sysmatch
IT consulting

PROGRAM
YOUR BUSINESS
FOR BETTER

www.sysmatch.com

Corruption and Related Offenses Risk Prevention Plan

INDEX

1. INTRODUCTION

General Objectives

The present Corruption and Related Offenses Risk Prevention Plan aims to identify and manage corruption risks and related infractions within Sysmatch. It also aims to plan and develop control activities and mitigation measures for identified risks, including preventive and corrective measures to reduce the likelihood and impact of these risks, and to monitor their execution.

Scope of Application

The PPR applies to all interactions among workers themselves, but also to relationships with third parties, whether public or private. This includes organs, services, public bodies or entities, and/or providers of public services and their employees or agents.

Definitions, Acronyms and Abbreviations

In the following tables, all definitions, acronyms, and abbreviations used in the document are identified, as well as the terms necessary for understanding it.
no documento, bem como os termos necessários ao seu entendimento.

DEFINITIONS	
Corruption	Illegal act in which a person offers, delivers, solicits, or accepts any type of offer, benefit, or promise, with the intention of obtaining for themselves or for a third party an illicit advantage involving an abuse of position.
Risk	Probability of a situation occurring with potential negative impact.
Threat	An event that can trigger an incident, resulting in material or immaterial damage to its assets.
Confidentiality	A feature that prevents unauthorized disclosure of assets. Considers all information assets..
Integrity	A characteristic that prevents unauthorized modification or destruction of assets. Integrity is linked to the functional reliability of information systems.

ACRONYMS AND ABBREVIATIONS	
RGPC	General Regime for Corruption Prevention
PPR	Corruption and Related Offenses Risk Prevention Plan

2. GENERAL FRAMEWORK

On December 9, 2021, Decree-Law No. 109-E/2021 ("Decree-Law") was published in the Official Gazette, creating the National Anti-Corruption Mechanism ("MENAC") and approving the General Regime for Corruption Prevention ("RGPC"). This Decree-Law follows the approval of the National Anti-Corruption Strategy and aims to prevent, detect, suppress, and sanction acts of corruption and related offenses.

In this context, a Corruption and Related Offenses Risk Management Plan has been developed for Sysmatch, as entities covered by the RGPC (50 or more employees) must implement a compliance program, which should include a Corruption and Related Offenses Risk Prevention Plan ("PPR" or "Plan"), a code of ethics and conduct, a whistleblowing channel, and a training plan.

It is further determined that the Corruption and Related Offenses Risk Prevention Plan (PPRCIC) must include:

- Identification of corruption risks and related offenses in each area;
- Identification of measures taken to prevent risks;
- Identification of those responsible for managing the risk management plan;
- Provision for the preparation of an annual execution report.

3. INTRODUCTION

Sysmatch, aware of the need to fulfill the obligations set forth in the RGPC and to promote a culture of transparency, has chosen to adopt a risk management system based on a Management Risk Prevention Plan (PPRG), which naturally includes those related to corruption and related offenses.

In this regard, Sysmatch has undertaken the recognition and evaluation of risks in each area of activity, through internal and external sources, also assessing the likelihood of occurrence and the impact of the risk, the preventive and corrective measures suitable for mitigation and/or contingency planning, as well as identifying those responsible for their development and proposing action.

The PPR thus covers the entire organization and activities carried out in the company Sysmatch, and its objectives are:

a) Identification, analysis, and classification of risks and situations that may expose Sysmatch to acts of corruption and related offenses, including risks associated with the performance of duties by members of the Management and Board of Directors, considering the sector's reality and the geographical areas in which it operates;
b) Preventive and corrective measures aimed at reducing the likelihood of occurrence and the impact of the identified risks and situations.
c) Increase awareness among employees;

4. METHODOLOGY, ACTIVITY IDENTIFICATION AND RISK

The methodology for identifying, analyzing, and classifying risks and situations that may expose Sysmatch to acts of corruption and related offenses, aligned with the requirements listed in Decree-Law No. 109-E/2021 of December 9, considered:

a) The areas of activity within the company where the risk of engaging in acts of corruption and related offenses is observed;
b) The likelihood of occurrence of situations that pose a risk and their foreseeable impact, in order to allow for the gradation of risks;
c) Preventive and corrective measures aimed at reducing the likelihood of occurrence and the impact of the identified risks and situations;
d) In situations of high or maximum risk, the most comprehensive preventive measures, with their execution being given priority;
e) The designation of the overall responsible person for the execution, control, and review of the PPR.

The PPR applies to all employees of Sysmatch, and its principles are extendable to external consultants, service providers, suppliers, and agents or any third parties with whom contractual/commercial relationships are maintained.

5. PROBABILITY OF OCCURRENCE

The assessment and classification of risks result from the combination of the probability of occurrence of situations posing a risk with the severity of their predicted impact, which leads to a risk level following a scale with four levels (very low, low, medium, high, and very high). Based on these levels, different response strategies will be defined.

PROBABILITY		
Value	**Level**	**Description**
1	Very Low	There is no historical record of occurrence (P=0)
2	Low	It may occur / has occurred at least once in the company's history and no more than once per year (1 < P ≤ 1x per year)
3	High	It may occur / has occurred more than once per year and up to once per month / occasional situation, non-recurring (1x per year < P ≤ 1x per month)
4	Very High	It may occur / has occurred more than once per month / recurring situation (1x per month < P)

6. RISK ASSESSMENT

Partial Risk Calculation

Partial risk is calculated by combining the level of impact with the level of probability of occurrence, using the following formula:

Partial Risk = Probability x Impact [1-16]

PARTIAL RISK LEVEL

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

Impact

Control Mechanisms - Preventive Measures

Once the risks have been assessed, the appropriate responses must be defined to ensure that Sysmatch is not exposed to residual risks above those defined.

As a result of the identification and assessment of risks, Sysmatch has drawn up the risk matrix shown in Annex 1, which presents the risks identified in Sysmatch's areas of activity, with exposure to the risks of corruption and related offenses, analyzes the probability of occurrence, the potential impact and, consequently, the degree of risk of each risk identified and identifies the preventive and control measures (implemented and/or being implemented associated with the mitigation of each risk).

With regard to the preventive and control measures (implemented and/or being implemented) identified, they can be based on transversal controls (policies, manuals, standards, among others that mitigate the risks of corruption and related infractions transversally) and operational controls (processes and procedures implemented at an operational level).

The control measures can be classified as follows:

CONTROL MEASURES		
Value	**Level**	**Description**
1	Low	Non-existent or ineffective
2	Medium	There are measures with room for improvement
3	High	Existence of effective measures

Calculation of Real Risk

The risk calculation is done by combining the impact level with the probability of occurrence level, using the following formula:

$$\text{Real Risk} = \frac{\text{Partial Risk (Probability x Impact)}}{\text{Control Measures}}$$

The real risk level can be classified as:

Value of Real Risk	Description
≤ 4	Acceptable Risk
5 – 9	The manager must analyze whether to accept the risk or take measures
≥ 10	If it's deemed unacceptable, it's mandatory to determine actions

Monitoring, Evaluation and Supervision of the PPR

Monitoring of the Plan is ensured through periodic review and testing of its implementation and effectiveness of the respective preventive measures.

In accordance with the provisions of subparagraphs a) and b) of paragraph 4 of article 6 of Decree-Law No. 109-E/2021 of December 9, the execution of the PPR is subject to the following controls:

- The preparation, in the month of October, of an interim evaluation report for situations identified with high or maximum risk;
- The preparation, in the month of April of the following year, of the annual evaluation report, which must include, among other things, the quantification of the degree of

implementation of the preventive and corrective measures identified, as well as the forecast for their full implementation.

The PPR is reviewed every three years or whenever there is a change that justifies its revision.

7. CONCLUSION

During the period under review, there is no evidence of violations of the mechanisms for prevention, detection, and response to cases of irregular or illicit conduct.

No complaints, grievances, or reports regarding acts of corruption, fraud, or related offenses have been directly brought to Sysmatch's attention concerning any of its employees, members of its social bodies, or any other entities.

As a result of internal analysis, the plan is being adhered to, and there are no actual or potential situations conducive to acts of corruption and/or related offenses.

ANNEX 1 - Risk Matrix for Corruption and Related Offenses

The risk matrix presented below covers the entire organization and activity of Sysmatch, in accordance with paragraph 3 of Article 6 of Decree-Law No. 109-E/2021.

AREA OF RISK	ACTIVITIES UNDERTAKEN	ASSOCIATED RISKS	IMPACT	PROBABILITY	RISK LEVEL	PREVENTION AND/OR MITIGATION MECHANISMS
Acquisition of Goods and Services	Management of procurement processes for goods and services and quality control of the services provided	Favoring suppliers of goods/services in order to benefit themselves or third parties.	2	1	2	Code of Conduct; Intervention by various departments in the process of acquiring goods or services; Control of expenditure by the Administrative and Financial (AF) department; Supplier qualification process under the ISO 9001 standard; Regular updating of the list of qualified suppliers; Quality control of the services provided; Regular audits by external bodies; Supplier audit process; Procedure for prior risk assessment of third parties; Implementation of a whistleblowing channel. Confidentiality awareness actions;
		Disclosure of confidential information.	3	2	6	
		Acquisition or misappropriation of assets for your own benefit or that of a third party.	2	1	2	
	Acquisition	Active or passive corruption.	2	1	2	Code of Conduct; Procedures for the Acquisition of Goods/Services; Internal control procedures; Procedure for prior risk assessment of third parties; Disciplinary procedures provided for and published for perpetrators of illegal acts; Regular review of procedures; Implementation of whistleblowing channels.
	Verification of Compliance with Deliveries of Goods and Services	Deviation from the quantity and/or quality of the goods/services contracted; Withholding of material by an employee; Abuse of power; Influence peddling.	2	2	4	Code of Conduct; Policy on the use of resources; Information and awareness-raising for employees; Internal control procedures; Disciplinary procedures laid down and published for perpetrators of illegal acts; Supplier qualification process under ISO 9001; Regular audits by external bodies;

AREA OF RISK	ACTIVITIES UNDERTAKEN	ASSOCIATED RISKS	IMPACT	PROBABILITY	RISK LEVEL	PREVENTION AND/OR MITIGATION MECHANISMS
		Counterfeiting.	2	1	2	Implementation of an internal whistleblowing channel.
Invoicing of goods or services	Invoicing of goods/services	Non-registration of services rendered; Active or passive corruption; Money laundering; Embezzlement; Tax evasion.	3	1	3	Code of Conduct; Record of employee hours spent on clients; Reinforcement of internal control measures with a view to tax evasion and prevention of corruption and related infractions; Measures to inform and raise awareness among employees of the consequences of corruption and related infractions; Internal and external audit program; Implementation of an internal whistleblowing channel.
	Invoice control	Non-registration of services rendered; Active or passive corruption; Money laundering; Embezzlement; Tax evasion.	3	1	3	
	Computer system failure	Receipt of amounts without the issuance of a discharge document by the computer system.	2	2	4	Code of conduct; Business continuity plan; Internal policies of the Management System; Controls arising from certification to the 27001 standards and the SG; Reinforcement of internal control measures with a view to preventing corruption and related infractions; Cybersecurity policies;
Administration	Decision-making process	Obstacles to transparency; Influence peddling; Misappropriation or misuse of assets, particularly for private purposes.	3	1	3	Code of Conduct; Meetings of the Board of Directors ATA's archive in an internal digital repository and on paper; Training and awareness-raising for employees and managers; Internal control procedures; Control and approval of accounts by the Administrative and Financial Department (AF); Strengthening of internal control measures with a view to preventing corruption and related offenses; Internal and external audits of financial reports; Implementation of an internal whistleblowing channel

AREA OF RISK	ACTIVITIES UNDERTAKEN	ASSOCIATED RISKS	IMPACT	PROBABILITY	RISK LEVEL	PREVENTION AND/OR MITIGATION MECHANISMS
Financial management	Budget control Accounting management	Adulteration and/or omission of information that conditions the truthful and transparent representation of the financial situation; Misappropriation of funds/value; Money laundering;	3	2	6	Code of Conduct; Internal control procedures; Access management; Various levels of information validation; Disciplinary procedures laid down and published for perpetrators of illegal acts; Periodic control of expenses by Business Unit; Control and approval by the Administrative and Financial Department (AF); Internal and external audits of financial reports; Strengthening of internal control measures with a view to preventing corruption and related infractions; Implementation of an internal whistleblowing channel. Training and internal awareness-raising activities for employees and managers; Implementation of internal control measures - periodic and random verification of Processes; Promote and increase the exercise of supervision and inspection activities in a constant and interventionist manner, in order to guarantee compliance with the rules in force and to sanction the infractions detected;
People	Recruitment and selection process	Ambiguous recruitment and selection criteria.	2	2	4	Code of Conduct; Multi-stage recruitment process; Participation of various stakeholders in the recruitment process; Existence of a structured recruitment procedure; Control and final approval by the company/business unit; Internal and external audits; Implementation of an internal whistleblowing channel. Preparation of an Annual Training Plan based on the initiatives proposed by the various Business Units, taking into account internal needs; Possibility for the employee to suggest the training required
		Illicit favoritism in the choice of human resources to be recruited.	2	2	4	
	Professional training	Falsification of training documents.	3	1	3	

AREA OF RISK	ACTIVITIES UNDERTAKEN	ASSOCIATED RISKS	IMPACT	PROBABILITY	RISK LEVEL	PREVENTION AND/OR MITIGATION MECHANISMS
						or desired; Control, monitoring and evaluation of the training activities carried out; DGERT certification; Internal and external audit process; Implementation of an internal whistleblowing channel.
	Processing pay, allowances, deductions and individual employee files	Manipulation of information in order to facilitate the undue payment of benefits and compensation; Risk of improper access to personal information / breach of confidentiality; Risk of failure to record information in personal databases; Tax evasion.	2	1	2	Code of Conduct; Access Management; General Data Protection Regulation; Automatic entry and exit control; Training and awareness-raising for managers and employees on the risks of corruption; Training and awareness-raising for employees on data protection; Intervention of more than one interlocutor in the processing of remuneration, allowances and discounts; Control by Administrative and Financial (AF) department; Internal and external audit plan; Implementation of an internal whistleblowing channel.
Information Systems	Information Systems Security; Management of computer programs and applications; Identification and Authentication of users; Authorization and access control; Audit logs in programs and applications	Failure to comply with internal security procedures for their own benefit or for the benefit of third parties; Misuse of databases and information in general; Passive corruption for illicit acts; Failures by employees in the information systems area for their own benefit Medium Low Weak Code of Conduct; Implementation of a Privacy Management System; Continuous	3	1	3	Code of Conduct; Implementation of a Privacy Management System; Continuous monitoring of information security; Training and awareness-raising for employees; Internal control procedures; Disciplinary procedures laid down and published for perpetrators of illegal acts; Controls arising from certification to ISO 27001, ISO 9001 and NP 4457 standards; Implementation of an internal complaints channel.

AREA OF RISK	ACTIVITIES UNDERTAKEN	ASSOCIATED RISKS	IMPACT	PROBABILITY	RISK LEVEL	PREVENTION AND/OR MITIGATION MECHANISMS
		monitoring of information security; Training and awareness-raising for employees; Internal control procedures; Disciplinary procedures laid down and published for perpetrators of illicit acts; Controls arising from certification of their own and third parties.				
Legal	Disciplinary procedures	Active or passive corruption; Failure to sanction illicit behavior by employees.	2	1	2	Code of conduct; Reinforcement of internal control measures with a view to preventing corruption and related infractions; Decentralization of the legal area for service providers; Implementation of a code of conduct for suppliers; Disciplinary procedures duly listed according to the type of unlawful act; Implementation of whistleblowing channels.
	Legal advice	Disclosure of confidential information.	2	2	4	Decentralization of the legal area for service providers; Implementation of a code of conduct for suppliers.
	Litigation	Disclosure of confidential information; Active or passive corruption; Influence peddling.	2	2	4	Decentralization of the legal area for service providers; Implementation of a code of conduct for suppliers.