorized users.) to network traffic and cloud apps, covering email, web uploads, and SaaS platforms.
        - Identifies potential compliance and security risks.
        - Uses AI and machine learning for automated risk detection in financial reporting.
        - Monitoria interna de mensagens de funcionários para verificação de brechas na política;
- Externo
    - Terceiros
        - Avaliação de risco de fornecedores (ou terceirizados);
        - Monitora ferramentas de terceiros utilizadas;
        - Atua com IA para detectar problemas de segurança em sistemas de terceiros.
        - Evaluates vendors and business partners for compliance risks.
        - Gestão de terceiros;
        - Faz cálculo um score de risco de cada terceiro;
        - Verificação de riscos em ferramentas terceiras;
        - Auxilia que a empresa compartilhe com terceiros problemas de segurança, de forma a ter uma troca mais dinâmica entre organizações;
        - Analyzes permissions, data leaks, and third-party SDK risks.
        - Due dilligence de clientes;
        - Avaliação da efetividade dos controles de segurança atuais impostos pela empresa;
        - Provides simple, secure remote access for trusted vendors connecting to your systems, eliminating the need for VPNs and known credentials.
        - Real-time visibility, persistent monitoring, and automated control across all network device vendors and connected endpoints.

            - Provides continuous monitoring capabilities, delivering security ratings of a third-party vendor's organizational risk posture with a comprehensive 'outside-in' view of security risks.
- Mistos
    - Mecanismos de proteção de sessão (Strengthens security against account takeovers)
        - Externa
            - Tokenização de pagamentos
            - Identifies risks of app cloning, code manipulation, and IP theft.
            - Lista PEP e de perfis prováveis fraudadores;
            - Score de risco;
            - Monitoria de clientes;
            - KYC automatizado; – background checks;
            - Verificação de identidades (documentos) globais e em diversos formatos;
            - Integração com sistemas bancários
            - Faz controle seguro de cartões de crédito;
            -
        - Ambas
            - MFA
            - Criptografia
            - Token authentication
            - Identifica vazamento de credenciais;
            - Identified malicious apps and data-leaking permissions.
            - SSO
            - Enables biometric and token-based logins.
            - Adjusts security requirements based on user behavior and risk factors.
            - Utiliza biometria (facial ou de fingerprint) e comportamento para autenticação de usuários;
            - Utiliza autenticação baseada em risco;
            - Faz verificação real-time antes de garantir acesso;
            - Criptografia da identidade do usuário;
            - Gera certificados digitais para rede
            - Detects and blocks DNS-based threats like phishing and malware;
            - Previne que fraudes aconteçam em pagamentos, já que existe todo um controle de dados financeiros
            - user behavior analysis;
    - Mecanismo de CAPTCHA.

Detecção

- Automação
    - Filtro de tráfico

    - Quarantines and blocks malicious emails (phisihng)
    - Identifies and automatically blocks unauthorized user access with real-time prevention and adaptive false positive filtering
    - Utiliza IA para detectar anomalias, padrões de ataques e trazer mecanismos imediatos de defesa
    - Blocks phishing sites and malicious Wi-Fi hotspots
    - Blocks unauthorized devices and network intrusions (high-risk endpoints)
    - Bloqueio de URLs suspeitas (evitando phishings)
    -
- Alertas & marcações
    - Alerta para tentativas de acessos irregulares
    - Flags unauthorized actions by employees
    - Inclui alertas e uso de IA para detectar problemas
    - Monitoramento de possíveis riscos de data leak, roubo de informações, vazamentos de dados e violações de políticas de segurança
    - Tracks who accesses data and detects suspicious activity
    - Detecta vazamento de informações como credenciais
    - Detectam problemas com a senha, como vazamentos, solicitando troca imediata
    -
- Detecção de padrões e anomalias
    - Flags suspicious data movement
    - Checagem de anomalias
    - Identifies inconsistencies and potential fraudulent activities in documents (isso aqui é durante, por exemplo, ao fechar contratos)
    - Tecnologias de detecção de comportamentos/ padrões suspeitos
    - Regras customizadas e correlações para detectar possíveis incidentes
    - Possui mecanismos para verificar anomalias nos perfis dos usuários
    - Uso de IA para detecção de padrões ruins como bots, contas falsas etc
    - Detected unusual app activity and unauthorized data access
    - Uses AI-driven analytics to detect anomalies
    - Learns individual user behavior to detect anomalies and potential security threats
    - Utiliza IA para detectar anomalias, padrões de ataques e trazer mecanismos imediatos de defesa
    - Utiliza dados anteriores (de usuários, dispositivos e aplicações) para configuração de modelos de detecção
    - Utilizes AI, machine learning, and heuristics to identify malicious and suspicious threats
    - Detected unusual app activity and unauthorized data access
    - Verificação de atividades suspeitas ou manipulações em tempo de execução
    - Ataques / problemas específicos
        - Uses AI to detect malware, phishing, and data exfiltration attempts
        - Monitoria em realtime de ataques baseados em identidade (tais como roubo de credenciais e escalação de privilégios)

        - Identifica ataques como phishing, spoofing, impersonation, hijacking, ransomware, online fraud, and data exfiltration
        - Monitoramento e detecção automática de diversos ataques: DDoS, bot attack, ATO, injection, API scraping etc
        - Defends against common OWASP threats (SQLi, XSS, CSRF), as well as emerging attack patterns targeting APIs and microservices
        - Detecção de fraudes e crimes como lavagem de dinheiro
        - Detects and prevents Segregation of Duties (SoD) violations to mitigate internal fraud risks
        - Utiliza IA para detectar produtos falsos (relacionados a marca), vendedores falsos de modo a evitar engenharia social e phishings
        - Utiliza IA para verificar erros de pagamentos/ fluxo de caixa
        - Identificação de ataques pass-the-hash e pass-the-ticket e roubo de credencial
        - Detecção de SQL injection, XSS e CSRF
        - Validação de inputs e ataques brute-force
        - Detecta ATO, lateral movement, and ransomware propagation, utilizando MFA adaptativo.
- Autenticação e Identidade
    - MFA
    - KYC (Know Your Customer)
    - AML (Anti-Money Laundering) Compliance
    - Detects synthetic identities, deepfakes, and stolen IDs
    - Uses AI to detect compromised accounts
    - Verificação de dispositivo – Uso de fingerprint de dispositivos, considerando localização, ip entre outros
    - Possui biometria comportamental
    - Lets users call or email directly from the CRM and automatically logs all interactions
    - Utilização de ML para análise de comportamento de usuários de entidades
    - Learns individual user behavior to detect anomalies and potential security threats
    - Employs threat intelligence, behavioral analysis, and automated workflows to rapidly identify and contain threats
    - Biometria com ML
    - Algoritmos avançados para comparar nomes
    - Behavioral Analytics & Risk Scoring, flagging suspicious user activity
    - Marca contas com suspeita alta de fraude
    - Liveness
    - Utilização de biometria de voz
    - Documentoscopia (OCR)
    - AI-supported video streaming to verify user identities
    - Watchlists, sanctions list and risk database
-
- Segurança em aplicações

    - Rede
        - Threat detection for HTTP and HTTPS traffic
        - Uso de IA e ML para detecção de anomalias (em nuvem) e potenciais ataques de intrusão
        - Network and host intrusion detection
        - Blocks malicious domains and IPs at the DNS layer, preventing threats before they reach the network or endpoints
        - Verificação de Malwares
        - Enables secure (VPN) connections for remote workers
        - Allows granular, attribute-based access controls for specific IP ranges, geographies, or request attributes
    - Dispositivos
        - Detecção de ameaças vindas de dispositivos
        - Identifies apps that may access personal information without consent
        - Blocks infected or non-compliant devices
        - Detects and removes malicious applications and files
        - Checks devices for compliance (OS updates, antivirus status, etc.) before granting network access
    - API
        - Inspects and validates API traffic (REST, SOAP) for malicious payloads or protocol misuse
        - EDR (endpoint detection and response)
        - Offers SSL certificates and ensures secure data transmission between the website and its users
    - Outros
        - Integrates across 300+ third-party tools and supports 2,800+ automated actions, connecting and coordinating complex workflows across teams and tools
        - Supports TDE, Always Encrypted, and auditing
        - Offers the flexibility to create custom rules tailored to specific application needs, allowing organizations to fine-tune their security posture
        - RASP – Runtime application self-protection (RASP) is a security technology that uses runtime instrumentation to detect and block computer attacks by taking advantage of information from inside the running software
- Transações
    - Utiliza informações anteriores (como chargeback, fraudes, informação de dispositivos, KYC etc) para gerar um score e decidir se deveria ou não continuar a transação
    - Identifica transações suspeitas - Identifies high-risk financial transactions.
    - Utiliza análise de relacionamento entre clientes suspeitos
    - Possui scoring de comprometimento de urls
    - Verifica uso diferente do padrão de meios de pagamento

        - Quando existe algum tipo de padrão suspeito nos pagamentos, essas ferramentas ajudam a detectar
- Score
    - Score de risco calculado com ML
    - Cálculo de score
    - Utilização de score da transação por meio de IA para bloquear acessos

Mitigação

- Auxílio técnico especializado
    - Estratégia pré-incidente
        - Faz planejamento operacional para reduzir o tempo de recuperação de incidentes.
    - Treinamentos
        - Enables security teams to investigate and respond to attacks.
        - Documentação de ações tomadas para remediar problemas.
        - Propostas de plano de mitigação.
        - Auxilia no desenvolvimento de estratégias para o caso de um incidente de segurança acontecer.
        - Auxilia na criação de estratégias para mitigar problemas e reduzir impactos.
        - Provides IT governance and risk mitigation strategies.
        -
    - Ações durante incidentes
        - Provides guided response actions to contain threats.
        - Delivers detailed remediation guidance.
        - Remediation guidance during security events.
        - Identifies and mitigates risks like phishing, malware, and data leakage in real-time.
        - Auxílio para remediar problemas de segurança.
        - Forensic analysis to quickly address and resolve DLP incidents.
    - SOC
        - Security Operations Centers (SOCs) to detect and respond to threats in real-time.
        - Se conecta com o SOC, providenciando uma resposta rápida para incidentes.
- Automação
    - Respostas
        - Automated Incident Response.
        - Automated Investigation & Remediation.
        - Possui automações de respostas a incidentes, que mitigam imediatamente problemas com vazamento de informações.
        - Automated Threat Mitigation workflows.

        - Automates security workflows for known attack patterns.
        - Criação de regras personalizadas e workflows para automatizar a resposta a possíveis ataques.
        - Possibilidade de configurar respostas automatizadas no caso de detecção de ataques.
    - Bloqueios
        - Automação de bloqueios a possíveis ataques.
        - Bloqueio de acessos suspeitos.
        - Bloqueios de URLs e/ou tráfico de rede suspeito.
        - Automated Threat Remediation – Identifies and removes malicious emails.
        - Bloqueio do sistema de um usuário específico.
        - Isolamento de dispositivo.
        - Para a execução do app em caso de tentativa de engenharia reversa.
        - Usam IA para parar o ataque.
        - Provides automatic protection from vulnerabilities by analyzing web traffic and blocking malicious requests, ensuring that applications remain secure without manual intervention.
    - Correções automáticas
        - Aumentam e distribuem tráfego anormal de modo a não derrubar o sistema.
        - Redirects non-compliant devices to security updates before granting access.
        - Isolates non-compliant endpoints and guides users through steps to fix issues before granting full access.
        - Eliminar mensagens de e-mail.
        - Differentiates legitimate user activity from bots or scrapers, enforcing rate limiting or blocking suspicious traffic.
        - Automatiza solicitações para derrubada de sites falsos.
    - Resiliência de serviços
        - Ensures email availability even during service outages.
- Controles remotos
    - Possibilita emissão/ revogação de credenciais remotamente.
    - Acompanhamento em tempo real do status da mitigação.
    - Permite acesso remoto a dispositivos na rede.
- Análise e insights
    - Utilização de dados real-time e ML para identificar onde pode estar o possível ataque ou violação da política da empresa.
    - Realizar uma análise antivírus etc.
    - Incident tracking and disaster recovery plans.
    - Provides detailed insights into attack vectors and methods for effective remediation.
    - Análise em tempo real de possíveis ataques, com alertas e planos para remediar.

    - Possui um dashboard visual para auxiliar a gestão.
    - Insights real-time para auxiliar na tomada de decisão rápida.
    - Facilitates the tracking and resolution of incidents to minimize impact.
- Melhorias de segurança
    - Learns application behavior and refines detection logic to reduce false positives and improve threat detection.
    - Identity Analytics – Utilizes AI to enhance access decision-making and automate compliance processes.
- Alertas e Notificações
    - Alertas sobre uso suspeito;
    - Trás alertas de problemas para que medidas sejam tomadas o mais rapidamente possível.
    - Generates immediate notifications for identified issues, enabling prompt resolution.
    - Providing early breach warnings.
    - Alerts on employee credential leaks.
    - Enriches alerts with context from threat feeds, reputation services, and threat intelligence platforms.
    - Real-time alerts.
    - Trás alertas e detalhes específicos sobre o que causou o problema.
    - Utiliza automações para alertar sobre vulnerabilidades e iniciar um processo de remediação.
    - Monitors data access patterns to alert on suspicious activities.
- Suporte Financeiro e Transnacional
    - Algumas plataformas auxiliam a repor dinheiro que foi retirado de forma incorreta de terceiros.
    - Acelera o processo de cobrança de pagamentos não efetuados.
    - Offers case management.
    - Uses AI to detect financial anomalies, patterns and fraud (após a fraude ocorrer).
    - Fornece ferramentas para automatizar reconciliações de contas.

Análise

- Voltado a melhorias
    - Delivers detailed reports on security posture, incidents, and improvement recommendations
    - Trás, de forma automática, relatórios sobre os ataques e métricas dos sistemas
    - Gera relatórios com possíveis vulnerabilidades e sugestões para corrigir o problema
    - Gera relatórios que ajudam a entender problemas encontrados e problemas detectados
    - Trás relatórios e insights de melhorias
    - Traz insights de melhoria e de onde estão os potenciais riscos

    - Provê insights para desenvolvedores a respeito de eventos e ataques potenciais
    - Resume logs e dados em sugestões de melhorias
    - Delivers detailed insights into data usage patterns, user behavior, and potential insider threats
    - Faz análise da causa-raiz e traz insights para melhoria de processos da empresa
    - Provides insights on case volume, resolution times, and investigation outcomes
    - Possui mapeamento com métricas e gráficos sobre pontos de segurança a serem melhorados
    - Relatórios e dashboards avançados para auditoria, incluindo insights de onde melhorar, quais as ações necessárias entre outras
    - Possui compartilhamento de dados para melhoria nas estratégias de antifraude
    - Provides actionable insights and best-practice recommendations for improving internal controls, business processes, and overall risk management
    - Uses machine learning to mitigate emerging threats in real time
    - Incorporates advanced analytics tools to enhance risk identification, detect anomalies, and improve audit quality
    -
- Voltado a reanálise detalhada
    - Auxílio de ML para classificar e analisar dados que possuem maior risco
    - Prioritizes high-risk transactions for deeper review
    - Representação visual das ameaças existentes
    - Tracks database transactions for unauthorized access
- Voltado para acompanhamento RealTime
    - Comprehensive dashboards for security posture tracking
    - Insights em realtime, trazendo contextos e riscos de todas as autenticações e tentativas de autenticação
    - Provides insights into user behavior and fraud detection
    - Provides real-time insights into risk exposure
    - Provides reports and dashboards to help teams track improvements over time
    - Dashboards para auxílio da identificação de padrões, com alertas configuráveis
    - Provides a unified portal for accessing critical systems with session recording and monitoring
    - Tracks organization-wide susceptibility, reporting rates, and improvements over time
- Sem detalhes
    - Delivers real-time notifications
    - Provides real-time monitoring and alerts
    - Agregação de dados de escaneamentos automáticos
    - Integração com bancos de dados, dando insights em real time
    - Integrates with machine learning and analytics services to derive insights from data
    - Ferramentas Analíticas e Recursos Visuais
        - Dashboards com gráficos
        - Mantém logs e utiliza normalização de dados para auxiliar a análise

        - Uso de UI para buscar, salvar informações e customização de reports
        - Ferramentas visuais para fluxos de dados e transformações para entender as origens e o uso dos dados
        - Centralização de metadados e trazer visibilidade
        - Provides built-in intelligence tools, such as reporting dashboards, charts, maps, and graphs, to help make sense of gathered metrics and data
        - Dashboard customizável em tempo real do status da operação
        - Centralized dashboard
        - Dashboards com gráficos
        - Provides security dashboards and reporting
        - Offers a centralized dashboard for managing security across the entire organization, providing instant visibility of network security
        -
- Política / compliance / governança / risco
    - Também auxilia no entendimento e comprovação de que o software está dentro das políticas e regulações necessárias
    - Provides dashboards and reports for compliance teams
    - Provides dashboards and reports for auditing
    - Auxiliar na padronização de termos em diversos setores
    - Provides role-based dashboards for real-time insights into compliance and risk status
    - Relatórios e dashboards avançados para auditoria, incluindo insights de onde melhorar, quais as ações necessárias entre outras
    - Representação visual do processo de auditoria
    - Dashboards com detalhes do atendimento de compliance de terceiros
    - Provides real-time tracking of key risk indicators and compliance violations
    - Uses data analytics, automation, and continuous controls monitoring to enhance the accuracy and timeliness of audit results
    - Includes features to monitor security events and compliance status
    -
- Específico para Negócios/ Financeiro
    - Auxílio na criação de relatórios financeiros
    - Offers dashboards and reports to monitor key performance indicators and response effectiveness
    - Traz análises detalhados sobre o contexto, indicadores entre outros itens
    - Gera relatórios, gera e organiza dados analíticos de forma inteligente
    - Insights correlacionados com contexto de negócios feitos por IA
    - Possui ferramentas de análise poderosas, que apresentam gráficos resumidos sobre pagamentos efetuados e pendentes
    - Traz dados de segurança de forma visual, de forma a auxiliar comunicação com pares menos técnicos
    - Traz informações de pagamento por meio de dashboards (alguns em Real-Time)
- Integration of bot mitigation and Layer 7 DDoS protection (Responds to threats in real-time with automated blocking and rate-limiting.)

Políticas

- Helps meet requirements – GDPR, HIPAA, FCPA, PSD2, PCI DSS, SOC 2, ISO 27001, IFRS, CCPA, SOC 2, SEC, PCAOB, ESIGN e eIDAS, SOX, anti-bribery laws, FATF, FinCEN
    - Policy templates and audit-ready reporting.
    - Adheres to strict data security protocols, including encryption, role-based access, and compliance with regulations
    - Ajuda a seguir regras por meio de processos automatizados.
    - Assists organizations in meeting regulatory requirements by securing data and providing necessary compliance tools.
    - 164.Supports regulatory compliance by mapping security risks.
    - Auxilia na documentação e no processo para cumprimento de medidas regulatórias
    - Cumprimento de regulações relacionadas a assinaturas (ESIGN e eIDAS)
    - Possui modelos prontos de relatórios de regulamentações;
    - Compliance audits and regulatory guidance
    - Comply with legal regulations, functional requirements (LEITSC, UCADFR), data exchange standards (NIEM, GJXML, ODBC), data encryption (CJIS), and reporting protocols (NIBRS, NFIRS).
    - Generates reports to demonstrate adherence to security policies and regulations.
    - Ensured corporate policies on BYOD and managed devices
    - Allows organizations to assess their compliance with quality standards;
    - Generates comprehensive reports to demonstrate adherence to regulatory requirements.
    - Preenchimento automatizado de regulamentações;
    - Regulatory compliance assessments.
    - Provides guidance on financial reporting obligations.
    - Addresses industry-specific regulations and provides guidance on emerging requirements.
    - Atendimento das regulamentações FATF, FinCEN e diretivas do AML;
    - Auxilia a fazer relatórios que as regulamentações exigem;
    - Identifies, assesses, and mitigates risks while ensuring regulatory compliance
    - Suporte em questões de compliance e regulamentação;
    - Tracks incidents and ensures regulatory compliance.
    - Identifies compliance gaps and manages regulatory risks.
- Políticas internas (e auditoria interna)
    - Applies context-aware policies to control how sensitive data can be shared (e.g., blocking emails with PII, encrypting attachments).
    - Automates the enforcement of communication policies across various channels.
    - Manages the creation, approval, and dissemination of organizational policies.
    - Adaptação de políticas baseadas em roles, saúde do dispositivo, localização entre outras.

    - Garante que os dispositivos estejam seguindo as políticas de segurança de redes.
    - DRM (Políticas de copyright);
    - Ferramentas para detectar não-conformidades.
    - Offers a unified console for deploying, configuring, and managing security policies across all endpoints.
    - Identificação inteligente de violações da política;
    - Restricts data access based on policies.
    - Provides insights into security and compliance risks.
    - Enables automation of security processes based on policies;
    - Workflow Automation – Reduces manual compliance tasks.
    - Customização de regras para se adequar à politica da empresa.
    - Traz medidas de privacidade de informações;
    - Zero-trust policy
    - Workflow Automation – Reduces manual compliance tasks.
    - Detecta gaps dentro do compliance empresarial.
    - Centralized repository for corporate policies with automated workflows for approvals and updates.
    - Automated Policy Management: Streamlines document distribution and enforcement.
    - Manages the creation, approval, and dissemination of organizational policies.
    - Políticas para proteção contra Malwares;
    - Compliance-focused training modules.
    - Adaptação de políticas baseadas em roles, saúde do dispositivo, localização entre outras;
    - Policy Lifecycle Management;
    - Workflow Automation – Streamlines policy approvals and compliance processes (Reduces manual effort in compliance tracking).
- Acompanhamento Real time
    - Monitors and classifies sensitive data (PII, financial records, IP) in real time.
    - Analisa mudanças em dados sensíveis.
    - Visibilidades de brechas na governança empresarial;
    - Provides real-time monitoring dashboards.
- Governança (acessos e privilégios)
    - Enforces least-privilege access principles.
    - Fornece um repositório centralizado de controles para facilitar a gestão.
    - Trabalha com SAML, OAuth e IAM.
    - Zero Trust Network Access (ZTNA): Implements least privilege access controls.
    - Controle de acesso;
    - Examines internal controls across various operational and financial processes to ensure compliance and efficiency;
    - Controles automáticos baseados em contratos (Seja expirados, sejam contratos não assinados);
    - Detecção de mudanças de privilégios indevida;

    - Manages user roles, permissions, and policies.
    - Detects and prevents conflicts in user permissions.
    - Group Policy Management: Simplifies GPO administration and enforcement.
    - Integração com sistemas de compliance e governança;
    - Centralização de informações, relatórios, políticas, procedimentos entre outros que estão relacionados a políticas com controle de acesso;
    - Possibilidade de ‘ligar e desligar’ métodos de autenticação com base em horários;
    - Fornece um repositório centralizado de controles para facilitar a gestão.
    - Automação de dispositivos conectados (de forma a dar visibilidade);
    - Cataloga dados e metadados, auxiliando na gestão de dados (incluindo processos e pessoas) de toda empresa.
    - Garante que os dispositivos estejam seguindo as políticas de segurança de redes;
- Riscos
    - Análise de impacto em mudanças nos sistemas.
    - Third-party risk management, vendor compliance checks, automated audits.
    - Auto-implementa políticas baseadas em novos tipos de ataque para bloquear furos de segurança;
    - Third-party risk management, vendor compliance checks, automated audits.
    - Supports regulatory compliance by mapping security risks.
    - Automatiza fluxos de trabalho de conformidade e risco para aumentar a eficiência.
    - Análise de impacto em mudanças nos sistemas.
    - Gestão de Acessos e Identidades:
        - Automatizar fluxos de trabalho de conformidade e risco para aumentar a eficiência.
        - Permite gestão inteligente de identidades, segurança e dispositivos.
        - Possibilidade de ‘ligar e desligar’ métodos de autenticação com base em horários.
        - Dynamically adjusts access rights based on real-time context (user risk, device compliance).
        - Consegue modificar permissões de funcionários de forma fácil;
        - Trabalha com SAML, OAuth e IAM;
        - Permite gestão inteligente de identidades, segurança e dispositivos;
- Organização da auditoria
    - Organizes and stores evidence securely in the cloud or on-premises.
    - Deixa materiais para auditoria organizados.
    - Cataloga dados e metadados, auxiliando na gestão de dados (incluindo processos e pessoas) de toda empresa.
    - Automates legal discovery and document review processes.
    - Assists organizations in aligning internal audit functions with corporate governance requirements and regulatory frameworks (e.g., Sarbanes-Oxley, SOC).

- Planejamento e execução de auditorias;
- Audit logs for compliance; Possui registros (e logs) auditáveis.
- Discovers, manages, audits, and monitors privileged accounts at the enterprise level.
- Auxilia a interação entre diversos auditores;
- Supports corporate governance by providing insights on internal controls and risk exposures to audit committees and executive management.
- Automação de auditoria de tercerizados
- Automação de auditorias de software;
- Relatórios
    - Allows customization of fields, templates, and rules to fit the unique needs of an organization, adapting workflows accordingly.
    - Auxílio para elaborar relatórios regulatórios.
    - Generates detailed reports to support audit findings and compliance efforts.
    - Relatórios automáticos recorrentes;
    - Comprehensive reporting and compliance tracking;
    - Gera relatórios a fim de demonstrar que está de acordo com as regularmentações;

Investigação

- Proteção de dados de investigação
    - Strong encryption, two-factor authentication, and robust security protocols (Ensures that sensitive investigative data is stored and transmitted securely, maintaining confidentiality and integrity.);
    - Provides secure archiving of communications for legal and compliance purposes
    - Enforces strict authentication policies
- Auxílio técnico e pericial
    - Assists in investigating potential fraudulent activities
    - Busca possíveis vetores que causaram o ataque, além de um relatório sobre o ataque
    - Supports financial audit and risk management frameworks
    - Auxilia na condução de relatórios de auditoria e pós-incidente
    - Facilitates internal audits and regulatory compliance
    - Supports the planning, execution, and reporting of audits
    - Terceirização de análise
        - Enables proactive investigation of security incidents
        - Investigates financial irregularities. Forensic Accounting

        - Faz investigação forense de incidentes
- Acompanhamento de tratativas
    - Monitors risk treatment actions.
    - Tracks incidents and ensures regulatory compliance
    -
- Evidências Digitais
    - Detecção de dados passíveis de investigação
        - Fraud Investigation & Forensic Auditing – Detects irregularities and fraudulent transactions
        - Uses AI-driven analytics to detect anomalies in financial transactions
        - Identifies high-risk financial transactions
        - Tracks security incidents, fraud cases, and non-compliance issues with AI-driven insights
        - Logs auxiliam na investigação de possíveis ocorrências
    - Coleta de dados
        - Automated data extraction and analysis tool for financial documents
        - Captura logs para auditoria posterior
        - Automates evidence collection
        - Preserves electronic records for litigation and regulatory investigations
        - Retrieves deleted and hidden files for investigations.
        - Uses AI to extract insights from videos, images, and documents
        - Captures and records privileged sessions for audit purposes
        - Log de ações para auditorias
        - Mantém logs de diversas fontes e utiliza normalização/correlação de dados para auxiliar a análise
        - Registros de logs relacionados ao uso de recursos e seus acessos
        - Telemetria forense
        - Tracks user activity for regulatory reporting
        - Logs security events and tracks responses
        - Logs security breaches and anomalies
        - Possui logs que identificam padrões do ataque
    - Plataforma para visualização / organização de dados
        - Agrega informações de diversos locais para gerar insights para diversos profissionais, incluindo investigadores internos, externos e da polícia
        - Auxilia na visualização passo-a-passo do ataque, tornando claro de onde surgiu o ataque, qual foi a causa e qual a severidade
        - Offers the ability to link related cases, providing a comprehensive view of interconnected incidents and entities
        - Organizes digital evidence for quick retrieval.

        - Links evidence to case files for streamlined investigations
        - Organizes digital forensics data
        - Helps investigators organize documents, interviews, and evidence in one system
        - Combine data sources
        - Empower investigators with intuitive visualisation tools to bring data to life
        - Centralizes security incidents for investigation
        - Offers a centralized repository for storing all case-related information, ensuring data is safe, secure, and searchable
        - Possui ferramentas para identificação do autor dos ataques
        - Relatórios automatizados
            - Relatórios automatizados
            - Generates legal and forensic documentation
            - Tracks policy violations and generates reports
            - Audit Trail & Reporting
- Tomada de decisão
    - AI-powered insights and search tools to enhance the intelligence management
    - Offers a platform for managing and analyzing investigative data, aiding organizations in uncovering insights and making informed decisions
    - Use entity matching technology to automatically uncover links within the data
    - Easily uncover insights, identify new leads, and drive informed actions that enhance investigative outcomes
    - Leverage a focused AI model to enhance investigative precision. The AI guides investigators through a consistent process, helping to identify, analyze, and map relevant evidence to key case elements
- Trabalho colaborativo
    - Facilitates task segmentation, assignment, and documentation, ensuring a cohesive and collaborative investigative process
    - Enables secure collaboration between agencies
    - Fluxos de trabalho de investigação integrados e colaborativos
- Integrações com outros sistemas
    - Integrates with various identity providers and logs all access attempts for compliance
    - Integração com sistemas e plataformas, de forma a trazer automaticamente evidências, mudanças e outras informações

Acusação

- Automação
    - Tirar do ar sites falsos

        - Montar relatório forense, incluindo dados coletados
        - Montar outros documentos necessários para a acusação (excel, documentação)
        - Templates para diversos procedimentos
- Uso de IA e NLP
    - Coleta de dados de forma inteligência (para encontrar culpado)
    - Revisão dos relatórios de inquérito
- Integrações com sistemas
    - Integração com sistemas do governo
    - Integração com sistemas regulatórios
    - Integração com sistemas de investigação