ICT Strypes

Plan for the Prevention of Risks of Corruption and Related Infractions

2025-2028

Regulatory Compliance Officer	Jolanda dos Santos
General responsible for the implementation, control and review of the PRP	Jolanda dos Santos

Documentary control

Version No.	Approval	Notes	Review
01			

Acronyms

Acronym	Definition
EU	European Union
MENAC	National Anti-Corruption Mechanism
PPR	Plan for the Prevention of Risks and Corruption and Related Infractions
RCN	Regulatory Compliance Officer
RGPC	General Regime for the Prevention of Corruption

Table of Contents

Introduction

ICT Strypes Technical Software, Unipessoal Lda. (hereinafter, "ICT Strypes") is a Portuguese-Dutch software development company, based in Lisbon and Porto.

ICT Strypes is one of several specialized companies that are part of ICT Group B.V., acting in a coordinated manner to offer strategic solutions adapted to the needs of its customers.

With extensive experience in complex software projects, ICT Strypes is able to fully execute in-house, from the development of low-level characterized software for hardware control to the implementation of middleware applications, adopting agile methodologies and ensuring efficient and end-to-end solutions.

Through the combination of innovation, precision and technology, ICT Strypes aims to create integrated software solutions that expand the limits of what is possible, always as a point of focus beyond technology - valuing the deep knowledge of its customers and the markets in which they operate, allowing it to deliver customized and high-impact solutions.

ICT Strypes combines the most advanced technologies with its dedication and experience, maintaining a firm commitment to customers, and develops strategic partnerships that produce innovative, efficient and high-impact solutions.

In view of the growth of regulation and the need to reinforce responsible and transparent management practices, ICT Strypes has developed this Risk Prevention Plan (PPR), with the aim of ensuring full compliance with the General Regime for the Prevention of Corruption (RGPC), established by Decree-Law No. 109-E/2021.

This document aims not only to ensure alignment with the Portuguese regulatory framework, but also to strengthen the business integrity and internal control mechanisms adopted by ICT Strypes.

For its preparation, a detailed analysis of the company's organizational structure and operational processes was carried out, focusing on the identification, assessment and mitigation of risks associated with acts of corruption and related infractions. Based on this diagnosis, preventive and corrective measures were defined, consolidating a robust

risk management model in line with the best international practices.

In addition to ensuring compliance with the obligations provided for in the RGPC, especially in its article 6, this PPR has as its main objective to foster an organizational culture based on transparency, ethics and corporate responsibility.

The implementation of this plan reaffirms ICT Strypes' commitment to the prevention and mitigation of corruption risks and related infractions, promoting a solid and sustainable management model, essential for an honest and safe business environment.

I. Initial provisions

1. Framework

The General Regime for the Prevention of Corruption imposes a set of obligations and opportunities that must be implemented by ICT Strypes.

Decree-Law No. 109-E/2021, of 9 December, which establishes and regulates the General Regime for the Prevention of Corruption (RGPC), applies, among other public and private entities, to companies headquartered in Portugal and to branches in national territory of foreign companies that employ 50 or more workers.

This diploma, in addition to recognising the need to adjust some aspects of the repressive system, considers it essential to strengthen and enhance the mechanisms for preventing and detecting corruption crimes and related offences and is structured around the following pillars:

1. The National Anti-Corruption Mechanism (MENAC), which is responsible for monitoring the implementation of the regime:
    a. issues guidelines and directives on regulatory compliance programs;
    b. evaluates the application of the GDPR;
    c. defines the planning of control and supervision;
    d. supervises compliance with the rules;
    e. initiates, instructs and decides on proceedings relating to the practice of the administrative offences provided for therein;
    f. manages information on compliance with standards;
2. The regulatory compliance program integrates four instruments:
    a. plan for the prevention of risks of corruption and related infractions (PPR);
    b. code of ethics and conduct;
    c. training program;

d. reporting channel.

3. Measures to ensure the independence and impartiality of the members of its governing bodies, managers and employees.

In view of the increasing level of scrutiny to which organizations are subjected, both by regulatory and supervisory entities and by civil society, it is essential that companies adopt processes and systems that minimize the risk of non-compliance with laws, regulations and internal standards.

In addition, the organizations with which ICT Strypes maintains business relationships increasingly require its partners to adopt robust policies, processes and controls to ensure compliance with applicable laws and regulations.

In this way, it is possible to manage reputational risks and promote continuous improvement of the *compliance process*, which includes the following elements:

- Plan for the Prevention of Risks of Corruption and Related Infractions (PPR);
- Code of Ethics and Conduct;
- Internal Training Program on policies and procedures for the prevention of corruption and related offenses implemented;
- Reporting Channel;
- Designation of the Regulatory Compliance Officer

2. Objectives

With the implementation of this Plan, ICT Strypes intends to continue its commitment to the prevention and mitigation of corruption risks and related infractions, establishing the following objectives:

1. Identify, analyze and classify the risks of acts of corruption and related infractions to which the organization is exposed, ensuring firm and rigorous action on any suspicions of this type of crime;

2. Develop control and mitigation activities of the identified risks, namely to identify and implement preventive and corrective measures that reduce the probability of

occurrence and the degree of impact of the risks;

3. Increase awareness and training of management positions and other employees;
4. Monitor the implementation of the PPR, periodically, or whenever there are changes that justify the review.

II. Characterization of ICT Strypes

ICT Strypes is part of a solid business group, with a consolidated presence both in Portugal and in the international market. The company operates directly in Lisbon and Porto.

ICT Strypes, which has a team of 115 employees, asserts itself in the national and international market, always guided by the values of credibility and professional responsibility, and promoting the realization of innovative and challenging projects, which strengthen the solid relationships of trust it establishes with its customers.

In turn, the company's organization is based on small teams spread across several solution areas, ensuring a strong and mutual development through knowledge sharing.

1. Mission | Vision | Values

Mission

It’s our mission to develop complex embedded software enabling our customers to deliver innovative products, and to build a sustainable future that supports the growth of our employees and their families. Another equally important aspect of our mission is to be an innovative employer by creating a workplace that encourages and supports our employees in expressing their full potential.

Vision

At ICT Strypes, we always seek for the most complex projects, ensuring ground-breaking solutions that challenge our employees and provide our customers with a competitive advantage.

Values

Our company's core values are courage, ownership, authenticity, willingness to learn and fun.

2. Services provided by ICT Strypes

ICT Strypes specializes in the development of complex software solutions, with a focus on embedded and backend software engineering, particularly for the semiconductor and agricultural sectors.

3. Organic structure of ICT Strypes

The company's organizational structure is directed by the *CEO*, who ensures the coordination of three fundamental areas: *Project Delivery, Operations & HR* and *Finance*.

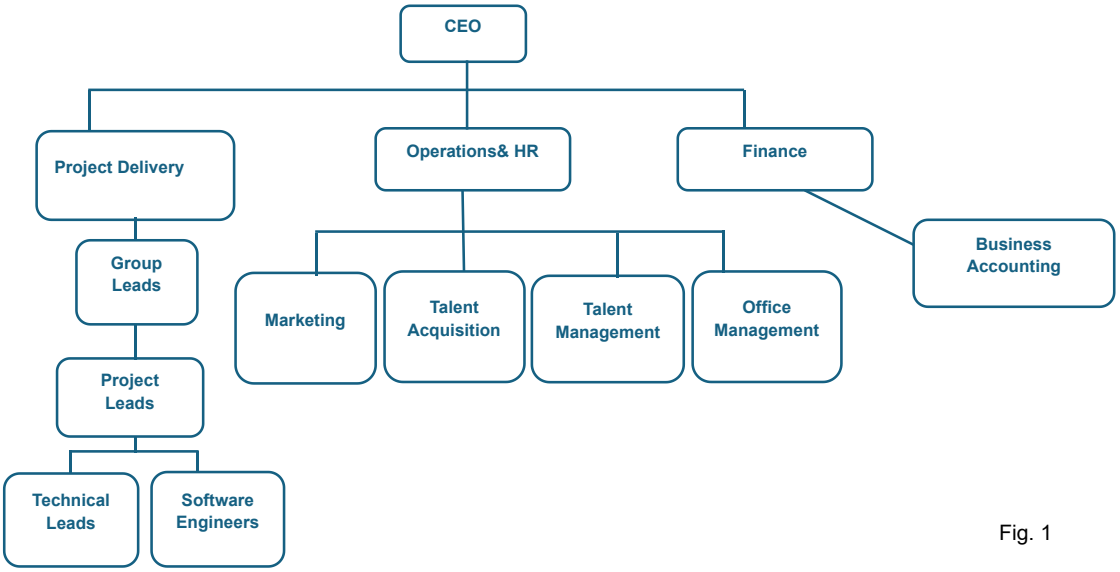


Fig. 1

The CEO is the entity responsible for the overall management of the company, ensuring the profit and loss account (*P&L*), defining and executing the business plan, and conducting Stakeholder Management.

Within the Project Delivery area, we have a Project Director who is responsible for developing internal expertise, allocating resources to projects, and overseeing their full life cycle. The role also includes managing strategic accounts, ensuring certifications and quality standards, defining processes and guidelines, supervising the IT function, and coordinating the management of commercial proposals (including their preparation, updating, and reporting to the finance department).

The Operations & HR area is led by a Director who manages and administers events, marketing, and communication. This role also covers office management, the definition

of benefits and initiatives aimed at employee satisfaction and personal development, ensuring compliance with ARBO standards, and overseeing legal matters.

The Finance area is likewise coordinated by a Director. The Finance Director is responsible for budgeting and forecasting, payroll management, liquidity control, fleet leasing administration, and facility management.

The information provided is summarised schematically in the schedule below:

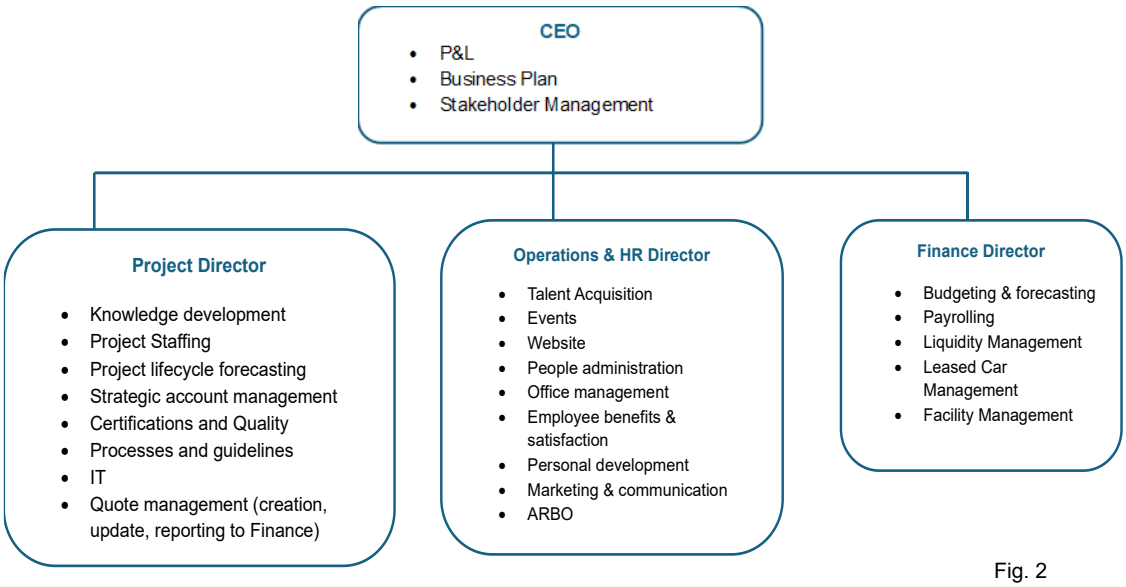


Fig. 2

3.1. Project Delivery

Continuing the hierarchical structure established in Project Delivery, Group Leads assume responsibility for all projects within their group, from initiating new engagements to allocating teams. They are also accountable for developing expertise within their domain, conducting performance and appraisal meetings, making hiring and dismissal decisions, and managing client relationships, including preparing business proposals and project budgets.

Below the Group Leads, we have Project Leads, who manage individual projects from both an operational and financial perspective. They report progress to the Group Lead and maintain direct communication with the client. Their responsibilities also include acting as the internal Product Owner and applying the ‘Right Person, Right Seat’ principle to ensure that each function is performed by the most suitable individual.

The information provided is summarised schematically in the schedule below:

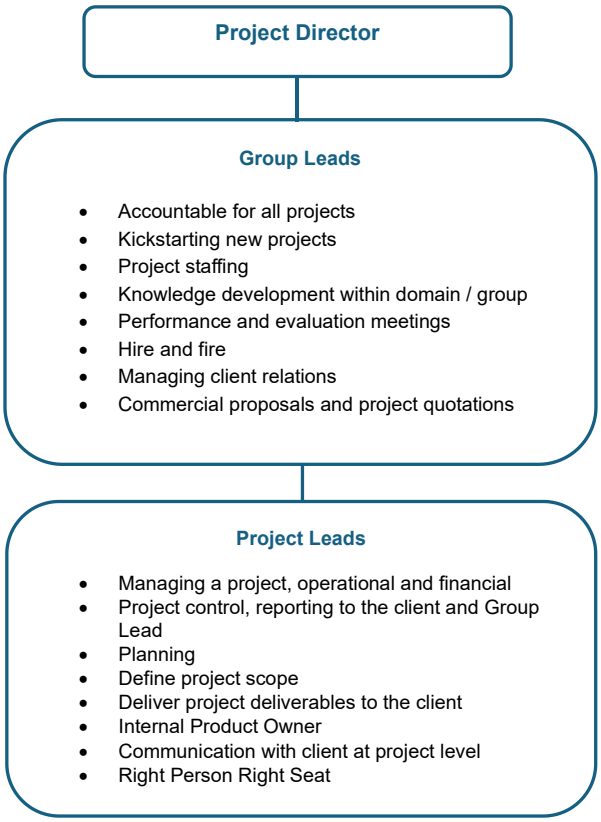


Fig. 3

In turn, the Project Leads area is divided into two roles: the Technical Lead and the Software Engineers.

The Technical Lead is responsible for producing designs, breaking down work packages, and providing technical guidance to project members. The role ensures technical alignment with the client, proposes technical improvements, guarantees the technical quality of deliverables, and resolves any technical issues that may arise throughout the project.

The Software Engineers are responsible for documenting, developing, testing, reviewing, and delivering their assigned tasks, ensuring the quality of the work performed. They identify risks and gaps in specifications, promote cooperation and knowledge sharing within the team, and identify opportunities to optimise process efficiency.

The information provided is summarised schematically in the schedule below:

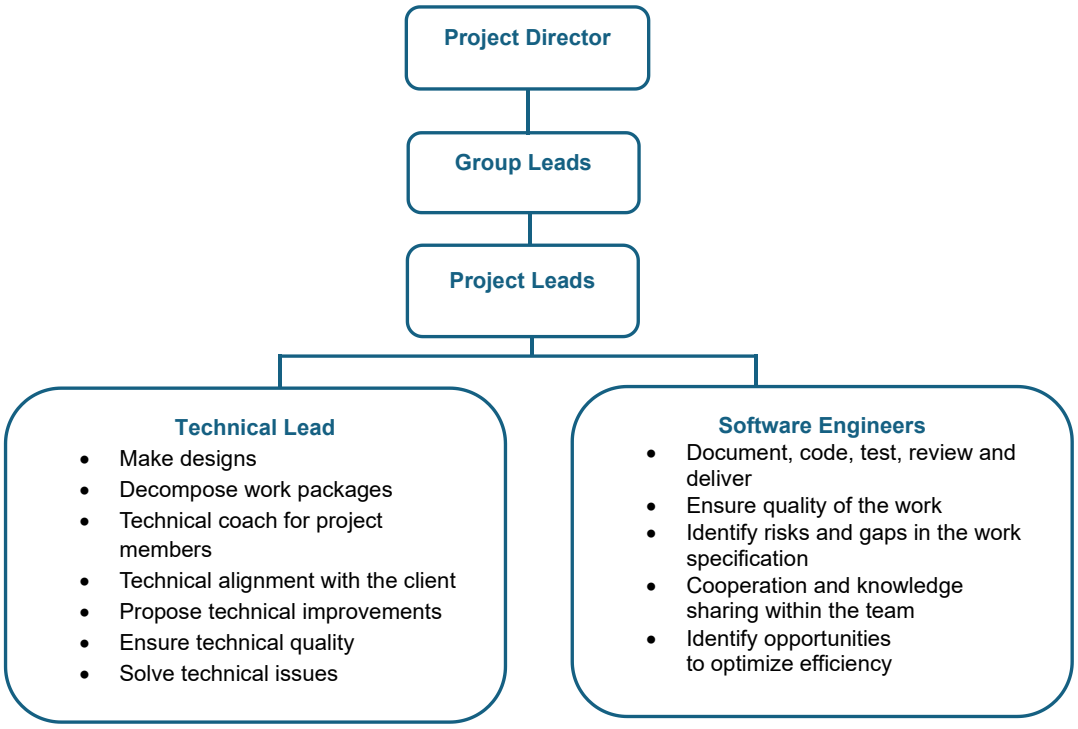


Fig. 4

3.2. Operations & HR

On the second hierarchical level, reporting to the CEO – who is responsible for the overall management of the company – we find Operations & HR, which is composed of several clearly defined functions and hierarchical roles. As mentioned above, the area is led by the Director of Operations and Human Resources, who provides overarching supervision and coordination of all subordinate functions.

Within Communication and Marketing, responsibilities include managing internal and external communications, maintaining and updating the corporate website, and participating in and organising labour-market and business fairs, thereby ensuring the company's visibility and public presence.

Next, the Talent Acquisition Lead is responsible for talent acquisition and labour-market communications. This area includes Recruiters, who implement strategies for attracting new talent and manage communications across social media platforms to ensure a consistent inflow of qualified candidates.

The Talent Manager is responsible for promoting employee well-being, coordinating the integration and onboarding of new employees, supporting professional development programmes, and implementing initiatives to enhance employee motivation and engagement.

Finally, the Personal Assistant is responsible for the administrative management of the office, HR administration related to personnel matters, the organisation of events and travel, and ensuring compliance with occupational health and safety standards (ARBO). Reporting to this role are the Office Managers, who oversee the administration and operational management of the company's workspaces.

The information presented is summarised schematically in the schedule below:

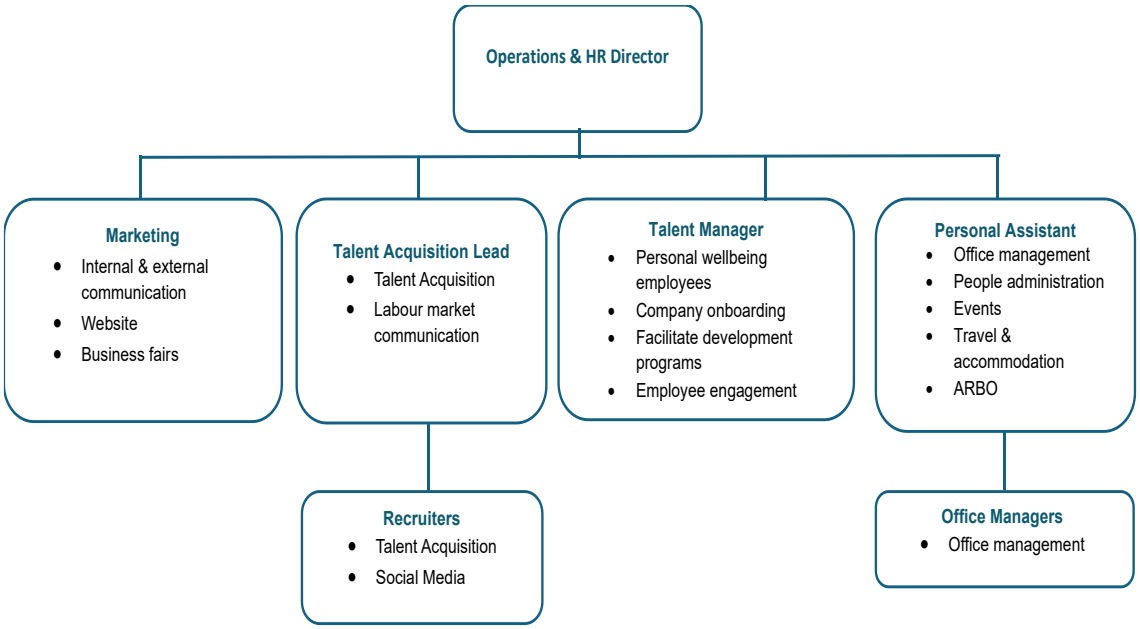


Fig. 5

3.3. Finance

Finally, at the third hierarchical level, reporting to the CEO, is the Finance area, led by the Finance Director, who holds ultimate responsibility for all financial and administrative functions of the organisation.

Reporting to the Finance Director is the Business Accounting department, which is responsible for a range of specific functions, including financial administration, the execution of key financial processes, the control and recording of working hours, project invoicing, and the verification and maintenance of the status of purchase orders (POs).

The department is also responsible for payroll management and the administration of employee benefits.

The information presented is summarised schematically in the schedule below.

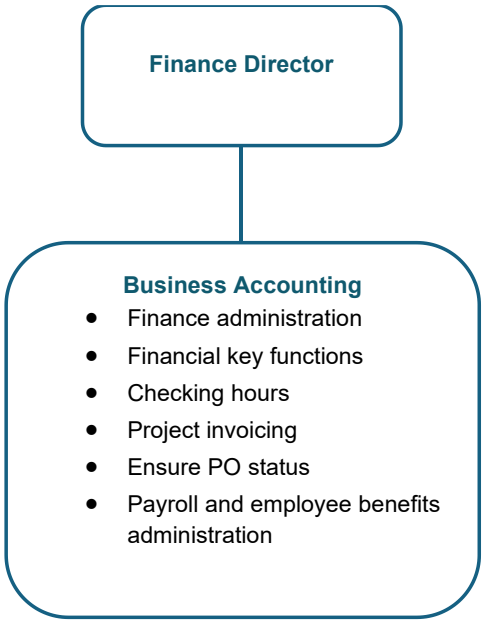


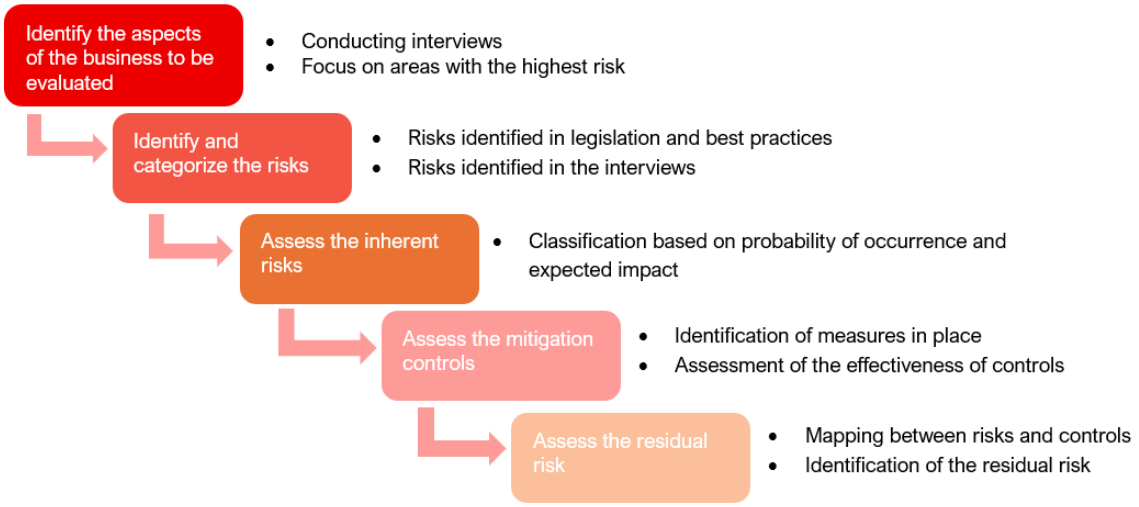
Fig. 6

III. Risk Analysis Methodology

According to NP EN ISO 9001:2015, risk is understood as the effect of uncertainty, which is often characterized as the combination of the probability of occurrence of an event — of a positive or negative nature — and its consequences.

The methodology for identifying, analysing and classifying the risks and situations that may expose ICT Strypes to acts of corruption and related infractions, in line with the requirements listed in Decree-Law No. 109-E/2021, of 9 December, considered:

- Identification of risks associated with acts of corruption;
- Quantification of inherent risk and grading of associated risk levels;
- Assessment of the risk control environment:
- Identification of aspects for improvement in the risk control environment;
- Quantification of residual risk and grading of risks.



To carry out the current assessment, the following process of identifying and classifying risks and controls has been carried out:

1. Collection of data from the Regulatory Compliance Officer.
2. Implementation of structured questionnaires to identify potential risks and assess the effectiveness of existing controls.

3. Request and analysis of internal documents, including policies, procedures and operational reports.

4. Under the terms of the matter under analysis, information was collected and an interview was conducted with the Financial Director.

5. After excluding the risks associated with impossible compliance, the inherent risks of corruption and other related infractions were identified, in accordance with the applicable legal regime and with the good practices recognized in the sector.

6. Classification and evaluation of inherent risks according to their degree of probability of occurrence and the foreseeable impact they may cause

7. Identification and evaluation of the controls implemented by ICT Strypes, based on the survey of processes mentioned in the previous points.

8. Mapping of the risks inherent to the controls, identifying those that are implemented, implemented with exceptions or to be implemented, with their respective strength in view of the impact and probability – subsequently assessing the residual risk.

In order to classify the risk events, the following scale was considered for probability, impact and inherent risk, respectively:

A. Probability

Probability is the possibility of an adverse event happening. In this financial year, it is the event related to risks of corruption and related infractions or other operational management issues.

The Probability assessment shall be based on the occurrence probability scale represented below:

1. Remote: event expected to occur in exceptional circumstances (qualitative assessment);

2. Possible: event expected to occur occasionally (qualitative);

3. Probable: event expected to occur in almost half of the circumstances (qualitative);

4. Very Likely: event expected to occur in most circumstances (qualitative).

B. Impact

The Impact of a risk represents the severity of the consequences for the Organization, if the event materializes.

The impact magnitude assessment takes into account the following five dimensions:

a) Financial Impact;

b) Strategic Impact;

c) Regulatory Impact and Regulatory Compliance;

d) Operational and Technological Impact;

e) Reputational Impact.

Impact is categorized into the following levels:

1. Low;

2. Medium;

3. Elevated;

4. Strong.

C. Inherent Risk

Inherent risk is the likelihood of an adverse event occurring before any risk mitigation measures are implemented, i.e., the pure and natural risk associated with an activity or process, without regard to any action taken to mitigate it.

Thus, the Inherent Risk results from the multiplication operation between probability and impact, on its scales from 1 to 4 identified above, being quantified through the following scale:

Risk Level	
Low	Between 1 and 3
Medium	Between 4 and 6
High	Between 8 and 12
Critical	16

Graphically, the grading of the risk is represented as follows:

Probability	**4**	**8**	**12**	**16**
	3	**6**	**9**	**12**
	2	**4**	**6**	**8**
	1	**2**	**3**	**4**
	Impact			

D. Controls and Residual Risk

To determine the residual risk, the effectiveness and strength of the controls were considered, that is, the relevance of the control for mitigating the impact and reducing the probability of the risk event being assessed.

Based on the strength of the control, the evaluation of the Impact and Residual Probability is obtained. By multiplying the probability of the residual impact, the residual risk is obtained.

Residual Risk corresponds to the part of the inherent risk not mitigated by the associated controls, that is, the risk remaining after considering how the internal control system manages to mitigate the inherent risk.

IV. Identification of corruption risks and related offences

In accordance with the foregoing, Decree-Law No. 109-E/2021, of 9 December, in its article 1, approves the General Regime for the Prevention of Corruption. This regime, annexed to the aforementioned legal diploma, provides in article 5 that the subject entities, including ICT Strypes, must adopt and implement a regulatory compliance program that includes, among other elements, a plan for the prevention of the risks of corruption and related infractions (PPR).

In this sense, Article 3 of the General Regime for the Prevention of Corruption (RGPC) defines the concept of corruption and related offences for the purposes of its application: "*corruption and related offences are understood to be the crimes of corruption, undue receipt and offer of advantage, embezzlement, economic participation in business, concussion, abuse of power, malfeasance, influence peddling, laundering or fraud in obtaining or embezzling a subsidy, subsidy or credit, provided for in the Criminal Code, approved in annex to Decree-Law No. 48/95, of 15 March, as amended, in Law No. 34/87, of 16 July, as amended, in the Code of Military Justice, approved in annex to Law No. 100/2003, of 15 November, in Law No. 50/2007, of 31 August, in its current wording, in Law No. 20/2008, of 21 April, in its current wording, and in Decree-Law No. 28/84, of 20 January, in its current* wording".

For the purposes of identification and in compliance with its functions of supporting obliged entities in their implementation (Article 2(3)(b) and (d) of Decree-Law No. 109-E/2021), MENAC issued Guide No. 1/2023, entitled *"The Instruments of the General Regime for the Prevention of Corruption".* This document includes an annex, identified with no. 3, in which MENAC has structured tables relating to the crimes covered by the RGPC. This annex is subdivided into six sub-annexes, in which each of the offences is analysed individually

Annex 3.1 covers the crimes provided for in the Penal Code, approved by Decree-Law No. 48/95, of 15 March, in its current wording, applicable to employees and workers of public sector entities and organisations, of a public nature or who, in any way, carry out activities that serve the public interest or benefit from public support.

Annex 3.2 refers to the crimes of responsibility of political office holders, provided for in Law No. 34/87, of 16 July, as subsequently amended.

Annex 3.3 covers the crimes contained in the Code of Military Justice, approved by Law No. 100/2003, of 15 November.

Annex 3.4 deals with the crimes provided for in Decree-Law No. 50/2007, of 31 August, relating to the regime of criminal liability for behaviours likely to affect the truth, fairness and correctness of the sporting competition.

Annex 3.5 focuses on the crimes provided for in Law No. 20/2008, of 21 April, which establishes the criminal regime for corruption in international trade and in the private sector.

Finally, Annex 3.6 covers the crimes provided for in Decree-Law No. 28/84, of 20 January, relating to anti-economic offences and offences against public health.

1. Framework of Applicable Risks under the RGPC

Using this support tool, it is possible to draw preliminary conclusions in the process of identifying the risks to which ICT Strypes is exposed. At first glance, it is clear that, given the nature of the organisation's activities and structure, most of the risks are not applicable. This results from the fact that ICT Strypes is a private entity, is not composed of civil servants, does not perform public functions, does not hold political office, and does not carry out sporting activities.

Thus, all types of offences that presuppose the quality of public official, the exercise of public functions, the holding of political or military offices, or the connection to sporting activities are excluded, as they are incompatible with the organisational reality of the company, and are therefore not subject to analysis.

On the other hand, the unlawful acts effectively applicable to ICT Strypes are identified, which will constitute the basis for the preparation of this Plan for the Prevention of Risks of Corruption and Related Infractions (PPR).

Thus, the following criminal offenses were identified as possible within the scope of the General Regime for the Prevention of Corruption (RGPC):

A) Active corruption (art. 374 of the Penal Code): Anyone who, by himself or through a third party, with his consent or ratification, gives or promises to an official, or to a third party by indication or with the knowledge of the latter, a patrimonial or non-patrimonial advantage, for the purpose provided for in paragraph 1 of article 373, namely for the practice of an act or omission contrary to the duties of the position

B) Undue receipt and offer of advantage (art. 372.2 of the Penal Code): Anyone who, by himself or through another person, with his consent or ratification, gives or promises to an official, or to a third party by indication or with the knowledge of the latter, a patrimonial or non-patrimonial advantage that is not due to him, in the exercise of his functions or because of them.

C) Influence peddling (art. 335 of the Penal Code): Whoever, by himself or through another person, with his consent or ratification, solicits or accepts, for himself or for a third party, patrimonial or non-patrimonial advantage, or the respective promise, with the intention of abusing his influence, real or supposed, with any public entity, national or foreign.

D) Money Laundering (art. 368-A of the Criminal Code): Anyone who converts, transfers, assists or facilitates any conversion or transfer operation of advantages obtained by himself or by a third party, directly or indirectly, with the purpose of concealing its illicit origin or preventing the respective author or participant from being criminally prosecuted or subject to criminal reaction. Likewise, anyone who conceals or conceals the true nature, origin, location, disposition, movement or ownership of these advantages, or the rights related to them, is liable. Finally, anyone who, not being the author of the unlawful act from which the advantages originate, acquires, holds or uses them, knowing, at the time of acquisition, possession or initial use, their illicit origin, also incurs liability.

E) Corruption to the detriment of international trade (Article 7 of Law No. 20/2008 of 21 April): Whoever, by himself or through another person, with his consent or ratification, gives or promises to an official — national, foreign or of an international organisation —, to a holder of a political office, national or foreign, or to a third party with knowledge thereof, a patrimonial or non-patrimonial advantage that is not due to him, for the purpose of obtaining or retaining a business, contract or other undue advantage in international trade

F) Passive corruption in the private sector (Article 8 of Law No. 20/2008 of 21 April): A private sector employee who, by himself or through a third party, with his consent or ratification, requests or accepts, for himself or for a third party, a patrimonial or non-patrimonial advantage, or the respective promise, which is not due to him, in return for the practice or omission of an act that constitutes a breach of its functional duties

G) Active corruption in the private sector (Article 9 of Law No. 20/2008, of 21 April): Whoever, by himself or through another person, with his consent or ratification, gives or promises to a private sector employee, or to a third party with his knowledge, a patrimonial or non-patrimonial advantage that is not due to him, with the aim of obtaining the practice or omission of an act that constitutes a violation of the functional duties provided for in the previous article.

H) Fraud in obtaining a subsidy or grant (Article 36 of Decree-Law No. 28/84 of 20 January):

a. Who obtains a subsidy or grant:

i. Providing the competent authorities or entities with inaccurate or incomplete information about themselves or third parties and regarding facts important for the award of the grant or subsidy;

ii. Omitting, contrary to the provisions of the legal regime of the subsidy or subsidy, information on facts important for its award;

iii. Using a document justifying the right to the subsidy or subsidy or facts important for its award, obtained through inaccurate or incomplete information;

b. Particularly serious are cases in which the agent:

i. obtains a subsidy or subsidy of a considerable amount for yourself or a third party or uses false documents;

ii. Commits the act with abuse of his functions or powers;

iii. He obtains assistance from the holder of a public office or job who abuses his functions or powers.

I) Fraud in obtaining credit (art. 38 and 36 of Decree-Law No. 28/84, of 20 January): Who, when submitting a proposal for granting, maintaining or modifying the conditions of a credit intended for an establishment or company:

a. Provide inaccurate or incomplete written information intended to support you or that is relevant to the decision on the application;

b. Using inaccurate or incomplete documents relating to the economic situation, such as balance sheets, profit and loss accounts; general descriptions of the assets or expert opinions;

c. Conceal any deterioration in the economic situation which has occurred in the meantime in relation to the situation described at the time of the application and which is important for the decision on the application.

J) Deviation of subsidy, grant or subsidized credit (Article 37 of Decree-Law No. 28/84, of 20 January): Anyone who uses benefits obtained as a subsidy or subsidy for purposes other than those legally established, as well as those who apply benefits obtained as subsidized credit for a purpose other than that provided for in the respective credit line set by the legally competent entity.

V. Inherent risks

In this section, the risks of corruption and related infractions to which ICT Strypes is exposed are analysed, taking into account the object of this Prevention Plan, as well as the structure and activities developed by the organization.

Based on these elements, it was possible to determine a first level of risk of materialization of such offences, applying the methodology described in Section III. The assessment of probability and impact, without considering the control measures already in place at ICT Strypes, made it possible to identify the level of inherent risk, reflected in the respective risk matrix.

It is important to note that the assessment of probability and impact is directly related to the sector of activity and the structure of the organization. For this reason, some of the risks identified are of a low level at this stage of the analysis, although they cannot be considered impossible to materialise.

VI. Control Measures

To prevent and manage the risks of corruption and related offences, ICT Strypes has adopted a structured set of control measures within its organisational model. Some of these measures are targeted at specific areas or processes, while others operate across the board, ensuring a uniform level of integrity and compliance across the organization.

1. Prevention and control model adopted by the organization

Specifically, the entity has the following control mechanisms, duly appropriate to mitigate the identified risks:

a) **Designation of a Regulatory Compliance Officer**: responsible for supervising the implementation of integrity policies, monitoring compliance with legal and internal obligations, ensuring the effectiveness of prevention mechanisms and detecting any irregularities, promoting the continuous improvement of the internal control system.

b) **Designation of a PRP Implementation Officer**: responsible for ensuring the implementation, monitoring and continuous updating of the Risk Prevention Plan, ensuring that the measures provided for are effectively applied, evaluated and adjusted in accordance with the evolution of the organization's activity and risks.

c) **Compliance Officer**: responsible for ensuring the organization's compliance with the applicable legal and regulatory framework, monitoring the execution of internal policies, evaluating the effectiveness of control mechanisms and promoting a culture of integrity and business ethics in all areas of ICT Strypes.

d) **Quality Officer**: responsible for ensuring the compliance of internal processes with the defined quality standards, supervising the implementation of procedures and good practices, monitoring performance indicators, identifying deviations or non-conformities and proposing corrective measures that ensure the continuous improvement of the services provided by ICT Strypes.

e) **CISO (Chief Information Security Officer):** responsible for defining, implementing, and overseeing the organization's information security strategy, ensuring the protection of systems, data, and digital infrastructures. It is also responsible for assessing technological risks, ensuring compliance with security standards and

policies, coordinating incident responses and promoting a cybersecurity culture across ICT Strypes.

a. The CISO and his ICT Group department conduct **annual audits on data security and privacy**, using interviews and sampling as evaluation methods.

f) **Code of Conduct**: which establishes the principles, norms and standards of behavior expected of all employees, service providers, business partners and suppliers of ICT Group, promoting integrity, ethics and legal compliance in all activities of the organization.

g) **Anti-Bribery and Corruption Rules (ABC-Rules):** which define the specific guidelines and procedures to prevent, detect and respond to acts of bribery and corruption, ensuring that all interactions, transactions and business relationships of ICT Group are conducted in compliance with the highest standards of integrity and applicable legislation.

h) **Whistleblowing Channel:** secure and confidential mechanism through which employees, service providers, partners and third parties can report suspected irregularities, legal or ethical violations, ensuring the proper investigation of occurrences and the protection of the whistleblower against any retaliation. The channel can be accessed through the following address: Policy-Whistleblower-ICT-2025

i) **Annual financial audit**: carried out by an external agent (PricewaterhouseCoopers), aimed at verifying the compliance of accounting records, the reliability of financial statements and the effectiveness of internal controls, ensuring transparency and accuracy in ICT Strypes' financial information.

j) **Four-Eyes Principle:** Invoice and banking transaction processes require the intervention of two people to carry them out, ensuring the segregation of duties, mutual supervision and the reduction of risks of error or fraud in ICT Strypes' financial management.

k) **Internal audits:** the ICT Group, to which ICT Strypes belongs, has the Finance & Control Department, responsible for auditing ICT Strypes' financial report on a

monthly basis. In addition, it conducts random sampling, although there is no formal procedure regulating the frequency or methodology of these reviews.

l) **Rules on Conflicts of Interest:** in its employment contracts, ICT Strypes defines the obligation to inform and obtain approval from the hierarchical superior, in order to prevent situations that may compromise professional judgment and ensure integrity in internal and external relations.

m) **ISO 27001:** certification that establishes the requirements for an Information Security Management System (ISMS), ensuring the protection of ICT Strypes' information assets, the management of security risks, the confidentiality, integrity and availability of data, as well as compliance with recognized international standards.

n) **AllSolutions ERP Program:** accessible only to the Management and the Finance department, through credentials and authorization levels, with access continuously supervised by the Group's Finance Department and audited by the external auditor.

o) **Annual internal audit:** carried out by the ICT Group Department, which includes level 2 controls and issues reports on the following aspects: fraud risks, compliance and anti-money laundering (AML) prevention.

p) **Legal, financial and payroll management advice, provided externally**: by specialized entities, ensuring technical support, legal compliance and operational efficiency. Taking into account the identified risks and their assessment (see risk matrix in the annex)., ICT Strypes has planned the introduction of new control mechanisms, designed to strengthen the mitigation and effective management of this risk.

2. Measures proposed under the Risk Prevention Plan

As part of the plan, these measures will be effectively applied in the company, ensuring their practical implementation and the reinforcement of the mitigation of the identified risks.

a) **Internal training program**. Within the scope of this Plan for the Prevention of Risks of Corruption and Related Infractions, the organization promotes training actions aimed at strengthening the culture of ethics, integrity, transparency and regulatory

compliance, in accordance with the National Anti-Corruption Strategy (ENAC) and the guidelines of the National Anti-Corruption Mechanism (MENAC). The training will be given in e-learning format, with a total duration of 2 hours per session, and is divided into two complementary strands:

a. Training for decision-making staff, focused on management responsibilities, decision-making, risk prevention and implementation of internal control mechanisms, as well as the strategic role of regulatory compliance and ethical leadership;
b. Training for other employees, focused on raising awareness of the phenomenon of corruption, knowledge of the applicable internal and legal rules, and the correct use of prevention tools, namely the whistleblowing channel.

The syllabus addresses, in a synthetic and practical way, the following topics: definition and types of corruption; main axes of the National Anti-Corruption Strategy; the role and competencies of MENAC; regulatory compliance program and respective responsible; promotion of a culture of ethics and business integrity; the organization's anti-corruption policy; and operation of the whistleblowing channel, including the protection of whistleblowers and the handling of reports received.

At the end of each action, participants take a knowledge assessment test consisting of multiple-choice questions, aimed at assessing their understanding of the content. Approval requires a minimum of 70%, and a digital certificate of completion is issued through the e-learning platform.

The training actions are mandatory and are conducted during the integration phase for new employees, as well as under a biennial recycling regime, ensuring the continuous updating of knowledge and the strengthening of good integrity practices. The implementation of this training plan contributes to fulfilling legal obligations related to corruption prevention and consolidates the institutional commitment to ethics, responsibility and transparency.

b) Fund Management Policy: defines how financial resources are managed, including payment or transfer authorization procedures, spending limits and transaction approval, as well as the necessary controls to prevent misappropriation, fraud or errors.

c) **Supplier Assessment**: which establishes criteria and procedures for selecting, monitoring and re-evaluating ICT Strypes suppliers, ensuring that they meet standards of quality, integrity, legal compliance and contractual requirements, contributing to the mitigation of operational and reputational risks.

d) **Control of conflicts of interest**: which defines procedures to identify, declare and manage situations in which personal interests may conflict with the interests of ICT Strypes, ensuring that all decisions are made impartially, transparently and in accordance with applicable internal and legal standards.

e) **Due diligence procedures**: which establish systematic methods for evaluating partners, suppliers and third parties, including background checks, legal, financial and compliance risk analysis, in order to ensure that all ICT Strypes business relationships are conducted safely, ethically and in compliance with applicable law.

f) **Anti-Money Laundering (AML) Policies:** which define standards and procedures for identifying, monitoring and reporting suspicious transactions, ensuring that ICT Strypes complies with legal and regulatory obligations regarding the prevention of money laundering and terrorist financing.

VII. Residual risk

Taking into account the identified risks, the control measures already in place and those foreseen, and in accordance with the methodology described in Section III, the effectiveness of the mitigation mechanisms was assessed.

The analysis resulted in a reduction in risk levels, which, even in the initially highest cases, do not exceed the average level. The measures currently implemented, together with those that are in the planning phase, thus ensure a level of risk considered to be assumable by the organization.

ICT Strypes will focus its efforts, on the one hand, on the continuous monitoring of the areas of greatest exposure, ensuring the execution and effectiveness of existing controls,

and, on the other hand, on the implementation and verification of the new measures outlined.

VIII. Action plan

The control of the implementation and effectiveness of the existing control measures, as well as the implementation and monitoring of the new mechanisms, will be the responsibility of the General Responsible for the implementation, control and review of the PPR .

The General Responsible will act in conjunction with the Compliance Officer, who will provide monitoring and support for the execution of the plan.

The heads of each department assume the role of primary executors in implementing the new control measures and must follow the guidelines and the schedule defined together with the General Manager. They are also responsible for reporting on the status of implementation upon request, as well as providing the necessary documentation and evidence. In addition, they must report any irregularity detected in the execution or in the activities classified as higher risk in the matrix.

It is the responsibility of all ICT Strypes employees, in line with corporate values, to ensure that their actions are guided by ethical principles and meet the required standards. Irregular conduct will not be allowed, under any circumstances, and it is everyone's duty to report any infraction of which they are aware, through the reporting mechanisms established by the organization.

IX. Attachment.

As an annex to this PRP, ICT Strypes has prepared a risk matrix, in which the departments of the organization that, due to their activity, are most exposed to the identified risks were selected.

The risk events faced by these departments were also identified, accompanied by the corresponding assessment of the inherent risks, the control measures, the assessment of their effectiveness and the level of residual risk.

In such a structure, the control measures to be supervised by the General Manager, both for monitoring and for the implementation of the new mechanisms, are easily identified, in accordance with the guidelines set out in the previous section, "Action Plan".

ANNEX I – Risk Matrix

a) CEO

Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
Active corruption (Article 374 of the Criminal Code) Undue receipt and offer of advantage (Article 372, paragraph 2 of the Criminal Code)	1. Offer advantage to public officials to expedite licenses or permits 2. Favoring public officials in administrative decisions that benefit the branch 3. Accepting favors or payments from public officials in exchange for decisions	POSSIBLE	ELEVATED	MEDIUM	1. Designation of key people who ensure regulatory compliance: Responsible for regulatory compliance; Responsible for the implementation of the plan for the prevention of corruption and related infractions; *Compliance officer and Quality Officer.* 2. Code of Conduct and Anti-Bribery and Corruption Rules (ABC Rules) 3. Annual financial audit by external agent. 4. Monthly internal audits. 5. Rules of Conflicts of Interest and Acceptance of Offers: in its employment contracts. 6. ISO 270001 7. AllSolutions ERP Program 8. Annual internal audit	REMOTE	MODERATE	LOW
Influence peddling (Article 335 of the Penal Code)	1. Invoking personal relationships with authorities to obtain favorable decisions 2. Payment to intermediaries for the purpose of influencing authorities responsible for technology contracts or digital transformation projects.	POSSIBLE	ELEVATED	MEDIUM		REMOTE	MODERATE	LOW

Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
	3. Invocation of privileged relationships to change decisions in technical evaluations of proposals.				9. Legal, financial and payroll management advice, provided in an outsourced manner Possible measures: 10. Fund Management Policy 11. Supplier Evaluation 12. Control of conflicts of interest 13. Due diligence procedures 14. Money Laundering (AML) Prevention Policies			
Money Laundering (Article 368-A of the Criminal Code)	1. False billing for system maintenance, cybersecurity services, or non-existent software development. 2. Approval of financial *reporting* changes without evidence justifying the modification. 3. Internal or external movement of capital through related technological entities, without real economic basis.	REMOTE	STRONG	MEDIUM		REMOTE	ELEVATED	LOW

Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
Corruption to the detriment of international trade (Law 20/2008, art. 7)	1. Offer of undue advantages to commercial representatives outside Portugal 2. Undue influence on certification or technical approval processes required by international customers.	REMOTE	STRONG	MEDIUM		REMOTE	ELEVATED	LOW
Passive corruption in the private sector (Article 8 of Law No. 20/2008 of 21 April)	1. Receiving advantages from technology providers, *cloud* platforms, specialized hardware, development tools or cybersecurity services to favour their hiring. 2. Acceptance of benefits from private customers to influence prices, delivery priorities or contractual conditions. 3. Receipt of undue commissions associated with the selection of technology partners.	LIKELY	STRONG	HIGH		POSSIBLE	ELEVATED	MEDIUM

Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
Active corruption in the private sector (Article 9 of Law No. 20/2008 of 21 April)	1. Granting of illicit benefits to obtain exclusivity in the supply of technological solutions. 2. Payment of undeclared incentives to influence technological *procurement* processes.	LIKELY	STRONG	HIGH		POSSIBLE	ELEVATED	MEDIUM
Fraud in obtaining a subsidy or subsidy (Article 36 of Decree-Law No. 28/84 of 20 January)	1. Overestimation of research costs, engineering hours or acquisition of computer equipment to increase the value of funding. 2. Concealment of relevant revenues or liabilities in incentive programs for technological modernization.	LIKELY	STRONG	HIGH		REMOTE	MODERATE	LOW
Fraud in obtaining credit (art. 38º 36º del Decreto-Lei nº 28/84, of 20 January)	1. Approval of manipulated financial information to obtain internal or external credit lines associated with development, cybersecurity or technological dependencies projects. 2. Concealment of real risks of the company to approve credit	LIKELY	STRONG	HIGH		REMOTE	MODERATE	LOW

Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
	3. Overvaluation of technological assets, equipment or intellectual property to serve as collateral.							
Deviation of subsidy, subsidy or subsidized credit (Article 37 of Decree-Law No. 28/84, of 20 January)	1. Redirecting funds intended for training, wellness or benefits to unauthorized purposes. 2. Transfer of support to related entities without justification 3. Application of subsidies to personal or non-classified expenses	LIKELY	STRONG	HIGH		REMOTE	MODERATE	LOW

b) Project Delivery

Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
Active corruption (Article 374 of the Criminal Code) Undue receipt and offer of advantage (Article 372, paragraph 2 of the Criminal Code)	1. Offering advantages to public entities in certifications, audits or technical inspections. 2. Granting undue benefits to speed up the approval of digital solutions, embedded systems or cybersecurity services.	POSSIBLE	ELEVATED	MEDIUM	1. Designation of key people who ensure regulatory compliance: Responsible for regulatory compliance; Responsible for the implementation of the plan for the prevention of corruption and related infractions; *Compliance officer and Quality Officer.* 2. Code of Conduct and Anti-Bribery and Corruption Rules (ABC Rules) 3. Annual financial audit by external agent. 4. Monthly internal audits. 5. Rules of Conflicts of Interest and Acceptance of Offers: in its employment contracts.	REMOTE	MODERATE	LOW
Influence peddling (Article 335 of the Penal Code)	1. Payment to intermediaries to change evaluation criteria or approve technological deliveries. 2. Invocation of privileged relationships to obtain favorable decisions in audits or project checkpoints.	POSSIBLE	ELEVATED	MEDIUM		REMOTE	MODERATE	LOW

Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
Money Laundering (Article 368-A of the Criminal Code)	1. Manipulating budgets or project financial reports to justify improper payments. 2. Recording fictitious hours or inflating supplier costs. 3. Concealment of internal financial transactions between projects.	REMOTE	STRONG	MEDIUM	6. ISO 270001 7. AllSolutions ERP Program 8. Annual internal audit 9. Legal, financial and payroll management advice, provided on an outsourced basis Possible measures: 10. Fund Management Policy 11. Supplier Evaluation 12. Control of conflicts of interest 13. Due diligence procedures 14. Money Laundering (AML) Prevention Policies	REMOTE	ELEVATED	LOW
Passive corruption in the private sector (Article 8 of Law No. 20/2008 of 21 April)	1. Receiving advantages from software providers, *cloud* platforms, development tools or subcontractors in exchange for awarding or prioritizing tasks 2. Acceptance of gifts or benefits that influence resource allocation or choice of partners.	LIKELY	STRONG	HIGH		POSSIBLE	ELEVATED	MEDIUM

Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
Active corruption in the private sector (Article 9 of Law No. 20/2008 of 21 April)	1. Favoring suppliers, consultants or freelancers through payment or advantage. 2. Approval of costs or changes in scope that unduly benefit third parties.	LIKELY	STRONG	HIGH		POSSIBLE	ELEVATED	MEDIUM
Fraud in obtaining a subsidy or subsidy (art. 36 of Decree-Law No. 28/84 of 20 January)	1. Inflating project reports or documentation to justify internal funds or support programs. 2. Declaration of non-existent hours or resources. 3. Falsification of documentation of certifications or technical training.	LIKELY	STRONG	HIGH		REMOTE	MODERATE	LOW
Fraud in obtaining credit (art. 38 of Decree-Law No. 28/84, of 20 January)	1. Alteration of budgets or financial forecasts to justify internal funds of the parent company.	LIKELY	STRONG	HIGH		REMOTE	MODERATE	LOW

Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
	2. Falsification of documents submitted to obtain internal financing approved by the group.							
Deviation of subsidy, subsidy or subsidized credit (Article 37 of Decree-Law No. 28/84, of 20 January)	1. Redirecting training, certification or quality funds to unauthorised expenditure. 2. Use of project resources for personal expenses or those of other departments. 3. Appropriation of funds intended for the technical improvement or know-how of the project.	LIKELY	STRONG	HIGH		REMOTE	MODERATE	LOW

c) Operations & HR

Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
Active corruption (Article 374 of the Criminal Code) Undue receipt and offer of advantage (Article 372, paragraph 2 of the Criminal Code)	1. Offering advantages to Social Security employees or other public entities to expedite employee discharges or discharges. 2. Offering gifts or perks to public officials linked to labor inspection to obtain favorable decisions. 3. Receiving gifts or benefits from public officials in exchange for favorable decisions in HR management or social charges.	POSSIBLE	ELEVATED	MEDIUM	1. Designation of key people who ensure regulatory compliance: Responsible for regulatory compliance; Responsible for the implementation of the plan for the prevention of corruption and related infractions; *Compliance officer and Quality Officer.* 2. Code of Conduct and Anti-Bribery and Corruption Rules (ABC Rules) 3. Annual financial audit by external agent. 4. Monthly internal audits. 5. Rules of Conflicts of Interest and Acceptance of Offers in its employment contracts. 6. ISO 270001 7. AllSolutions ERP Program 8. Annual internal audit	REMOTE	MODERATE	LOW
Influence peddling (Article 335 of the Penal Code)	1. Use of the director's contacts to influence decisions of public officials in Social Security or labor inspections. 2. Pressure on public authorities to speed up internal administrative processes.	POSSIBLE	ELEVATED	MEDIUM		REMOTE	MODERATE	LOW

Plan for the Prevention of Risks of Corruption and Related Infractions

Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
Money Laundering (Article 368-A of the Criminal Code)	1. Redirecting funds from operations, salaries or department budgets to conceal the illicit source of funds. 2. Using marketing, recruitment, or development program budgets to hide illicit funds.	REMOTE	STRONG	MEDIUM	9. Legal, financial and payroll management advice, provided in an outsourced manner Possible measures: 10. Fund Management Policy 11. Supplier Evaluation 12. Control of conflicts of interest 13. Due diligence procedures 14. Money Laundering (AML) Prevention Policies	REMOTE	ELEVATED	LOW
Passive corruption in the private sector (Article 8 of Law No. 20/2008 of 21 April)	1. Receiving advantages from suppliers or partners to influence decisions related to marketing, recruitment, training or administrative management. 2. Receiving incentives from private partners in exchange for favoring internal processes.	LIKELY	STRONG	HIGH		POSSIBLE	ELEVATED	MEDIUM
Active corruption in the private sector (Article 9 of Law No. 20/2008 of 21 April)	1. Offering advantages to suppliers or partners to obtain more favorable commercial or administrative conditions. 2. Illegitimate incentives to decision-makers of private companies to favor HR events or services.	LIKELY	STRONG	HIGH		POSSIBLE	ELEVATED	MEDIUM

Plan for the Prevention of Risks of Corruption and Related Infractions

Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
Fraud in obtaining a subsidy or subsidy (Article 36 of Decree-Law No. 28/84 of 20 January)	1. Falsifying proof of training or integration expenses for employees to divert funds.	LIKELY	STRONG	HIGH		REMOTE	MODERATE	LOW
Fraud in obtaining credit (art. 38 and 36 of Decree-Law No. 28/84, of 20 January)	1. Misrepresentation of marketing expenses, recruitment, development programs, or administrative events to obtain grants or support.	LIKELY	STRONG	HIGH		REMOTE	MODERATE	LOW
Deviation of subsidy, subsidy or subsidized credit (Article 37 of Decree-Law No. 28/84, of 20 January)	1. Handling reports or documentation of marketing expenses, recruitment, development programs, or administrative operations to justify payments or lines of credit. 2. Redirecting funds intended for operations, salaries, marketing, recruitment, development programs or administrative management for unauthorized purposes.	LIKELY	STRONG	HIGH		REMOTE	MODERATE	LOW

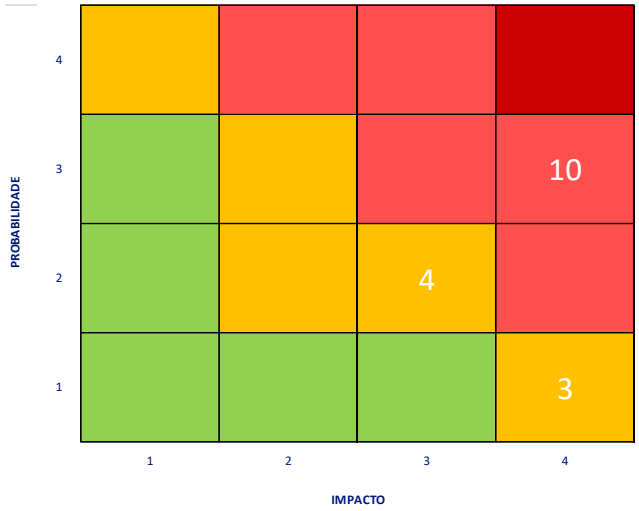
d) Finance

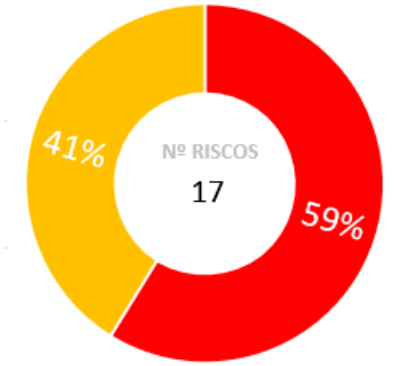
Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
Active corruption (Article 374 of the Criminal Code) Undue receipt and offer of advantage (Article 372, paragraph 2 of the Criminal Code)	1. Offering advantages to public officials for approval of tax credits, payments or deductions. 2. Payment to public agents to streamline payroll or liquidity inspection processes. 3. Acceptance of gifts or benefits from public officials in connection with tax or social security inspections.	POSSIBLE	STRONG	HIGH	1. Designation of key people who ensure regulatory compliance: Responsible for regulatory compliance; Responsible for the implementation of the plan for the prevention of corruption and related infractions; Compliance officer and Quality Officer. 2. Code of Conduct and Anti-Bribery and Corruption Rules (ABC Rules) 3. Annual financial audit by external agent. 4. Monthly internal audits. 5. Rules of Conflicts of Interest and Acceptance of Offers in its employment contracts. 6. ISO 270001 7. AllSolutions ERP Program	REMOTE	ELEVATED	LOW
Money Laundering (Article 368-A of the Criminal Code)	1. Illicit fund transfers disguised as payroll or vendor payments. 2. Use of accounts or third parties to mask the origin of misappropriated funds. 3. Manipulation of fleet payments or facility management to hide illegitimate financial flows.	REMOTE	STRONG	MEDIUM		REMOTE	ELEVATED	LOW

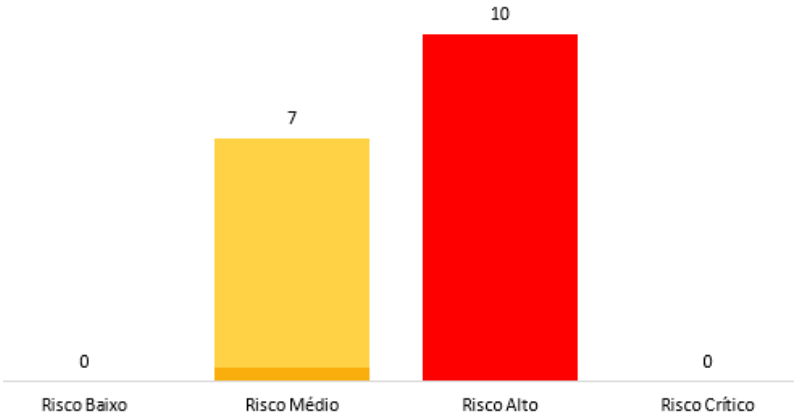
Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
Passive corruption in the private sector (Article 8 of Law No. 20/2008 of 21 April)	1. Receiving advantages from suppliers (leasing, maintenance, facility services, insurance) in exchange for awards or better contractual conditions. 2. Acceptance of benefits to influence payment approvals or contract renewals.	LIKELY	STRONG	HIGH	8. Annual internal audit 9. Legal, financial and payroll management advice, provided in an outsourced manner Possible measures: 10. Fund Management Policy 11. Supplier Evaluation 12. Control of conflicts of interest 13. Due diligence procedures 14. Money Laundering (AML) Prevention Policies	POSSIBLE	ELEVATED	MEDIUM
Active corruption in the private sector (Article 9 of Law No. 20/2008 of 21 April)	1. Offering advantages to suppliers in order to obtain more favourable conditions in leasing, insurance, maintenance or *facility* management. 2. Attempting to influence private audits or evaluations through undue compensation.	LIKELY	STRONG	HIGH		POSSIBLE	ELEVATED	MEDIUM
Fraud in obtaining a subsidy or subsidy (Article 36 of Decree-Law No. 28/84 of 20 January)	1. Provision of false financial information in applications for public support or incentives for facilities, fleet or operations. 2. Manipulation of *facility* costs or operating expenses to artificially increase support granted.	LIKELY	STRONG	HIGH		POSSIBLE	ELEVATED	MEDIUM

Crime	Risk Event	Probability	Impact	Inherent Risk	Preventive and Corrective Measures	Probability	Impact	Residual Risk
Fraud in obtaining credit (art. 38º 36º del Decreto-Lei nº 28/84, of 20 January)	1. Alteration of liquidity forecasts or budgets for obtaining internal financing. 2. Omission of liabilities or risks in the submitted reports.	LIKELY	STRONG	HIGH		REMOTE	MODERATE	LOW
Deviation of subsidy, subsidy or subsidized credit (Article 37 of Decree-Law No. 28/84, of 20 January)	1. Redirecting *payroll* funds, benefits or project expenses for unauthorized purposes. 2. Misuse of approved funds for personal or other departmental expenses. 3. Appropriation of resources intended for projects or benefits for undocumented purposes.	LIKELY	ELEVATED	HIGH		REMOTE	MODERATE	LOW

ANNEX II – Inherent Risk







ANNEX III – Residual Risk