moOngy.
Minds on the move

Plano de Prevenção de Riscos de Corrupção e Infrações Conexas

Índice

CONTROLO DO DOCUMENTO

1.1 – Identificação	
Empresa / Departamento	Grupo MoOngy S.A.
Nome	Plano de Prevenção de Riscos de Corrupção e Infrações
Localização	Moongy S.A.
Versão atual	R 1

1.2 – Histórico de Revisões			
Versão	Data de Revisão	Sumário de Alterações	Autor
R 0	18/07/2023	Redação Inicial	DPG
R 1	15/01/2025	Revisão por motivos de alterações na estrutura orgânica nos termos do disposto no artigo 6º, nº5 do DL nº 109-E/2021, de 9 de dezembro	G&C

1.3 – Aprovação do Documento			
Aprovado por:	Data de Aprovação	Cargo/Departamento/Empresa	Versão
André Dias Lopes	06/02/2025	CEO	R1

CAPÍTULO I – O GRUPO MOONGY S.A.

1.1. Enquadramento

Com um expresso objetivo de aumentar a confiança dos cidadãos nas suas instituições, a União Europeia desafiou os Estados-membros a reforçar as políticas de combate à corrupção.

Portugal, enquanto estado-membro subscreveu e integrou na ordem jurídica instrumentos internacionais em matéria de prevenção e repressão da corrupção e do branqueamento de capitais. A montante do fenómeno advém a Estratégia Nacional Anticorrupção 2020-2024, que propõe um conjunto de ações, articuladas e integradas, tendentes a permitir ao estado agir tanto no domínio publico como no privado assumindo um claro compromisso e empenho na missão por parte de Portugal.

Neste sentido, o Decreto-Lei nº109-E/2021 estabelece a autoridade de controlo específica para a monitorização e fiscalização do cumprimento e empenho desta missão por parte das instituições (públicas e privadas): o Mecanismo Nacional Anticorrupção("*MENAC*") aprovando também o Regime Geral de Prevenção da Corrupção("*RGPC*").

O RGPC estabelece a implementação de ferramentas que consolidam toda a missão referida até ao momento nas instituições:

- Plano de Prevenção de Riscos de Corrupção e Infrações Conexas;
- Código de Conduta (remissivo à temática)
- Canal de Denúncias
- Programa de Formação

Por sua vez, a Norma Internacional *ISO 37 001:2016 "Anti-Bribery Management Systems – Requirements with guidance for use"*, a qual institui requisitos e linhas de orientação para o estabelecimento, implementação, manutenção, revisão e melhoria dos sistemas de gestão anticorrupção, oferece uma definição mais ampla e simples do risco de corrupção considerando-o como um "efeito de incerteza nos objetivos" podendo esse "efeito" ser positivo ou negativo mas representando sempre um desvio face ao esperado.
Na prática pode-se falar em corrupção quando uma pessoa abusa do poder que lhe é confiado em troca de receber uma vantagem indevida.

O Grupo MoOngy reconhece a necessidade, concorda com a importância da implementação do RGPC, comprometendo-se com este objetivo, entendendo o real valor do combate à corrupção para o reforço da qualidade da democracia, plena realização do Estado de Direito, assegurando a igualdade de oportunidades e favorecendo um ambiente de crescimento económico, robustecendo as Instituições e respetiva credibilidade por forma a aumentar o nível de confiança dos cidadãos em particular, os *stakeholder*s do Grupo MoOngy.

Empenhado nesta missão, na sequência de um compromisso de aprofundamento da Compliance do Grupo, a MoOngy S.A. elabora o seu Plano de Prevenção de Riscos de Corrupção e Infrações Conexas do Grupo MoOngy (doravante designado "PPR"), aplicável às várias empresas constituintes do Grupo.

Este PPR almeja ser a resposta a uma das (na nossa ótica) mais exigentes obrigações estabelecidas pelo RGPC, consolidando-se como um passo e um instrumento importante de combate à corrupção e projetando-se no presente e novíssimo Sistema implementado. Este, resulta de uma análise exaustiva aos diferentes setores do grupo, identificando os fatores e classificando-os, por forma a implementar os mecanismos de controlo existentes para mitigar esses riscos.

1.2. Caraterização do Grupo

O Grupo Moongy é a nova denominação do que era anteriormente o Grupo HIQ Consulting, que detém um vasto conjunto de empresas e marcas, destacando-se a agap2IT, a KCSIT, a Bee Engineering e a Adentis, para referir apenas algumas.

O Grupo Moongy nasceu em Portugal, em 2005, através da incorporação da HIQ Consulting, SA, por iniciativa de 3 empreendedores franceses, que reconheceram em Portugal as condições ideais para criar um grupo focado na engenharia e nas tecnologias de informação. Efetivamente, estes 3 empreendedores identificaram em Portugal um enorme potencial, dada a existência de recursos humanos de elevada qualidade, com uma formação de excelência, com capacidade de trabalho em contexto internacional e com um custo de vida muito interessante segundo os padrões europeus.

Desde a sua criação que o Grupo Moongy tem no seu ADN uma vocação internacional. Assim, ainda em 2007 foi criada a agap2 France, tendo a sede social do grupo passado a localizar-se em Paris, e a faturação do grupo ascendeu a €8mn.

Em Portugal o Grupo Moongy possui seis empresas, designadamente:

- Moongy, também conhecida como agap2it Portugal
- KCSIT
- Bee Engineering Portugal
- Adentis Portugal
- Team IT
- CodeWin

Cada uma destas empresas foca-se em atividades ou segmentos distintos.

1.2.1. MoOngy / Agap2it Portugal

Sendo a primeira empresa do grupo, esta define-se como uma organização global de consultoria empenhada na inovação e na aplicação das tecnologias de informação. A Agap2IT coopera com os seus clientes, na perspetiva de otimizar os seus desempenhos, e organiza-se em várias áreas especializadas:

- DXSpark: a DXSpark desenvolve um trabalho de proximidade com os seus clientes, auxiliando-os no seu processo de transformação digital;
- Highdome: A highdome apresenta soluções de segurança para diferentes tipos de cliente, assegurando o futuro das organizações;
- ATS: a agap2 Technology Services, apresenta aos seus clients uma nova marca e uma forma distinta de pensar e fazer tecnologia.
- ISM: As plataformas digitais que gerem ao pormenor a evolução desportiva, escolar, social e pessoal do principal ativo desportivo: os atletas;

Por outras palavras, a Agap2IT gosta de ser distinguida por ser uma organização *people-oriented*, capaz de mobilizar pessoas e gerir os seus colaboradores tendo presente o conceito e as virtudes do *Employeeship*, competências e tecnologias, pela sua excelência e inovação e com o princípio orientador de fazer sempre mais e melhor na resposta de ajudar e qualificar as suas pessoas e o seu mercado.

Para conquistar os desafios permanentes da evolução das Tecnologias de Informação, a Agap2IT aposta na sua equipa porque pretende ser uma referência no mercado das Tecnologias de Informação, com os melhores profissionais.

1.2.2. KCS IT

É uma empresa de serviços de consultoria e *outsourcing*, especialista em *Project Management*. Desenvolve soluções tecnológicas customizadas às necessidades específicas dos seus clientes, e apesar da sua especialização em gestão de projetos na área dos sistemas de informação, o seu core é a prestação de Serviços Tecnológicos, nomeadamente Desenvolvimento Aplicacional, Análise Funcional, Administração de Sistemas, Testes e Qualidade.

A sua atividade divide-se nas seguintes áreas de especialização:

- **Outsourcing Services**: externalização de talentos de IT adequados à realidade de cada organização, assegurando a flexibilidade e agilidade necessárias.
- **Consultoria**: consultoria estratégica nas áreas de *Research & Development*, *Team as a Service* e Projetos *Turn Key*.
- **Inovação**: desenvolvimento de projetos de inovação e de desenvolvimento de produto.

1.2.3. Bee Engineering Portugal

A Bee Engineering é uma consultora de tecnologias da informação e comunicação que apoia as organizações a encontrar a solução tecnológica certa para catalisar o seu crescimento, caracterizando-se por levar as melhores práticas de engenharia e tecnologia ao mundo das empresas.

A empresa tem vindo a apostar na especialização em gamificação, tanto que criou uma área de distinção na sua oferta – *Nectar Interactive* – com o objetivo de gamificar as experiências digitais das marcas e suas audiências.

A empresa divide-se nas seguintes áreas:

- **Consultoria**: leva a sua equipa de consultores e gestores ao cliente, por forma a responder às suas necessidades e desafios de engenharia de sistemas e engenharia de software.

1.2.4. Adentis

É uma empresa de consultoria de informação que se apresenta como impulsionadora do processo de transformação digital do país, através do seu centro de competências em Lisboa e no Porto, bem como pela aposta que fazem no desenvolvimento da carreira dos seus colaboradores, essencial para responderem aos desafios tecnológicos emergentes.

A oferta da Adentis está globalmente alinhada com a 3ª plataforma, descrita pela IDC, assente em 4 pilares tecnológicos: *Mobility*, *Big Data*, *Social Business* e Cloud Computing, e divide-se nas seguintes áreas:

- **Strategy**: presta um serviço especializado de desenvolvimento de projetos sob a orientação e responsabilidade de gestão do cliente.

- **Nearshore Services**: esta oferta possibilita que um projeto seja desenvolvido num país diferente do local de implementação.
- **Research & Development**; materializa soluções inovadoras em conjunto com os parceiros para os mais diversos setores de mercado.

1.2.5. Team IT

A Team-IT posiciona-se como uma empresa especialista em consultoria, procurando também ser uma extensão das equipas técnicas dos seus parceiros, por forma a garantir um apoio de qualidade para os projetos, com vista a potenciar o crescimento e a inovação.

As suas equipas são especializadas no Desenvolvimento, Manutenção e Qualidade de Software; Business Intelligence; Administração de Sistemas, Redes e Bases de Dados; assim como outros que os apoiam nas respostas destas áreas.

1.2.6. Codewin

A Codewin é uma empresa especializada em desenvolvimento de software, ERP e CRM. A Codewin cria, implementa e suporta soluções que dão vida a ideias inovadoras, utilizando tecnologia de ponta para proporcionar experiências intuitivas aos utilizadores.

A empresa oferece três principais modelos de Serviço

- **Outsourcing Estratégico:** Adiciona competências necessárias às equipas dos parceiros, aumentando as suas capacidades estratégicas.
- **Soluções Chave na Mão:** Assume total responsabilidade pelo design, desenvolvimento e entrega de projetos prontos a utilizar.
- **Equipa como Serviço**: Fornece equipas especializadas que se integram totalmente nos projetos dos parceiros, permitindo escalabilidade rápida e agilidade no desenvolvimento.

O **Grupo Moongy**, detentor das empresas acima descritas, reúne as competências necessárias para assumir as diferentes fases de um projeto, desde o levantamento de requisitos até à implementação, entrega e manutenção da solução, aplicando as metodologias adequadas a cada fase e ao objetivo de cada projeto, e está organizada em seis unidades técnicas especializadas descritas anteriormente.

E como se observa, as atividades desenvolvidas pelas empresas do Grupo Moongy são muito especializadas, requerendo não só conhecimentos técnicos elevados, como também a sua aplicação em situações exigentes e muito diversificadas.

1.3. Estrutura Orgânica e Competências

O Grupo é constituído pelas unidades de estrutura, transversais a todas as empresas do Grupo. Estas são responsáveis pela manutenção dos serviços de necessidade comum dentro do Grupo, as quais assumem genericamente, as seguintes competências:

1.3.1. MoOngy S.A.

- **Conselho de Administração**

Responsável por prosseguir os interesses gerais da sociedade, proceder a todos os atos previstos no Código Societário para o tipo de Sociedade Anónima, proceder à nomeação e fiscalização da atuação do CEO do Grupo.

- **Conselho Fiscal**

Responsável pela Fiscalização das Contas da Sociedade Anónima

- **Entidade Auditora**

Responsável pela fiscalização externa das contas da Sociedade, esta terá que ser totalmente independente da sociedade anónima, será uma sociedade externa.

- **CEO**

Responsável por assegurar a gestão corrente da sociedade, representar a sociedade em juízo e fora dele, estabelecer a organização do grupo e suas normas de funcionamento, constituir mandatários e representante máximo das relações externas do grupo.

- **COO**

O COO é o Responsável pelo departamento de IT Services que suporta o Grupo MoOngy S.A. por inteiro, além disso, é também o Responsável pelas operações nas empresas fora de Portugal.

- **CFO**

Responsável pelo departamento Administrativo e Financeiro do Grupo, procede à Gestão Financeira do Grupo, todas as operações que envolvem fundos financeiros são governadas por este Departamento. Responsabilidades referentes à Logística e Zelo pelas infraestruturas estão também

alocadas a este Departamento. Além disso, todos os processos de contratação estão também sob responsabilidade deste Departamento.

- Finance Control

Todos os temas relacionados com fornecedores, bancos, pagamentos, recebimentos e cash flow, DSO.

- People Management

Todos os temas relacionados com processos de admissão, documentos administrativos relacionados, seguro de saúde, medicina no trabalho, e diversos temas administrativos além disso, responsável por todos os temas relacionados com contratos de trabalho e questões laborais inerentes aos mesmos.

- Legal

Agora integrado no Departamento People Management, contudo, devido à sua especificidade, optámos por manter para efeitos. Responsável pela gestão dos processos migratórios, atos ordinários da vida das sociedades comerciais do grupo, gestão das marcas e validação de todos os contratos do Grupo MoOngy.

- Accounting & Fiscal

Todos os temas relacionados com contabilidade, fiscalidade, auditorias, inspeções, consolidação de contas com grupo, fechos anuais e certificação legal de contas

- Business Control

Todos os temas relacionados com Faturação.

- CHRO

Responsável pelas áreas de Recursos Humanos do Grupo MoOngy e respetiva gestão corrente.

- moOngy Human Capital

O departamento moOngy Human Capital é responsável por estabelecer a gestão centralizada dos departamentos de Recursos Humanos das diversas empresas do Grupo MoOngy, além disso,

estabelece o suporte direto à CHRO na tomada de decisões de grande relevância para as decisões em matéria de Recursos Humanos do Grupo MoOngy.

- Departamento de Training & Development

O Departamento do Training é responsável pelas mais distintas ofertas formativas do Grupo por forma a promover o conhecimento dos colaboradores do Grupo.

- CMO

Responsável pelo departamento de marketing e comunicação, este departamento é responsável por toda a imagem e comunicações externas e internas produzidas para o Grupo MoOngy S.A. Além disso, também os eventos e toda a gestão destes está sob responsabilidade deste Departamento.

- Governance & Compliance (anteriormente designado DPG)

Este departamento garante que a empresa opera em conformidade com regulamentos, normas e padrões, ajuda ainda na gestão da inovação e captação de financiamento para o desenvolvimento/otimização de atividades de investigação e desenvolvimento (I&D).

- CIO

Responsável pelos departamentos que têm como missão assegurar o correto funcionamento de todos os sistemas de informação que possibilitam o correto funcionamento das várias empresas e marcas do grupo moOngy em Portugal.

- ITCS

O departamento ITCS é responsável pela infraestrutura tecnológica da empresa, incluindo a gestão de servidores, sistemas de recuperação de desastre, redundâncias, backups, redes, licenciamento de software, e cloud.

Assegura também a gestão de dispositivos como portáteis e outros componentes associados. No âmbito da cibersegurança, o departamento implementa e gere políticas e ferramentas de segurança, monitorizando continuamente ameaças para proteger os dados e sistemas críticos da organização contra acessos não autorizados e ciberataques.

Este departamento trabalha para garantir a continuidade do serviço e a resiliência dos sistemas, em linha com as melhores práticas de segurança.

- MAD (Middleware & Application Development)

O departamento de Middleware & Application Development (MAD), em cooperação com restantes áreas de Moongy Information Systems e departamentos do grupo MoOngy, é especializado na criação, manutenção, gestão e otimização de soluções que garantem a comunicação e operacionalidade entre sistemas do grupo e suas empresas/marcas.

- Research & Development (LABs)

O departamento LABs é uma área dedicada à exploração de tecnologias emergentes e ao teste de novas metodologias no desenvolvimento de software.

A equipa concentra-se em áreas de inteligência artificial (IA), blockchain, e outras tecnologias inovadoras que possam trazer benefícios futuros para a empresa.

LABs testa, implementa e avalia novos conceitos e soluções que, após avaliação, poderão ser incorporados em futuros projetos.

Este departamento funciona como uma incubadora, estando separado das operações diárias, para permitir uma maior liberdade criativa e foco em inovação tecnológica.

- Digital Transformation (DT)

A equipa de transformação digital (DT) está focada em melhorar processos internos para aumentar a eficiência e a agilidade organizacional.

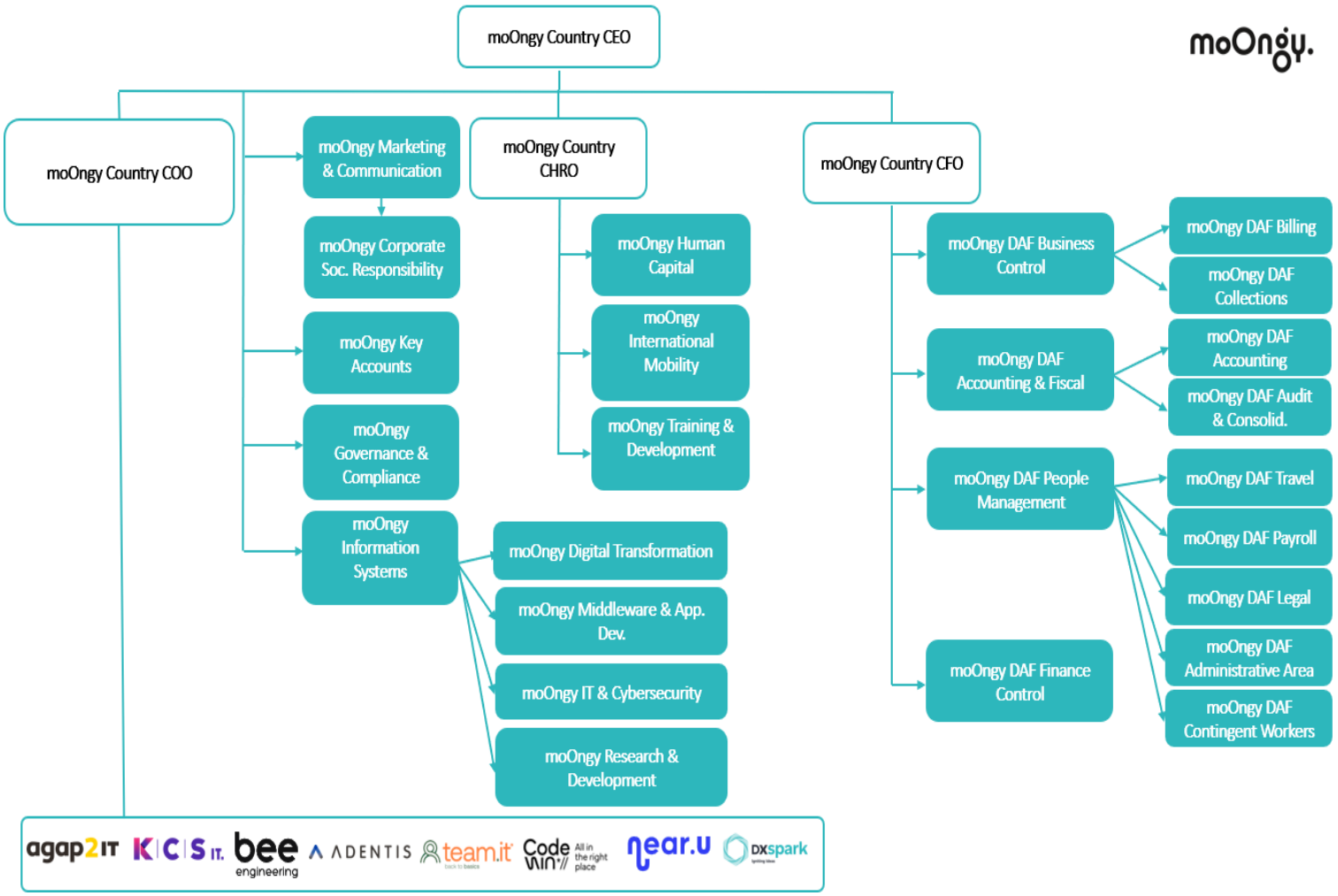
O seu objetivo central é otimizar operações, promover uma cultura digital e de dados entre as equipas, e implementar soluções que tragam maior produtividade e integração de sistemas., centralizando o ponto de acesso pelo utilizador.

Além disso, procura assegurar a integridade e conformidade digital, preparando a organização para enfrentar os desafios futuros com resiliência e inovação.

- Outras Áreas

De notar, as áreas moOngy Key Accounts (no caso das áreas de reporte ao CEO), moOngy International Mobility (no caso das áreas de reporte à CHRO) estão contempladas já nas áreas de responsabilidade respetiva nas demais empresas uma vez que de uma forma ou de outra, elas atuam no mesmo contexto das Áreas Funcionais de Outsourcing e RH (respetivamente). As equipas de última ramificação, para o caso das linhas de reporte à CFO (área financeira) acoplam-se nas principais, por forma a não granular demasiado o risco nos efetivos departamentos, tendo em conta atuarem em setores tão específicos que para contexto da nossa matriz, não contribui para a boa análise do PPR, não relevando para estes efeitos, Portanto perante os riscos identificados, considerámos pertinente granular o menos possível nas áreas financeiras, excetuando o caso do Legal, uma que conforme teremos oportunidade de verificar, persistem com alguns riscos detetados

com um nível de Severidade que importa atentar, teremos ter oportunidade de analisar em pormenor sendo importante para contexto do presente PPR.



Estes departamentos são transversais, fazem o suporte ao Grupo MoOngy S.A. por forma a permitir uma centralização e acompanhamento de todas as empresas do Grupo, maior maturidade e experiência dos serviços além de um controlo centralizado naquilo que é tradicionalmente conhecido como *Centro de Serviços Partilhados* promovendo um *verum Modelo de Governança Corporativa*.

Em cada uma das empresas-filhas do grupo, a estrutura do Organigrama altera-se, assim, cabe-nos detalhar de forma pormenorizada como funciona a ramificação em cada uma das empresas-filhas do Grupo MoOngy S.A.

1.3.2. Agap2it

- **CEO**

O CEO é o Responsável por assegurar a gestão operacional corrente da sociedade, representar a sociedade em juízo e fora dele, determina a equipa e organiza a hierarquia dentro da Agap2it.

- **ATS**

A Equipa ATS é responsável pelas operações de Outsourcing da Agap2, estes, fazem a gestão dos projetos onde se inclui a angariação de novos clientes e gestão das necessidades dos consultores que temos em projeto.

- **DXSpark**

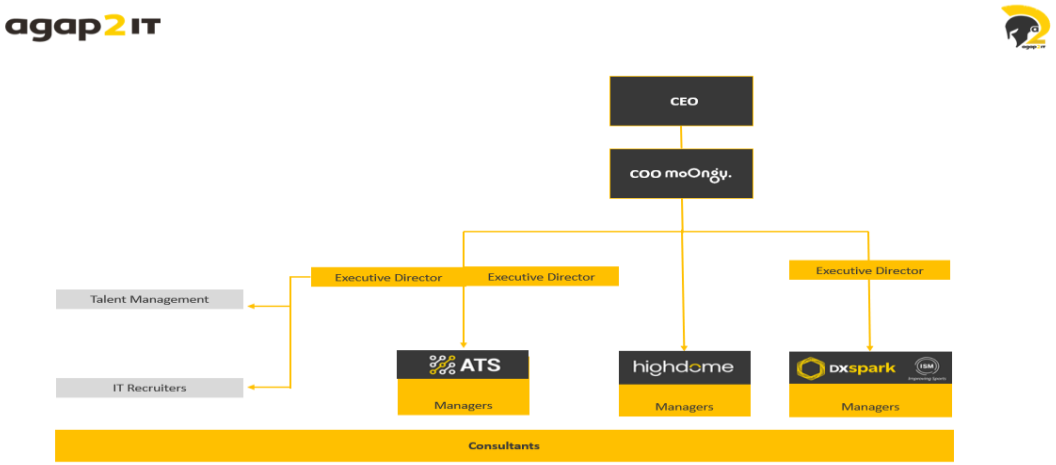
A equipa da DXSpark é responsável pelos designados Projetos Fechados, ou Projetos Chave na Mão. O trabalho de arquitetura de todo o produto está nas mãos da empresa, produtos à medida do cliente.

- **Talent Management**

Esta equipa é responsável pelo acompanhamento dos consultores da Agap2it, procuram ajudar a desenvolver a carreira através de contactos de proximidade com o consultor para atender às necessidades específicas dos consultores da Agap2it.

- **IT Recruiters**

Responsáveis pelo recrutamento na Agap2 as operações de contratação dos candidatos são geridas por este departamento que está encarregue de todo o processo até à entrada do Consultor.



1.3.3. KCS IT

- **Direto Geral**

O Diretor Geral é o Responsável máximo por assegurar a gestão de topo da sociedade, representar a sociedade em juízo e fora dele, estabelecer a organização da empresa e suas normas de funcionamento.

- **Diretor Executivo**

Responsável por assegurar a gestão corrente e operacional da sociedade, representar a sociedade em juízo e fora dele, gerir as operações, constituir mandatários e representante das relações externas do grupo.

- **Outsourcing Lisboa e Porto**

A equipa de Outsourcing tanto de Lisboa como do Porto, são responsáveis pelos negócios/angariação de clientes e novos projetos para a KCS-IT. Ambas as equipas (tanto de Lisboa como a do Porto), respondem cada uma às chefias das áreas geográficas de onde estão alocados.

- **Global Consulting Services**

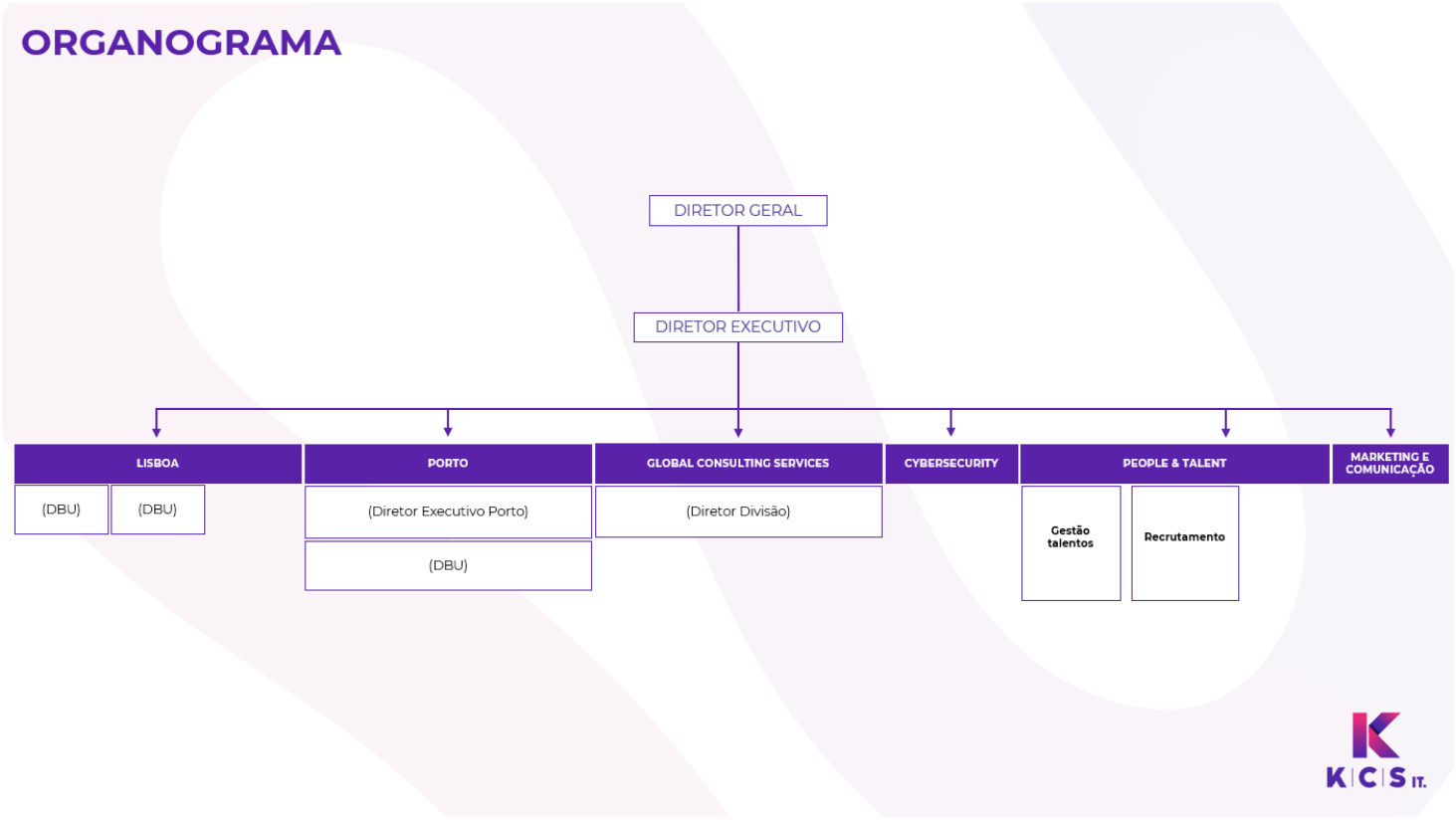
Dividido em duas equipas, uma das equipas é responsável pela gestão das operações internacionais da KCS-IT, consultores integrados em Projetos fora de Portugal constituem a equipa do Global, por outro lado, a equipa de projetos fechados, responsável pelos designados Projetos Fechados, ou Projetos Chave na Mão. O trabalho de arquitetura de todo o produto está nas mãos da empresa, produtos à medida do cliente.

- **Human Capital**

As operações de contratação dos candidatos são geridas por este departamento que está encarregue de todo o processo até à entrada do Consultor.

- **Marketing & Comunicação**

Este departamento é responsável por toda a imagem e comunicações externas e internas produzidas para a KCS-IT em específico. Além disso, também os eventos e toda a gestão destes está sob responsabilidade deste Departamento.



1.3.4. Bee Engineering

- COO

O COO é o Responsável por assegurar a gestão corrente da sociedade, representar a sociedade em juízo e fora dele, determina a equipa e organiza a hierarquia dentro da Empresa.

- Outsourcing de Lisboa e Porto

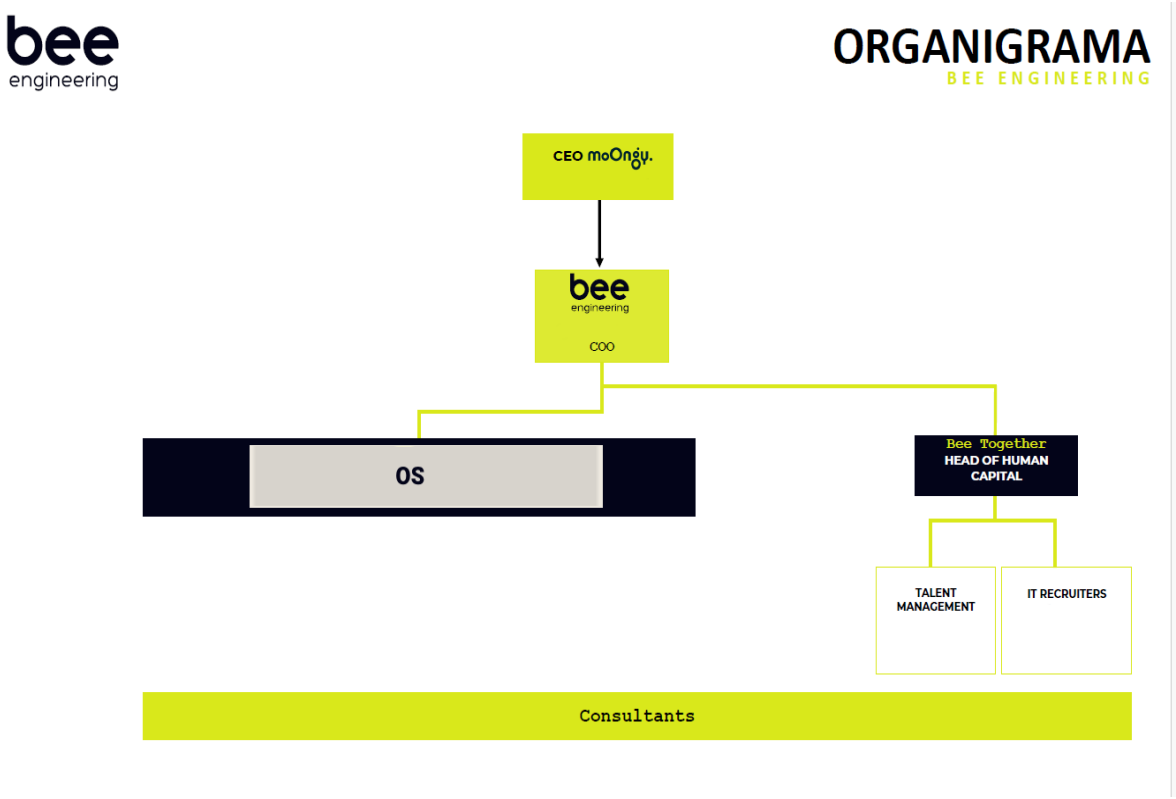
A equipa de Outsourcing tanto de Lisboa como do Porto, são responsáveis pelos negócios/angariação de clientes e novos projetos para a Bee Engineering. Ambas as equipas (tanto de Lisboa como a do Porto), respondem cada uma às chefias das áreas geográficas de onde estão alocados.

- Brand Manager

Este departamento é responsável pela imagem e comunicações externas e internas produzidas para a Bee Engineering em específico.

- Human Capital

As operações de contratação dos candidatos são geridas por este departamento que está encarregue de todo o processo até à entrada do Consultor. Por outro lado, a Gestão de Carreira do Consultor também está alocada a este departamento, com contactos de proximidade com o consultor.



1.3.5. Adentis

- Managing Director Lisbon / Porto

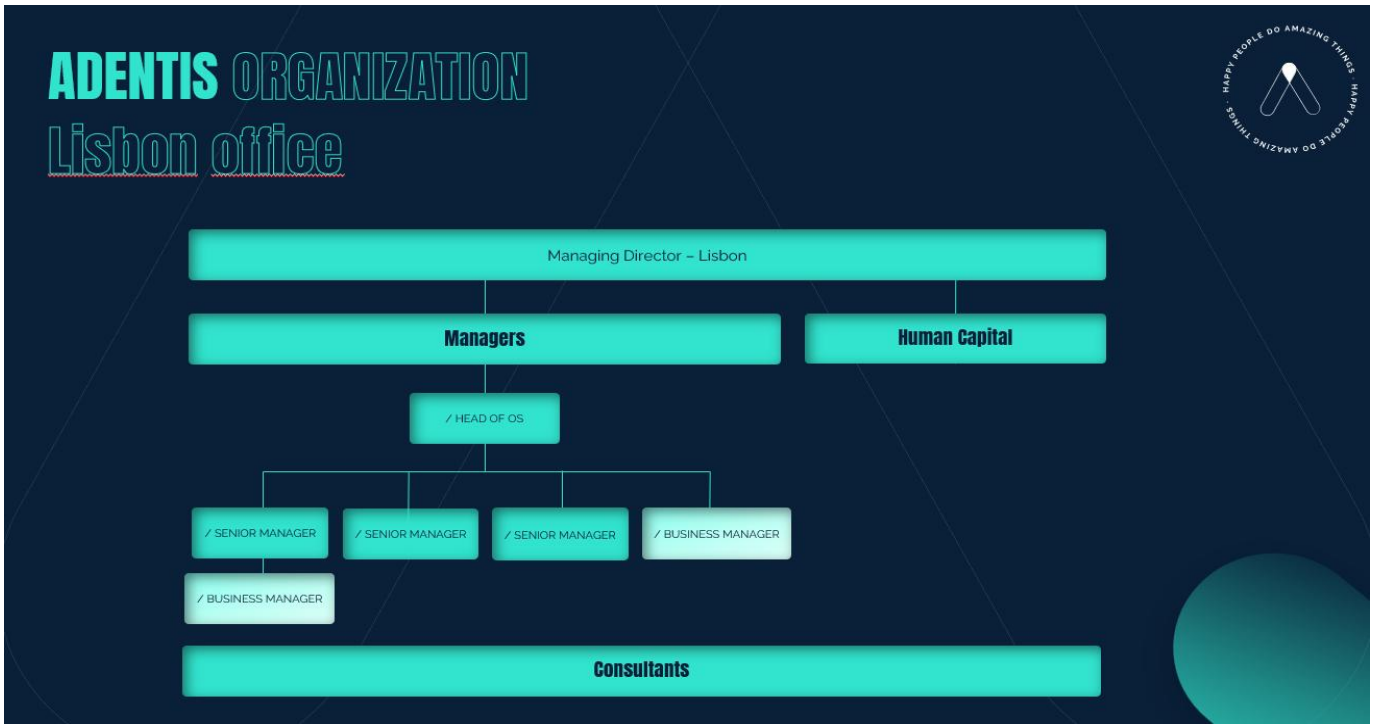
O Managing Director é o Responsável por assegurar a gestão corrente da sociedade respetivamente na área de Lisboa e do Porto, representar a sociedade em juízo e fora dele, determina a equipa e organiza a hierarquia dentro da Empresa. Responsável por assegurar as operações da sociedade, tanto as relativas aos Managers como aos Recursos Humanos.

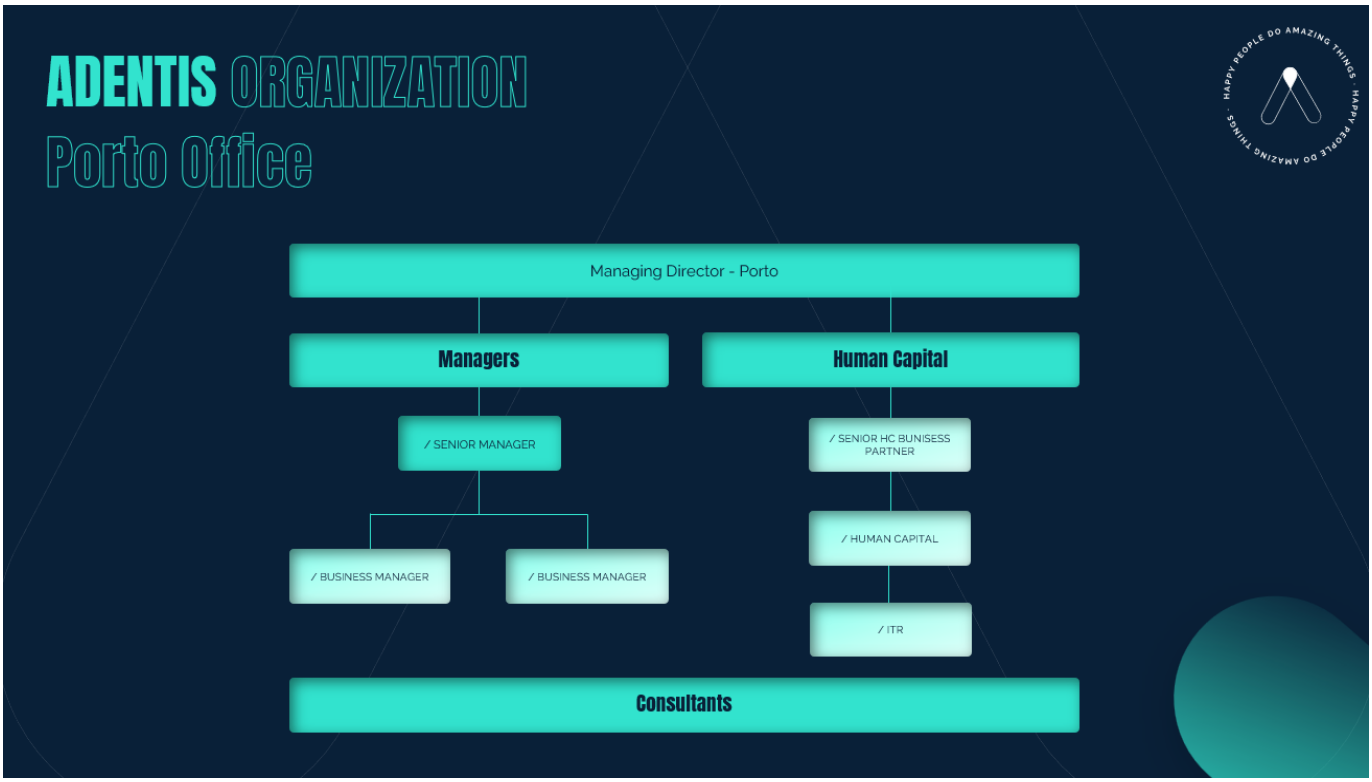
Managers

Responsáveis pelos negócios/angariação de clientes e novos projetos para a Adentis S.A.

- Human Capital

As operações de contratação dos candidatos são geridas por este departamento que está encarregue de todo o processo até à entrada do Consultor.


ADENTIS ORGANIZATION
Lisbon office
Managing Director – Lisbon
Managers
Human Capital
/ HEAD OF OS
/ SENIOR MANAGER
/ SENIOR MANAGER
/ SENIOR MANAGER
/ BUSINESS MANAGER
/ BUSINESS MANAGER
Consultants


ADENTIS ORGANIZATION
Porto Office
Managing Director - Porto
Managers
Human Capital
/ SENIOR MANAGER
/ SENIOR HC BUNISESS PARTNER
/ HUMAN CAPITAL
/ BUSINESS MANAGER
/ BUSINESS MANAGER
/ ITR
Consultants

1.3.6. CodeWin

- **Executive Director**

O Executive Director é o Responsável por assegurar a gestão corrente da sociedade, representar a sociedade em juízo e fora dele, determina a equipa e organiza a hierarquia dentro da Empresa.

- **Business Development Director**

Além de responsáveis pelos negócios/angariação de clientes e novos projetos, são também responsáveis pelo acompanhamento de managers.

- **Managers**

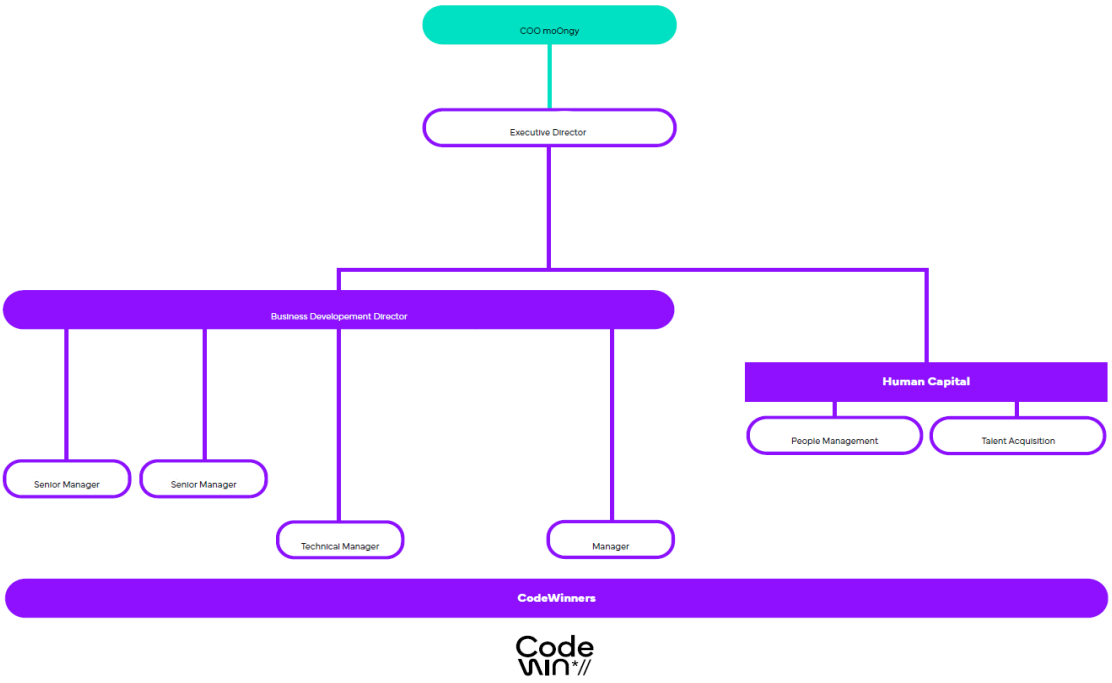
Responsáveis pelos negócios/angariação de clientes e novos projetos

- **IT Recruiter**

Responsáveis pelo recrutamento na Decode as operações de contratação dos candidatos são geridas por este departamento que está encarregue de todo o processo até à entrada do Consultor.

- **Human Capital**

A Gestão de Carreira do Consultor também está alocada a este departamento, com contactos de proximidade com o consultor.



1.3.7. Team IT

- CEO

O Team CEO é o Responsável máximo por assegurar a gestão de topo da sociedade, representar a sociedade em juízo e fora dele, estabelecer a organização da empresa e suas normas de funcionamento. É também o Responsável por assegurar a gestão operacional corrente da sociedade, representar a sociedade em juízo e fora dele, determina a equipa e organiza a hierarquia dentro da Team.

- COO

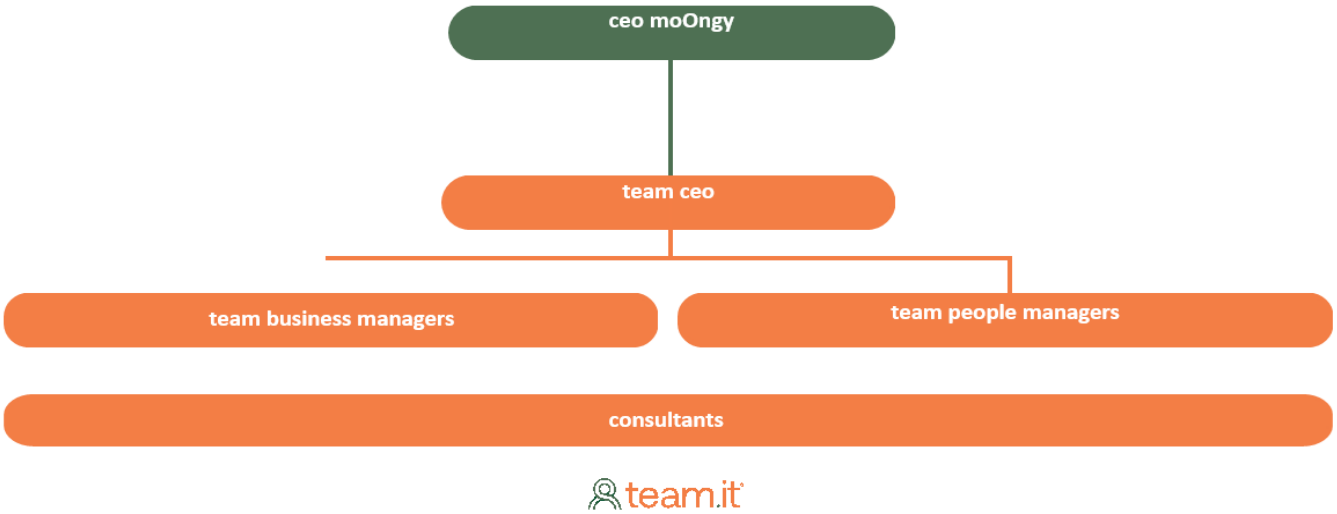
O Team COO é o Responsável por assegurar a gestão operacional corrente da sociedade, representar a sociedade em juízo e fora dele, determina a equipa e organiza a hierarquia dentro da Team IT.

- Team Business Managers

Responsáveis pela gestão dos managers, negócios/angariação de clientes e novos projetos para a Adentis S.A. Juntamente com um elemento da equipa "Team people managers", um elemento da team business managers é responsável pela gestão das operações dos consultores.

- Team People Managers

As operações de contratação dos candidatos são geridas por este departamento que está encarregue de todo o processo até à entrada do Consultor. Por outro lado, a Gestão de Carreira do Consultor também está alocada a este departamento, com contactos de proximidade com o consultor.



1.3.8. Divisão em Áreas Funcionais

Face à organização aqui elencada, e por forma a promover a eficiência na discriminação denotando que os departamentos entre empresas possuem uma clara concordância, para efeitos de mensuração da corrupção, servindo os propósitos do presente PPR, conseguimos claramente discriminar as diversas áreas entre empresas e integrar em áreas funcionais (uma vez que cada empresa promove áreas que possuem um objetivo social em sentido lato bastante consonante):

Área Funcional	Departamentos
Unidades de Outsourcing	• *Unidades de OS das várias empresas*
Direção	• *C-Level's do Grupo MoOngy;* • *Diretores das várias empresas;*
Unidades de Projetos Fechados	• *Unidades do Grupo MoOngy que realizam serviços Team as a Service*
RH	• *Unidades de RH das várias empresas do Grupo MoOngy;* • *Unidades de Talent das várias empresas do Grupo MoOngy;*
Accounting & Fiscal	• *Área Correspondente*
Finance Control	• *Área Correspondente*
Legal	• *Área Correspondente*
People Management	• *Área Correspondente*
Governance & Compliance	• *Área Correspondente*
Sistemas de Informação[1]	• *CIO* • *ITCS* • *MAD* • *LABs* • *DT*
Unidades Complementares[2]	• *Training;* • *Marketing & Communication;* • *Corporate Social Responsability;*

[1] Das conclusões que retirámos, o CIO insere-se na Direção nos riscos a cargo dessa responsabilidade, douta forma, partilha riscos com esta rubrica, atendendo às funções e responsabilidades que exerce.

[2] Devido a fatores de mitigação do risco, em geral, a questão de pagamentos a fornecedores exigirem o aval de dois elementos da Gestão de Topo, os riscos nesta matéria são transferidos para a Direção, pelo que, os Departamentos aqui contemplados possuem um risco residual que fundamenta a sua agregação numa unidade residual atendendo ao teor Baixo dos riscos detetados.

CAPÍTULO II – CONCEITOS DE ENQUADRAMENTO

2.1. Conceito de Corrupção

O Crime de Corrupção está previsto no Código Penal Português (artigos 372º a 374º), é consensual a conjugação dos seguintes quatro elementos:

1) **Uma ação ou omissão** – Pode ser um ato direto ou a falha em agir quando há um dever de fazê-lo;

2) **A prática de um ato lícito ou ilícito** – O Ato pode ser legal ou ilegal;

3) **A contrapartida de uma vantagem indevida** – Recebimento de algo de valor que não é devido;

4) **Para o próprio ou para terceiro** – A vantagem pode beneficiar diretamente a pessoa em posição de poder ou um terceiro;

De forma sistematizada, o Crime de Corrupção envolve a aceitação de uma vantagem indevida por parte de uma pessoa em posição de poder, em troca da prática de um ato, seja ele lícito ou ilícito.

Por outro lado, este conceito abrange tanto a corrupção ativa (quando o agente oferece/promete a vantagem patrimonial ou não patrimonial devida ou indevida) quanto a corrupção passiva (quando o agente solicita/aceita a vantagem patrimonial ou não patrimonial devida ou indevida), distinguindo-se cada um conforme o ato solicitado/praticado.

Conforme consta dos considerandos da Resolução do Conselho de Ministros nº37/2021 que Aprova a Estratégia Nacional Anticorrupção 2020-2024.

Os crimes de corrupção apresentam -se, essencialmente, com duas configurações: a corrupção ativa e a corrupção passiva, conforme o agente esteja, respetivamente, a oferecer/prometer ou a solicitar/aceitar uma vantagem patrimonial ou não patrimonial indevida, distinguindo -se ainda, cada uma, conforme o ato solicitado ou a praticar seja ou não contrário aos deveres do cargo do funcionário corrompido.

2.2. Conceito de Infrações Conexas

O Conceito de corrupção alcança na sociedade um sentido mais abrangente, abarcando outras condutas igualmente criminalizadas, comportamos essas condutas nas Infrações Conexas, entre outras, a título de elenco exemplificativo:

- recebimento e oferta indevidos de vantagem;

- peculato;
- participação económica em negócio;
- concussão;
- abuso de poder;
- prevaricação;
- tráfico de influência;
- branqueamento ou fraude na obtenção ou desvio de subsídio, subvenção ou crédito;

2.3. Canal de Denúncia

A Lei nº93 / 2021 (RGPDI) que transpõe a Diretiva 2019/1937 (Diretiva *Whistleblowing*), obriga as entidades a criar canais específicos, independentes e anónimos que internamente assegurem, de forma adequada, a receção, o tratamento e o arquivo das comunicações de irregularidades por forma a garantir a prevenção da corrupção. Os responsáveis pela gestão do risco devem garantir a confidencialidade das comunicações recebidas e a proteção dos dados pessoais do denunciante e do suspeito da prática da infração.

Por outro lado, a MoOngy entende a necessidade não só do cumprimento normativo, como reconhece a relevância para a organização da importância que tem a criação de canais que permitam e reforcem o controlo preventivo nesta matéria por um lado, por outro, possam atuar de forma reativa para garantir a eficácia e a ação neste tema.

2.4. Plano de Prevenção de Riscos de Corrupção e Infrações Conexas

Nos termos do artigo 6º, nº1 do RGPC, as entidades têm o dever de implementar um PPR, que possa abranger a sua organização e atividade, incluindo áreas de administração, direção operacionais ou de suporte e que contenha:

a) A identificação, análise e classificação dos riscos e das situações que possam expor a entidade a atos de corrupção e infrações conexas, incluindo aqueles associados ao exercício de funções pelos titulares dos órgãos de administração e direção, considerando a realidade do setor e as áreas geográficas em que a entidade atua;

b) Medidas preventivas e corretivas que permitam reduzir a probabilidade de ocorrência e o impacto dos riscos e situações identificados;

Decorrente do artigo 6º, nº2 do RGPC, devem constar do Plano de Prevenção do Riscos de Corrupção e Infrações Conexas:

a) As áreas de atividade da entidade com risco de prática de atos de corrupção e infrações conexas;

b) A probabilidade de ocorrência e o impacto previsível de cada situação, de forma a permitir a graduação dos riscos;

c) Medidas preventivas e corretivas que permitam reduzir a probabilidade de ocorrência e o impacto dos riscos e situações identificados;

d) Nas situações de risco elevado ou máximo, as medidas de prevenção mais exaustivas, sendo prioritária a respetiva execução;

e) A designação do responsável geral pela execução, controlo e revisão do PPR, que pode ser o responsável pelo cumprimento normativo.

CAPÍTULO III – ABORDAGEM

3.1. Metodologia de gestão e avaliação de risco adotada

Tendo por base a adoção do modelo de Três Linhas de Defesa, as responsabilidades relativas ao desenvolvimento, conceção/desenho, implementação, execução, manutenção e supervisão de um sistema de controlo interno adequado e eficaz encontram-se atribuídas transversalmente pela estrutura organizacional. As três linhas são compostas da seguinte forma:

- *Primeira Linha de Defesa* – Todas as Unidades, com exceção das Funções de Gestão de Riscos, Verificação do Cumprimento e Auditoria Interna, assumem os riscos e são responsáveis pelo ambiente de controlo interno dentro da sua área de responsabilidade (isto é, os riscos são identificados e monitorizados, as ações de mitigação são implementadas e os controlos internos estão implementados e eficazes).

- *Segunda Linha de Defesa* – É composta pela Função de Gestão de Riscos (*Risk Management*) e pela Função de Verificação do Cumprimento (*Compliance*) e providencia as estruturas para gerir os riscos, o desafio independente, a monitorização e o aconselhamento para apoiar a Primeira Linha de Defesa na gestão dos mesmos.

- *Terceira Linha de Defesa* – A Função de Auditoria Interna providencia a avaliação independente e objetiva em relação à adequação e eficácia dos processos de gestão do risco, de controlo interno e de governação

Para a avaliação do nível de risco, recorrendo a uma matriz, pode estabelecer-se uma relação entre a probabilidade e a severidade. Procedeu-se a entrevistas aos departamentos do Grupo MoOngy por forma a proceder-se à devida validação do Risco.

Assente no modelo das três linhas de defesa e na contínua reavaliação de risco residual, este Plano identifica as áreas funcionais potencialmente expostas aos riscos de suborno e corrupção.

A Identificação das áreas tem por base o exercício de avaliação de riscos de suborno e corrupção do Grupo MoOngy o qual sugere as áreas potencialmente mais expostas a este risco a nível global.

3.1.1. Se verificar uma situação adversa ou o dano com consequências negativas para as partes interessadas (Probabilidade)

Para a classificação da probabilidade de ocorrência, adotou-se um critério com base na reincidência (em caso de já ter ocorrido/exposição ao risco de ocorrência) e por outro lado, em função do número de vezes que essas operações são efetuadas por ano.

3.1.2. Importância desses acontecimentos na atividade da organização (Severidade)

Para a classificação da Severidade, recorreu-se ao Impacto do acontecimento na atividade da organização, adotando-se um critério com base no dano reputacional que poderá causar no Grupo MoOngy, por outro lado, no dano financeiro que poderá advir do acontecimento.

3.1.3. Fatores tidos em conta na Avaliação do Risco

Aplicada às situações de risco de corrupção e infrações conexas, na definição dos níveis de probabilidade e severidade de cada atividade, são tidos em conta os seguintes fatores:

I. A idoneidade dos gestores e decisores envolvidos na atividade, com um comprometimento ético e um comportamento rigoroso;

II. O *knowledgement* que o gestor e/ou decisor possui da equipa e segurança relativa à idoneidade e rigor da equipa para o pleno cumprimento das tarefas na respetiva esfera de responsabilidades;

III. A dimensão da equipa/existência da mesma (e impacto da mesma para o negócio);

IV. O nível de exposição ao contacto do departamento com órgãos externos;

V. A conduta dos colaboradores da instituição e a existência de normas e/ou princípios que regulem a sua atuação;

VI. O grau de discricionariedade que o Gestor e respetiva equipa possui para a tomada de decisões;

VII. A qualidade do sistema de gestão, em particular o controlo interno e a sua eficácia, verificável através da:

- ❖ participação de vários intervenientes ao longo do processo de decisão;
- ❖ documentação dos processos, incluindo a tomada de decisão;
- ❖ transparência e rastreabilidade dos processos.

3.1.4. Classificação concreta em função da probabilidade e da severidade aplicada a cada situação

3.1.4.1. Classificação do valor da Probabilidade

Probabilidade	
Rara	Não há registo nem indícios que tenha ocorrido ou que possa ocorrer, poderá ocorrer em vários anos de atividade / não há margem de manobra que possibilite a ação / há medidas preventivas ou corretivas adotadas e são adequadas
Ocasional	Poderá eventualmente ocorrer de forma esporádica (três a cinco anos) / há pouca margem de manobra que possibilite a ação por parte dos colaboradores pode requerer e justificar medidas preventivas adicionais relativamente às que existam
Frequente	Pode ocorrer regularmente, verificável em períodos mensais ou anuais / há bastante margem de manobra para possibilitar a ação por parte dos colaboradores requer medidas corretivas adicionais relativamente às que já existam
Elevada	Possibilidade de ocorrência é regular em períodos diários ou semanais / há total margem de manobra para possibilitar a ação por parte dos colaboradores, requer medidas corretivas adicionais relativamente às que já existam

3.1.4.2. Classificação do valor da Severidade

Severidade	
Insignificante	Impacto financeiro e/ou reputacional pouco significativo ou irrelevante.
Marginal	Impacto financeiro e/ou reputacional pouco significativo com consequências reversíveis no curto prazo.
Considerável	Impacto financeiro e/ou reputacional suportável com consequências reversíveis no curto/médio prazo.
Significativa	Impacto financeiro e/ou reputacional muito significativo, com consequências não reversíveis no curto e médio prazo.

3.1.5. Matriz de Avaliação do Risco

			Risco			
Probabilidade	Elevada	4	4	8	12	16
	Frequente	3	3	6	9	12
	Ocasional	2	2	4	6	8
	Rara	1	1	2	3	4
			1	2	3	4
			Insignificante	Marginal	Considerável	Significativa
			Severidade			

3.1.6. Identificação das Atividades, Riscos e das medidas preventivas e/ou corretivas

As atividades estão organizadas em função dos departamentos, o risco é detetado perante um rol de situações já evidenciadas no tempo (independentemente da existência de controlos de mitigação), possíveis situações que possam ocorrer às quais os agentes identifiquem-se como estando expostos,

situações geradas pela margem de manobra evidenciada pelo Gestor/Departamento, casos reportados para situações análogas dentro do Grupo e noutras organizações externas ao Grupo.

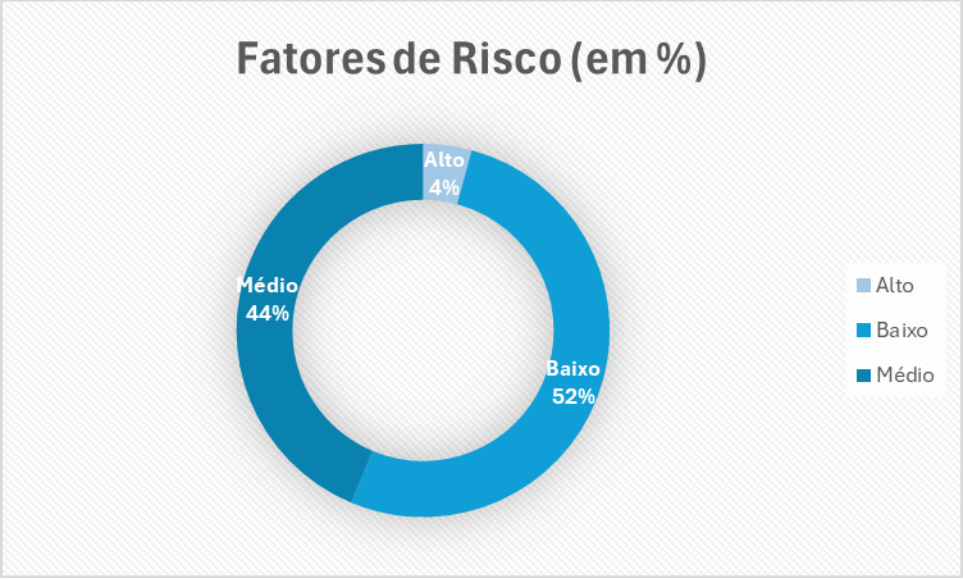
Após as entrevistas, procedeu-se à auscultação de forma informal das perceções externas de pessoas aleatórias conhecedoras da organização e, por fim, analisaram-se os dados recolhidos. Com essa análise pudemos claramente determinar um organigrama funcional onde podemos compactar as diferentes áreas funcionais, baseado nas suas respetivas áreas de atividade e que se coadunem com o risco intrínseco.

3.2. Análise Macro

Num plano geral de Grupo, foram mapeados/detetados 119 fatores de risco dispersos por todo o Grupo MoOngy.

Desse mapa de riscos:

- 5 foram classificados com Grau Alto;
- 52 foram classificados com Grau Médio;
- 62 foram classificados com Grau Baixo;



Os riscos classificados como baixos, foram mitigados ou não são considerados como relevantes a níveis de impacto.

Importa prestar o seguinte contexto: o Grupo MoOngy para qualquer tipo de pagamento exige assinatura de dois elementos da Gestão de Topo[3]. Pelo que, apercebemo-nos que qualquer ato financeiro produzido por qualquer departamento, possui controlos suficientes para garantir um nível digno de mitigar a possibilidade de constituir um risco em qualquer medida do Grupo.

O Risco ao qual há maior perceção de exposição por parte do Grupo é efetivamente o risco de Acesso, Modificação e Eliminação de Dados, constitui-se como o maior desafio e o foco das medidas de mitigação sem prejuízo da necessidade de mitigar prioritariamente os riscos altos.

Os restantes riscos serão monitorizados e reavaliados posteriormente por forma a garantir o correto tratamento dos riscos identificados, deteção de possíveis riscos não identificados no presente PPR e a mitigação destes.

Importa ainda referir que existe um departamento no grupo que serve como "*middle men*" (Ponte Operacional) às operações de outros departamentos financeiros, neste caso, o risco do departamento é totalmente nulo, uma vez que o trabalho produzido por este departamento é validado em toda a sua medida o departamento "*Business Control*" (vide organograma MoOngy).

3.3. Mecanismos de Controlo

A MoOngy planeou e concretizou um Programa de *Compliance* Anticorrupção através da implementação de mecanismos de riscos:

- Estabelecimento de procedimentos e normas que descrevem as diretrizes de integridade/anticorrupção, detalhes dos processos operacionais e respetivos controlos, bem como, os recursos necessários;
- Monitorização e medição (quando aplicável) dos indicadores relativos ao Programa de *Compliance* de Integridade/Anticorrupção;
- Definição e conservação de informações documentadas para garantir que os processos e respetivos controlos são conduzidos conforme planeado e estão de acordo com os requisitos do Programa de *Compliance* de Integridade/Anticorrupção.

Para todos os riscos de corrupção e infrações conexas identificados no contexto da organização e previstos no presente Plano, foram implementadas e são executadas medidas preventivas que permitem reduzir a respetiva probabilidade de ocorrência e o grau de impacto.

Estas medidas distinguem-se entre controlos globais (código, normas, políticas e outros mecanismos transversais) e controlos aplicacionais (processos e procedimentos a nível operacional).

Os controlos globais transversais, isto é, controlos suscetíveis de mitigar qualquer fator de risco de corrupção ou infrações conexas, são enquadrados por um conjunto de documentos (códigos,

[3] *Por razões de Segurança não serão identificados;*

normas, políticas) nos quais estão vertidos os princípios fundamentais a assegurar em matéria de *compliance* associada à integridade.

Na sequência da identificação e implementação de medidas preventivas é avaliado o nível de risco residual do fator, isto é, o risco que persiste após a implementação de controlos com o objetivo de mitigação. Nessa avaliação ponderam-se, por um lado, os atributos desses controlos, assim como a avaliação da eficácia dos mesmos. Se o resultado da última avaliação realizada implicar que algum dos controlos não é adequado/efetivo, estes não serão considerados para efeitos de mitigação de risco e, consequentemente, na avaliação de risco residual, isto é, no risco que persiste após a implementação de controlos com o objetivo de mitigação.

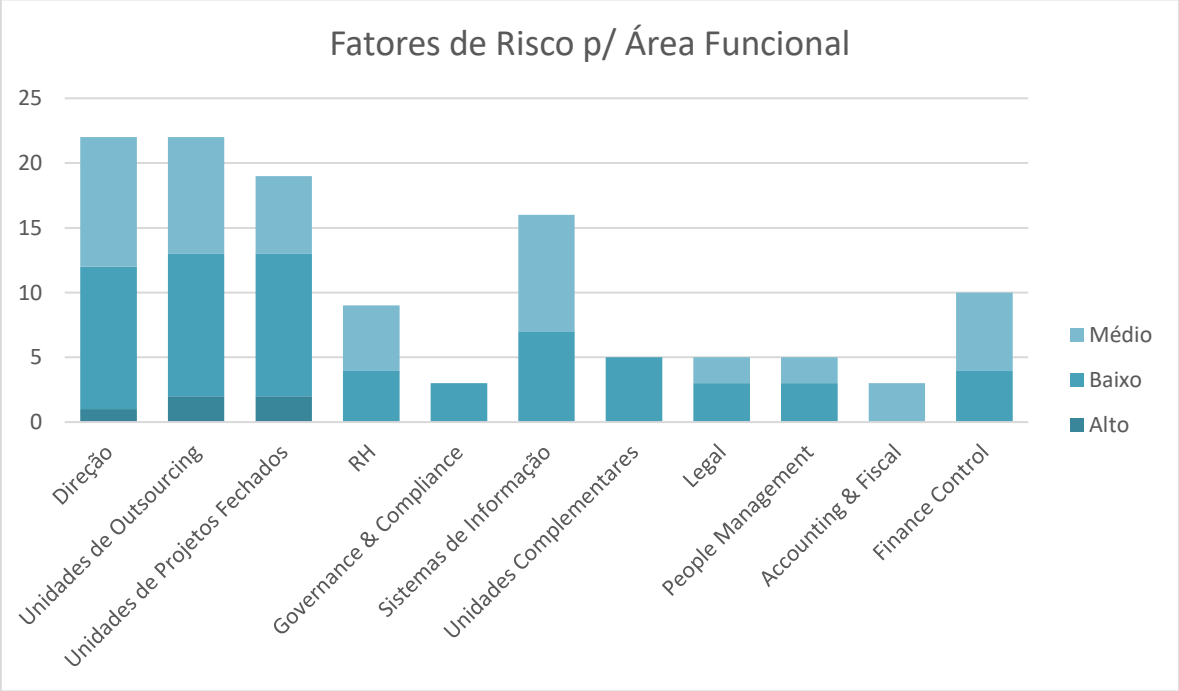
CAPÍTULO IV – GESTÃO DO RISCO

4.1. Identificação e Análise de Riscos

Com base na metodologia descrita no parágrafo anterior, procede-se ao elenco de riscos classificados de acordo com o risco de corrupção apurado através das entrevistas realizadas a todos os departamentos do Grupo MoOngy

A avaliação de aplicabilidade dos riscos e fatores de risco resulta do trabalho de análise ao contexto da organização. No Anexo I encontram-se descritas as áreas de atividade potencialmente expostas, sendo estas classificadas de acordo com o risco de suborno e corrupção apurado, com base na metodologia do Capítulo Anterior.

Dos respetivos concluiu-se que:



Poderemos observar que os riscos mais elevados são tidos pelas áreas funcionais que possuem contacto com Entidades/Pessoas Externas no normal decurso dos seus trabalhos com responsabilidades diretas no negócio/manter relações externas são estas áreas:

- *Direção*
- *Unidades de Outsourcing*

- *Unidades de Projetos Fechados*

Contudo, e da mesma forma, destacamos a área funcional dos Sistemas de Informação que comporta todas as áreas que ostentam todo o *knowledge* da Infraestrutura Tecnológica do Grupo, sendo esse o caso, não é de considerar atípico os níveis de risco estarem quase equiparados aos níveis de risco das áreas funcionais que comportam maior risco que estão necessariamente expostas ao Risco.

4.2. Resultado da Avaliação do Risco

Em resultado do exercício realizado, procedeu-se à identificação das circunstâncias e/ou atividades mais suscetíveis de comportarem riscos de corrupção e infrações conexas. O facto do Grupo já possuir mecanismos financeiros de prevenção e controlo conduz a uma mitigação do risco para "médio" noutros departamentos com maior exposição a riscos (*Direção; Unidade de Outsourcing; Unidade de Projetos Fechado; Sistemas de Informação;*).

A Unidade de Outsourcing, Unidade de Projetos Fechados e Direção, em termos gerais, mantêm-se como áreas de riscos com grau elevado, tendo em consideração o impacto das consequências para as empresas da verificação hipotética dos riscos identificados.

Após análise profunda, notamos também que a área *Business Control* não apresenta qualquer tipo de riscos de corrupção, uma vez que, o departamento e suas ramificações não possuem contacto com as entidades externas e, a sua área funcional é responsável pelas operações de nível intermédio no Grupo MoOngy S.A. que são escrutinados pelos vários departamentos da área financeira.

Por outro lado, cumpre dar expressão às Áreas Funcionais que possuem Grau de Severidade Alta e, como consequência, possuem maior risco reputacional e/ou financeiro em caso de verificação hipotética, ainda que cumpra entender que o grau de probabilidade é no geral classificado como "Raro", sendo os graus probabilísticos mais elevados estarem majoritariamente relacionados a riscos com Dados (*Tráfico de dados; Acesso, Modificação e Eliminação de Dados…*).

Áreas Funcionais	Nº de riscos com Alta Severidade
Unidades de Outsourcing	5
Sistemas de Informação	3
Unidades de Projetos Fechados	2
Direção	2
Legal	2
Accounting & Fiscal	1
RH	1

Cumpre por fim, indicar que os riscos aos quais mais departamentos estão expostos, assim, determina-se como mais suscetíveis de comportar um risco de exposição relativo ao crime de corrupção e infrações conexas através da existência de margem de manobra para que se sucedam:

Acesso, Modificação, Eliminação de dados
Accounting & Fiscal Direção Finance Control People Management RH Sistemas de Informação Unidades de Projeto Fechado
Conflito de Interesses
Direção Governance & Compliance RH Sistemas de Informação Unidades de Outsourcing Unidades de Projetos Fechado
Aquisições Pessoais
Direção Sistemas de Informação Unidades de Outsourcing Unidades de Projeto Fechado
Relacionamento com agentes públicos e/ou pessoas politicamente expostas
Direção RH Unidades de Outsourcing Unidades de Projetos Fechados
Tráfico de Dados
RH Sistemas de Informação Unidades de Outsourcing Unidades de Projetos Fechados

Destes riscos, tornam-se mais preponderantes o risco de "Acesso, Modificação e Eliminação de Dados" e o risco de "Tráfico de Dados" uma vez que possuem em todos os departamentos onde se encontram um grau Médio/Alto.

Estas áreas devem manter-se como áreas identificadas como prioritárias na adoção dos procedimentos preventivos aprovados, bem como quanto à monitorização e controlo dos mesmos até haver um grau de implementação expressivo que permita mitigar a verificação hipotética do presente risco.

Em geral, no caso dos riscos de grau residual apurado resulta do impacto diminuto ou maioritariamente ordinário que a respetiva verificação hipotética poderia conduzir a par de serem departamentos que se preconizam como departamentos de suporte a departamentos

Capítulo V – Plano de Ação

5.1. Medidas de Prevenção, Deteção e Correção de Mitigação do Risco

Área Funcional	Atividades	Riscos	Nível Risco	Medidas preventivas e/ou Corretivas
Unidade de Outsourcing	Angariação de Clientes	Cliente ligado a fins menos lícitos	Médio	*Consulta de Bases de dados relativa às entidades;* *Análise do Projeto a exercer no cliente;* *Canal de Denúncia;*
	Relação Comercial Contratação de Recursos Humanos	Conflito de Interesses	Médio	*Formação;* *Código de Conduta;* *Canal de Denúncia;*
	Faturação de Cliente	Faturar um serviço fictício ou faturar um cliente acima/ abaixo do estabelecido em troca de uma vantagem indevida	Médio	*Princípio dos Quatro Olhos;* *Aprovação do fluxo de Despesas;* *Segregação de funções e necessidade de vários níveis de autorização e decisão;* *Canal de Denúncia;*
	Contratação de colaborador	Favoritismo na contratação em troca de uma vantagem indevida	Médio	*Código de Conduta;* *Formação;* *Awarness;* *Canal de Denúncia;*
	Relação Comercial	Influenciar o resultado do projeto	Alto	*Código de Conduta;* *Formação;* *Awarness;* *Princípio dos Quatro Olhos;* *Canal de Denúncia;* *Proibição de Ajustes Indevidos;* *Cláusulas Anticorrupção;* *Rodízio de Funções;* *Controlo do Cumprimento Contratual;*
	Cumprimento do normativo RGPD	Negligência nos Pedidos de Exercício de Direito	Médio	*Princípio dos Quatro Olhos;* *Privacy by Design;* *Monitorização e envolvimento por parte da Equipa de Compliance;*

	Acesso à informação dos Sistemas	Negligência por parte do departamento. Acesso, desvio, eliminação de dados	Médio	*Princípio dos Quatro Olhos;* *Privacy by Design;* *Backup;* *Registo de Logs;* *Monitorização e envolvimento por parte da Equipa de Compliance;*
	Contratação de Colaborador	Privilegiação de certo candidato devido a benefícios	Médio	*Princípio dos Quatro Olhos;* *Código de Conduta;* *Formação:* *Awarness*
	Relação Comercial	Relacionamento com agentes públicos e/ou pessoas politicamente expostas	Médio	*Código de Conduta;* *Formação;* *Awarness;* *Canal de Denúncia*
	Acesso à informação dos Sistemas	Tráfico de Dados	Alto	*Princípio dos Quatro Olhos;* *Código de Conduta;* *Implementação de Boas Práticas de Segurança;* *Privacy by Design;* *Backup;* *Registo de Logs;* *Canal de Denúncia;* *NDA's;* *Cláusulas Anticorrupção;* *Proibição de Ajustes Indevidos;* *Rodízio de Funções;*
	Relação comercial	Utilização de Informação Privilegiada	Médio	*Código de Conduta;* *Formação;* *Awarness;* *Canal de Denúncia*
Direção	Ratificação por parte da Direção	Aceitação deliberada de documentação falsa e/ou incompleta;	Médio	*Princípio dos Quatro Olhos;* *Canal de Denúncia;* *Código de Conduta;*
	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Médio	*Implementação de Boas Práticas de Segurança;* *NDA's;* *Registo de Log's;* *Backups de Segurança;* *Limitação de Acessos à Informação;* *Privacy by design;*
	Compatibilidade de funções	Acumulação de Funções	Médio	*Código de Conduta;* *Formação;* *Awarness;* *Canal de Denúncia*
	Utilização dos Bens da Organização	Aquisições Pessoais	Médio	*Código de Conduta;* *Formação;* *Awarness;* *Canal de Denúncia* *Princípio dos Quatro Olhos;*

	Titularidade do Poder Decisório	Ato decisório não fundamentado (baseado em pareceres erróneos)	Médio	*Princípio dos Quatro Olhos;* *Análise de Rentabilidade;* *Avaliação mensal de Custos Diretos e Indiretos;* *Revisão do roadmap de investimento;*
	Gestão/Contratação dos Recursos Humanos	Contratação Indevida de colaboradores (com falta de competência técnica)	Médio	*Princípio dos Quatro Olhos;* *Background Check;*
	Representação	Despesas Fictícias	Médio	*Código de Conduta;* *Awarness;* *Aprovação do fluxo de Desoesas;* *Canal de Denúncia;* *Princípio dos Quatro Olhos;* *Políticas de Reembolso*
	Gestão/Contratação dos Recursos Humanos	Empregados Fantasma	Médio	*Princípio dos Quatro Olhos;* *Análise de Rentabilidade;* *Avaliação menal de Custos Diretos e Indiretos;* *Revisão do roadmap de investimento;* *Canal de Denúncia;* *Auditorias;*
	Gestão/Contratação dos Recursos Humanos	Favorecimento de Interesses	Alto	*Código de Conduta;* *Awarness;* *Formação;* *Aprovação do fluxo de Despesas;* *Canal de Denúncia;* *Princípio dos Quatro Olhos;* *Cláusulas Anticorrupção;* *Proibição de Ajustes Indevidos;* *Rodízio de Funções;* *Políticas de Reembolso* *Due Diligence de Fornecedores e Parceiros;* *Gestão de Contratos e Acordos;* *Monitorização de Irregularidades;*
	Relação Comercial	Tráfico de Influências	Médio	*Código de Conduta;* *Awarness;* *Formação;* *Canal de Denúncia;* *Princípio dos Quatro Olhos;* *Consulta de Bases de Dados relativa a entidades;*
	Relação comercial	Uso indevido de informação privilegiada.	Médio	*Código de Conduta;* *Formação;* *Awarness;* *Canal de Denúncia*
Unidade de Projetos Fechados	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Médio	*Implementação de Boas Práticas de Segurança;* *NDA's;* *Registo de Log's;* *Backups de Segurança;* *Limitação de Acessos à Informação;* *Privacy by design;*

	Utilização dos Bens da Organização	Aquisições Pessoais	Médio	*Código de Conduta;* *Formação;* *Awarness;* *Canal de Denúncia* *Princípio dos Quatro Olhos;* *Política de Reembolsos;*
	Relação Comercial	Cliente ligado a fins menos lícitos;	Médio	*Consulta de Bases de dados relativa às entidades;* *Análise do Projeto a exercer no cliente;* *Canal de Denúncia;*
	Acesso à informação dos Sistemas	Quebra do Dever de Sigilo Comercial	Médio	*Princípio dos Quatro Olhos;* *Código de Conduta;* *Implementação de Boas Práticas de Segurança;* *Privacy by Design;* *Backup;* *Registo de Logs;* *Canal de Denúncia;* *NDA's;*
	Acesso à informação dos Sistemas	Tráfico de Dados	Alto	*Princípio dos Quatro Olhos;* *Código de Conduta;* *Implementação de Boas Práticas de Segurança;* *Privacy by Design;* *Backup;* *Registo de Logs;* *Canal de Denúncia;* *NDA's;* *Cláusulas Anticorrupção;* *Proibição de Ajustes Indevidos;* *Rodízio de Funções;* *Due Diligence de Fornecedores e Parceiros;* *Gestão de Contratos e Acordos;* *Monitorização de Irregularidades;*
	Relação Comercial	Tráfico de Influências	Médio	*Código de Conduta;* *Awarness;* *Formação;* *Canal de Denúncia;* *Princípio dos Quatro Olhos;* *Consulta de Bases de Dados relativa a entidades;*

	Acesso à informação dos Sistemas	Utilização Ilícita da Informação	Alto	*Princípio dos Quatro Olhos;* *Código de Conduta;* *Implementação de Boas Práticas de Segurança;* *Privacy by Design;* *Backup;* *Registo de Logs;* *Canal de Denúncia;* *NDA's;* *Pacto de Não concorrência;* *Cláusulas Anticorrupção;* *Proibição de Ajustes Indevidos;* *Rodízio de Funções;*
	Desenvolvimento de Soluções Tecnológicas	Vulnerabilidades das soluções que ponham em causa a disponibilidade, integridade ou confidencialidade da informação	Médio	*Plano de Continuidade de Negócio;* *Implementação de Boas Práticas de Segurança;* *Privacy by Design;* *Backups de Segurança;* *Registo de Log's;* *Utilização de Tecnologias Seguras;*
RH	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Médio	*Implementação de Boas Práticas de Segurança;* *NDA's;* *Registo de Log's;* *Backups de Segurança;* *Limitação de Acessos à Informação;* *Privacy by design;*
	Contratação de Recursos Humanos	Denúncia de algum colaborador ou despoletamento de processos de reavaliação	Médio	*Princípio dos Quatro Olhos;* *Segregação de funções e necessidade de vários níveis de decisão;* *Código de Conduta;* *Formação;* *Background Check;* *Canal de Denúncia*
	Cumprimento do normativo RGPD	Negligência nos Pedidos de Exercício de Direito	Médio	*Princípio dos Quatro Olhos;* *Privacy by Design;* *Monitorização e envolvimento por parte da Equipa de Compliance;*
	Acesso à informação dos Sistemas	Negligência por parte do departamento. Acesso, modificação, eliminação de dados	Médio	*Implementação de Boas Práticas de Segurança;* *NDA's;* *Registo de Log's;* *Backups de Segurança;* *Limitação de Acessos à Informação;* *Privacy by design;*

	Acesso à informação dos Sistemas	Tráfico de Dados	Médio	*Princípio dos Quatro Olhos;* *Código de Conduta;* *Implementação de Boas Práticas de Segurança;* *Privacy by Design;* *Backup;* *Registo de Logs;* *Canal de Denúncia;* *NDA's;*
Accounting & Fiscal	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Médio	*Implementação de Boas Práticas de Segurança;* *NDA's;* *Registo de Log's;* *Backups de Segurança;* *Limitação de Acessos à Informação;* *Privacy by design;*
	Manuseamento de Dados	Utilização indevida de informação confidencial	Médio	*Implementação de Boas Práticas de Segurança;* *NDA's;* *Registo de Log's;* *Backups de Segurança;* *Limitação de Acessos à Informação;* *Código de Conduta;* *Formação;* *Canal de Denúncia;*
	Manuseamento de Dados	Pagamentos indevidos (por erro)	Médio	*Princípio dos Quatro Olhos;* *Auditorias;* *Política de Automação de Pagamentos Correntes;* *Aprovação do fluxo de despesas;* *Existência de relatórios aos stakeholders; sujeitos a escrutínio;* *Políticas de Reembolso;*
Finance Control	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Médio	*Implementação de Boas Práticas de Segurança;* *NDA's;* *Registo de Log's;* *Backups de Segurança;* *Limitação de Acessos à Informação;* *Privacy by design;*
	Processamentos do Tesouro	Erro/omissão no registo de informação	Médio	*Princípio dos Quatro Olhos;* *Auditorias;* *Política de Automação de Pagamentos Correntes;* *Aprovação do fluxo de despesas;* *Existência de relatórios aos stakeholders; sujeitos a escrutínio;*
	Processamentos do Tesouro	Esquema de Reembolso de Despesas	Médio	*Princípio dos Quatro Olhos;* *Auditorias;* *Política de Automação de Pagamentos Correntes;* *Aprovação do fluxo de despesas;* *Existência de relatórios aos stakeholders; sujeitos a escrutínio;* *Políticas de Reembolso;*

	Processamentos do Tesouro	Pagamento de despesa acima do limite autorizado	Médio	*Princípio dos Quatro Olhos;* *Auditorias;* *Segregação de Funções e necessidade de vários níveis de autorização e decisão;* *Política de Automação de Pagamentos Correntes;* *Aprovação do fluxo de despesas;* *Existência de relatórios aos stakeholders; sujeitos a escrutínio;* *Políticas de Reembolso;*
	Processamentos do Tesouro	Pagamento de despesas não elegíveis	Médio	*Princípio dos Quatro Olhos;* *Auditorias;* *Segregação de Funções e necessidade de vários níveis de autorização e decisão;* *Política de Automação de Pagamentos Correntes;* *Aprovação do fluxo de despesas;* *Existência de relatórios aos stakeholders; sujeitos a escrutínio;* *Políticas de Reembolso;*
	Processamentos do Tesouro	Pagamentos indevidos (por erro)	Médio	*Princípio dos Quatro Olhos;* *Auditorias;* *Segregação de Funções e necessidade de vários níveis de autorização e decisão;* *Política de Automação de Pagamentos Correntes;* *Aprovação do fluxo de despesas;* *Existência de relatórios aos stakeholders; sujeitos a escrutínio;* *Políticas de Reembolso;*
Legal	Acompanhamento de processos	Aceitação de benefícios para atribuição de vantagens ao próprio ou a terceiro	Médio	*Segregação de Funções e Necessidade de Vários Níveis de Autorização e Decisão;* *Formação;* *Código de Conduta;* *Canal de Denúncia;*
	Acompanhamento de processos no âmbito de PI	Utilização ou divulgação de informação privilegiada e/ou confidencial em benefício do próprio e/ou de terceiro	Médio	*Código de Conduta;* *Formação;* *Awarness;* *Canal de Denúncia;*
People Management	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Médio	*Implementação de Boas Práticas de Segurança;* *NDA's;* *Registo de Log's;* *Backups de Segurança;* *Limitação de Acessos à Informação;* *Privacy by design;*

	Gestão/Contratação dos Recursos Humanos	Erro no cálculo da prestação (manual/automático) ou a autorização para pagamento	Médio	*Princípio dos Quatro Olhos;* *Auditorias;* *Segregação de Funções e necessidade de vários níveis de autorização e decisão;* *Política de Automação de Pagamentos Correntes;* *Aprovação do fluxo de despesas;* *Existência de relatórios aos stakeholders; sujeitos a escrutínio;*
Sistemas de Informação	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Médio	*Implementação de Boas Práticas de Segurança;* *NDA's;* *Registo de Log's;* *Backups de Segurança;* *Limitação de Acessos à Informação;* *Privacy by design;*
	Cumprimento de normativos	Aplicação incorreta das normas e requisitos legais	Médio	*Princípio dos Quatro Olhos;* *Privacy by Design;* *Registo de Logs;* *Monitorização e envolvimento por parte da Equipa de Compliance;* *Formação;* *Código de Conduta;*
	Contratação de Recursos Humanos	Contratação Indevida de colaboradores (com falta de competência técnica)	Médio	*Princípio dos Quatro Olhos;* *Background Check;*
	Criação e Manutenção de Soluções Tecnológicas Internas	Existência de falhas no processo de validação dos produtos	Médio	*Princípio dos Quatro Olhos;* *Privacy by Design;* *Registo de Logs;* *Monitorização e envolvimento por parte da Equipa de Compliance;* *Documentação de validação de entradas em produção;* *Formação;* *Código de Conduta;*
	Criação e Manutenção de Soluções Tecnológicas Internas	Falha Crítica do Sistema por Erro Humano	Médio	*Implementação de Boas Práticas de Segurança;* *Princípio dos Quatro Olhos;* *Privacy by Design;* *Registo de Logs;* *Monitorização e envolvimento por parte da Equipa de Compliance;* *Formação;* *Código de Conduta;*

	Criação de Soluções Tecnológicas Internas	Falta de Critérios Técnicos (na arquitetura)	Médio	*Implementação de Boas Práticas de Segurança;* *Princípio dos Quatro Olhos;* *Privacy by Design;* *Registo de Logs;* *Monitorização e envolvimento por parte da Equipa de Compliance;* *Formação;* *Código de Conduta;*
	Cumprimento de normativos	Privacy by Design	Médio	*Implementação de Boas Práticas de Segurança;* *Princípio dos Quatro Olhos;* *Privacy by Design;* *Registo de Logs;* *Monitorização e envolvimento por parte da Equipa de Compliance;* *Formação;* *Código de Conduta;*
	Acesso à informação dos Sistemas	Tráfico de Dados	Médio	*Princípio dos Quatro Olhos;* *Código de Conduta;* *Implementação de Boas Práticas de Segurança;* *Privacy by Design;* *Backup;* *Registo de Logs;* *Canal de Denúncia;* *NDA's;*
	Manutenção de Soluções Tecnológicas Internas	Vulnerabilidades e intrusões que ponham em causa a disponibilidade da informação ou a confidencialidade/ integridade da informação	Médio	*Plano de Continuidade de Negócio;* *Implementação de Boas Práticas de Segurança;* *Privacy by Design;* *Backups de Segurança;* *Registo de Log's;* *Utilização de Tecnologias Seguras;*

Os mecanismos preventivos que já se encontram implementados, a par dos diversos mecanismos de *Compliance* numa lógica de melhoria contínua, são efetivamente as Boas Práticas de Segurança, a par disso, foram implementados diversos Controlos de Segurança para mitigar diretamente no Software qualquer tipo de riscos associados a Corrupção envolvendo Dados.

No decurso da elaboração deste PPR, a organização passou por um processo de implementação de Boas Práticas de Segurança, nomeadamente, implementação dos Controlos de Segurança da *ISO/IEC 27001:2022 – Sistema de Gestão da Segurança da Informação* o que permitiu reforçar os controlos técnicos de segurança que possibilitam mitigar alguns dos riscos identificados.

5.2. Controlo e Monitorização do Plano

Pode-se definir um sistema de Controlo interno como um conjunto de ações, estratégias, sistemas, processos, políticas e procedimentos definidos dentro de uma entidade, com o objetivo de garantir:

- O desempenho eficiente e rentável da atividade a médio e longo prazo;
- A existência de informação financeira e de gestão completa, pertinente, fiável e tempestiva;
- O cumprimento das disposições legais e regulamentares aplicáveis.

O Grupo MoOngy tem adotado uma abordagem coordenada na Gestão de Riscos e Controlo Interno. As diretrizes do Sistema de Controlo Interno são estabelecidas a nível do Grupo e com implementação transversal a todas as entidades legais do Grupo. Ademais, são considerados os requisitos e recomendações emanadas pelas autoridades de supervisão.

O Sistema de Controlo Interno, é em conjunto com o Sistema de Gestão de Riscos, é um elemento essencial do processo de governação do Grupo MoOngy, na medida em que engloba o plano de organização, políticas, métodos e procedimentos de controlo que permitem assegurar um ambiente de controlo eficaz e uma gestão sã e prudente das suas atividades.

O Sistema de Controlo Interno do Grupo MoOngy é um processo levado a cabo transversalmente por toda a estrutura organizacional, desde a direção aos colaboradores, com o objetivo de proporcionar um grau de confiança razoável na concretização dos seguintes objetivos:

- Executar as operações de uma forma eficiente e eficaz;
- Possuir e prestar informação, financeira e não financeira, fiável e completa;
- Deter um Sistema de gestão de riscos eficiente;
- Avaliar correta e adequadamente os ativos e responsabilidades;
- Desempenhar prudentemente a atividade;
- Prevenir e detetar as fraudes e erros;
- Cumprir a legislação e regulamentação, assim como as políticas e procedimentos internos.

A documentação dos controlos internos é a base para uma avaliação da sua eficácia. O Sistema de Controlo Interno é eficaz se as atividades de controlo que o compõe forem:

- Desenhadas de forma eficaz, isto é, capazes de prevenir ou detetar perdas, erros ou falhas em tempo oportuno;
- Operacionalmente eficazes, isto é, executadas de acordo com o seu desenho e cuja evidência da sua realização está disponível e é mantida.

O acompanhamento do presente PRR será assegurado através da revisão periódica dos controlos, da implementação e dos registos da execução dos mesmos, mediante a realização de exercícios de avaliação interna.

CAPÍTULO VI – DISPOSIÇÕES FINAIS

6.1. Revisão do Plano

O responsável pela execução, controlo e revisão deste plano é o Departamento de Governance & Compliance (antigo DPG- Departamento de Projetos Globais), são estes os Responsáveis pelo Cumprimento Normativo do Grupo MoOngy.

Não obstante, todas as áreas do Grupo MoOngy S.A. são responsáveis pela adoção das medidas necessárias à operacionalização e cumprimento do Plano, no âmbito da sua área de intervenção. Acresce ainda o dever de comunicação caso alguém suspeite, de boa-fé, que outra pessoa ou área fora do seu âmbito de intervenção está a incumprir o determinado neste Plano.

Importa, ainda, mencionar que o PPR é revisto a cada três anos ou sempre que se opere uma alteração nas atribuições ou na estrutura orgânica ou societária da MoOngy, que justifique a sua revisão.

Adicionalmente, a execução do PPR está sujeita a controlo, efetuado nos seguintes termos:

a. Elaboração, no mês de outubro, de relatório de avaliação intercalar nas situações identificadas de risco elevado ou máximo;

b. Elaboração, no mês de abril do ano seguinte a que respeita a execução, de relatório de avaliação anual, contendo nomeadamente o estado de evolução das medidas preventivas e corretivas identificadas, bem como os resultados da monitorização da sua efetiva operacionalização.

6.2. Aprovação e Divulgação

O PPR do Grupo MoOngy, conforme dispõe o n.º 6 do artigo 6.º do diploma legal anteriormente mencionado, será disponibilizado, no prazo de 10 dias contados desde a sua implementação e respetivas revisões ou elaboração, na Intranet das Empresas do Grupo, bem como na sua página oficial da internet. Além do PPR, serão, também, disponibilizados, através dos mesmos meios, o relatório de avaliação intercalar e o relatório de avaliação anual.

O presente Plano de Prevenção de Riscos de Corrupção e Infrações Conexas e as suas sucessivas revisões são aprovados pela Gestão de Topo, por proposta do Responsável e Elementos do Departamento de Governance & Compliance.

ANEXO I – MATRIZ DE RISCOS DO GRUPO MOONGY

(Tabela revista para atualização das áreas funcionais a: 27/01/2025)

IDENTIFICAÇÃO DO RISCO				ANÁLISE DO RISCO		
#	Área Funcional	Atividades	Riscos	Probabilidade	Severidade	Nível Risco
1	Unidade de Outsourcing	Relação Comercial	Aceitação indevida de ofertas	Rara	Insignificante	*Baixo*
2	Unidade de Outsourcing	Utilização dos Bens da Organização	Aquisições Pessoais	Rara	Considerável	*Baixo*
3	Unidade de Outsourcing	Angariação de Clientes	Cliente ligado a fins menos lícitos;	Ocasional	Considerável	*Médio*
4	Unidade de Outsourcing	Relação Comercial Contratação de Recursos Humanos	Conflito de Interesses	Ocasional	Marginal	*Médio*
5	Unidade de Outsourcing	Relação Comercial	Despesas Fictícias	Rara	Insignificante	*Baixo*
6	Unidade de Outsourcing	Faturação de Cliente	Faturar um serviço fictício ou faturar um cliente acima/ abaixo do estabelecido em troca de uma vantagem indevida	Rara	Significativa	*Médio*
7	Unidade de Outsourcing	Acompanhamento do Consultor	Favorecimento de colaboradores (conflitos de interesses)	Rara	Insignificante	*Baixo*
8	Unidade de Outsourcing	Contratação de colaborador	Favoritismo na contratação em troca de uma vantagem indevida	Ocasional	Marginal	*Médio*
9	Unidade de Outsourcing	Relação Comercial	Gratificações ilegais	Rara	Marginal	*Baixo*
10	Unidade de Outsourcing	Relação Comercial	Influenciar o resultado do projeto	Frequente	Significativa	*Alto*
11	Unidade de Outsourcing	Cumprimento do normativo RGPD	Negligência nos Pedidos de Exercício de Direito	Ocasional	Significativa	*Médio*
12	Unidade de Outsourcing	Acesso à informação dos Sistemas	Negligência por parte do departamento. Acesso, desvio, eliminação de dados	Ocasional	Marginal	*Médio*
13	Unidade de Outsourcing	Relação Comercial	Oferta de Benefícios/Presentes para adjudicação de um contrato/mercado	Rara	Insignificante	*Baixo*
14	Unidade de Outsourcing	Participação económica em negócio	Pagamentos inadequados através de intermediários	Rara	Considerável	*Baixo*
15	Unidade de Outsourcing	Relação Comercial	Presentes ou pagamentos inapropriados relacionados com a adjudicação de um contrato/mercado	Rara	Considerável	*Baixo*
16	Unidade de Outsourcing	Contratação de Colaborador	Privilegiação de certo candidato devido a benefícios	Ocasional	Considerável	*Médio*
17	Unidade de Outsourcing	Relação Comercial	Relacionamento com agentes públicos e/ou pessoas politicamente expostas	Rara	Significativa	*Médio*
18	Unidade de Outsourcing	Relação Comercial	Subornos a clientes	Rara	Considerável	*Baixo*
19	Unidade de Outsourcing	Relação Comercial	Subsídios ilícitos, patrocínio e doações para obter um contrato/mercado	Rara	Considerável	*Baixo*
20	Unidade de Outsourcing	Acesso à informação dos Sistemas	Tráfico de Dados	Frequente	Significativa	*Alto*
21	Unidade de Outsourcing	Relação Comercial	Tráfico de Influências	Rara	Considerável	*Baixo*
22	Unidade de Outsourcing	Relação comercial	Utilização de Informação Privilegiada	Ocasional	Marginal	*Médio*

23	Direção	Seleção de Fornecedores	Aceitação de benefícios para atribuição a fornecedores	Rara	Marginal	*Baixo*
24	Direção	Ratificação por parte da Direção	Aceitação deliberada de documentação falsa e/ou incompleta;	Frequente	Considerável	*Médio*
25	Direção	Relação comercial	Aceitação indevida de ofertas	Rara	Considerável	*Baixo*
26	Direção	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Ocasional	Considerável	*Médio*
27	Direção	Compatibilidade de funções	Acumulação de Funções	Ocasional	Marginal	*Médio*
28	Direção	Utilização dos Bens da Organização	Aquisições Pessoais	Rara	Significativa	*Médio*
29	Direção	Titularidade do Poder Decisório	Ato decisório não fundamentado (baseado em pareceres erróneos)	Frequente	Considerável	*Médio*
30	Direção	Titularidade do Poder Decisório	Conflito de Interesses	Rara	Marginal	*Baixo*
31	Direção	Gestão/Contratação dos Recursos Humanos	Contratação Indevida de colaboradores (com falta de competência técnica)	Ocasional	Marginal	*Médio*
32	Direção	Representação	Despesas Fictícias	Frequente	Considerável	*Médio*
33	Direção	Gestão Patrimonial	Desvio de dinheiro ou valores;	Rara	Insignificante	*Baixo*
34	Direção	Gestão/Contratação dos Recursos Humanos	Empregados Fantasma	Frequente	Considerável	*Médio*
35	Direção	Governação	Enriquecimento Ilícito	Rara	Considerável	*Baixo*
36	Direção	Ratificação por parte da Direção	Falsificação de Documentação	Rara	Considerável	*Baixo*
37	Direção	Contratação de Recursos Humanos	Favorecimento (violação dos deveres de isenção, independência, transparência, imparcialidade e confidencialidade)	Rara	Considerável	*Baixo*
38	Direção	Gestão/Contratação dos Recursos Humanos	Favorecimento de Interesses	Elevada	Significativa	*Alto*
39	Direção	Titularidade do Poder Decisório	Patrocínio de Entidades em Conflito	Rara	Marginal	*Baixo*
40	Direção	Representação Institucional	Relacionamento com agentes públicos e/ou pessoas politicamente expostas	Rara	Considerável	*Baixo*
41	Direção	Relação Comercial	Relações de negócios com pessoas singulares/coletivas de países com elevado índice de corrupção	Rara	Considerável	*Baixo*
42	Direção	Relação Comercial	Tráfico de Influências	Ocasional	Marginal	*Médio*
43	Direção	Relação comercial	Uso indevido de informação privilegiada.	Ocasional	Marginal	*Médio*
44	Direção	Utilização dos Bens da Organização	Utilização de bens da empresa para fins duvidosos	Rara	Insignificante	*Baixo*
45	Unidade de Projetos Fechados	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Frequente	Considerável	*Médio*
46	Unidade de Projetos Fechados	Utilização dos Bens da Organização	Aquisições Pessoais	Ocasional	Significativa	*Médio*
47	Unidade de Projetos Fechados	Relação Comercial	Cliente ligado a fins menos lícitos;	Ocasional	Marginal	*Médio*
48	Unidade de Projetos Fechados	Contratação de Recursos Humanos	Conflito de Interesses	Ocasional	Insignificante	*Baixo*
49	Unidade de Projetos Fechados	Relação Comercial	Despesas Fictícias	Rara	Insignificante	*Baixo*

50	Unidade de Projetos Fechados	Relação Comercial	Dolo para Influenciar a decisão do cliente para aceitar proposta comercial	Rara	Marginal	*Baixo*
51	Unidade de Projetos Fechados	Faturação de Cliente	Faturar um serviço fictício ou faturar um cliente acima/ abaixo do estabelecido em troca de uma vantagem indevida	Rara	Considerável	*Baixo*
52	Unidade de Projetos Fechados	Contratação de Recursos Humanos	Favorecimento de candidatos (conflitos de interesses)	Rara	Insignificante	*Baixo*
53	Unidade de Projetos Fechados	Relação Comercial	Gratificações ilegais	Rara	Insignificante	*Baixo*
54	Unidade de Projetos Fechados	Relação Comercial	Influenciar o resultado do projeto	Rara	Marginal	*Baixo*
55	Unidade de Projetos Fechados	Participação em Concursos Públicos	Lobbying no contexto de um concurso (cliente público)	Rara	Marginal	*Baixo*
56	Unidade de Projetos Fechados	Desenvolvimento de Soluções Tecnológicas	Manipulação de código-fonte do cliente	Rara	Considerável	*Baixo*
57	Unidade de Projetos Fechados	Relação Comercial	Presentes ou pagamentos inapropriados relacionados com a adjudicação de um contrato/mercado	Rara	Marginal	*Baixo*
58	Unidade de Projetos Fechados	Acesso à informação dos Sistemas	Quebra do Dever de Sigilo Comercial	Frequente	Considerável	*Médio*
59	Unidade de Projetos Fechados	Relação Comercial	Relacionamento com agentes públicos e/ou pessoas politicamente expostas	Rara	Insignificante	*Baixo*
60	Unidade de Projetos Fechados	Acesso à informação dos Sistemas	Tráfico de Dados	Elevada	Considerável	*Alto*
61	Unidade de Projetos Fechados	Relação Comercial	Tráfico de Influências	Frequente	Marginal	*Médio*
62	Unidade de Projetos Fechados	Acesso à informação dos Sistemas	Utilização Ilícita da Informação	Elevada	Significativa	*Alto*
63	Unidade de Projetos Fechados	Desenvolvimento de Soluções Tecnológicas	Vulnerabilidades das soluções que ponham em causa a disponibilidade, integridade ou confidencialidade da informação	Frequente	Marginal	*Médio*
64	RH	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Ocasional	Considerável	*Médio*
65	RH	Contratação de Recursos Humanos	Denúncia de algum colaborador ou despoletamento de processos de reavaliação	Frequente	Marginal	*Médio*
66	RH	Contratação de Recursos Humanos Acompanhamento do Consultor	Conflito de Interesses	Rara	Marginal	*Baixo*
67	RH	Gestão/Contratação dos Recursos Humanos	Favorecimento de Interesses	Rara	Marginal	*Baixo*
68	RH	Contratação de Recursos Humanos	Favoritismo na contratação em troca de uma vantagem indevida	Rara	Considerável	*Baixo*
69	RH	Cumprimento do normativo RGPD	Negligência nos Pedidos de Exercício de Direito	Rara	Significativa	*Médio*
70	RH	Acesso à informação dos Sistemas	Negligência por parte do departamento. Acesso, modificação, eliminação de dados	Ocasional	Considerável	*Médio*
71	RH	Realização de atividades com as Faculdades	Relacionamento com agentes públicos e/ou pessoas politicamente expostas	Rara	Marginal	*Baixo*
72	RH	Acesso à informação dos Sistemas	Tráfico de Dados	Elevada	Marginal	*Médio*
73	Accounting & Fiscal	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Ocasional	Marginal	*Médio*
74	Accounting & Fiscal	Manuseamento de Dados	Utilização indevida de informação confidencial	Rara	Significativa	*Médio*

75	Accounting & Fiscal	Manuseamento de Dados	Pagamentos indevidos (por erro)	Ocasional	Marginal	*Médio*
76	Finance Control	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Frequente	Considerável	*Médio*
77	Finance Control	Processamentos do Tesouro	Despesas falsamente atribuídas	Rara	Considerável	*Baixo*
78	Finance Control	Processamentos do Tesouro	Erro/omissão no registo de informação	Ocasional	Marginal	*Médio*
79	Finance Control	Processamentos do Tesouro	Esquema de Reembolso de Despesas	Ocasional	Considerável	*Médio*
80	Finance Control	Processamentos do Tesouro	Falta de Justificação de Saída da Caixa	Rara	Insignificante	*Baixo*
81	Finance Control	Processamentos do Tesouro	Inserção de movimentos fictícios	Rara	Considerável	*Baixo*
82	Finance Control	Processamentos do Tesouro	Omissão de informação relevante;	Rara	Considerável	*Baixo*
83	Finance Control	Processamentos do Tesouro	Pagamento de despesa acima do limite autorizado	Ocasional	Marginal	*Médio*
84	Finance Control	Processamentos do Tesouro	Pagamento de despesas não elegíveis	Ocasional	Considerável	*Médio*
85	Finance Control	Processamentos do Tesouro	Pagamentos indevidos (por erro)	Ocasional	Marginal	*Médio*
86	Legal	Acompanhamento de processos	Aceitação de benefícios para atribuição de vantagens ao próprio ou a terceiro	Rara	Significativa	*Médio*
87	Legal	Apoio Jurídico	Elaboração de pareceres erróneos	Rara	Considerável	*Baixo*
88	Legal	Apoio Jurídico	Favorecimento (violação dos deveres de isenção, independência, transparência, imparcialidade e confidencialidade)	Rara	Considerável	*Baixo*
89	Legal	Seleção de Assessorias	Negociação/Contratação de entidades terceiras privadas	Rara	Marginal	*Baixo*
90	Legal	Acompanhamento de processos no âmbito de PI	Utilização ou divulgação de informação privilegiada e/ou confidencial em benefício do próprio e/ou de terceiro	Rara	Significativa	*Médio*
91	People Management	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Ocasional	Considerável	*Médio*
92	People Management	Gestão/Contratação dos Recursos Humanos	Aplicação incorreta das normas e requisitos legais	Rara	Marginal	*Baixo*
93	People Management	Gestão/Contratação dos Recursos Humanos	Erro no cálculo da prestação (manual/automático) ou a autorização para pagamento	Ocasional	Considerável	*Médio*
94	People Management	Gestão/Contratação dos Recursos Humanos	Falta de transparência nos procedimentos	Rara	Marginal	*Baixo*
95	People Management	Gestão/Contratação dos Recursos Humanos	Prática de ato por quem não detém competência para o mesmo	Rara	Marginal	*Baixo*
96	Governance & Compliance	Cumprimento de normativos	Análise inadequada do âmbito Contratual de Segurança de Informação	Rara	Considerável	*Baixo*
97	Governance & Compliance	Cumprimento de normativos	Aplicação incorreta das normas e requisitos legais	Rara	Considerável	*Baixo*
98	Governance & Compliance	Para todas as atividades desenvolvidas pelo Departamento	Conflito de Interesses	Rara	Insignificante	*Baixo*
99	Sistemas de Informação	Seleção de Fornecedores	Aceitação indevida de ofertas	Rara	Considerável	*Baixo*

100	Sistemas de Informação	Acesso à informação dos Sistemas	Acesso, Modificação, Eliminação de dados	Rara	Significativa	*Médio*
101	Sistemas de Informação	Cumprimento de normativos	Aplicação incorreta das normas e requisitos legais	Ocasional	Considerável	*Médio*
102	Sistemas de Informação	Gestão dos Equipamentos da Organização	Aquisições Pessoais	Rara	Marginal	*Baixo*
103	Sistemas de Informação	Contratação de Recursos Humanos	Conflito de Interesses	Rara	Insignificante	*Baixo*
104	Sistemas de Informação	Contratação de Recursos Humanos	Contratação Indevida de colaboradores (com falta de competência técnica)	Ocasional	Considerável	*Médio*
105	Sistemas de Informação	Criação e Manutenção de Soluções Tecnológicas Internas	Existência de falhas no processo de validação dos produtos	Ocasional	Marginal	*Médio*
106	Sistemas de Informação	Criação e Manutenção de Soluções Tecnológicas Internas	Falha Crítica do Sistema por Erro Humano	Ocasional	Marginal	*Médio*
107	Sistemas de Informação	Criação de Soluções Tecnológicas Internas	Falta de Critérios Técnicos (na arquitetura)	Ocasional	Marginal	*Médio*
108	Sistemas de Informação	Utilização dos Bens da Organização	Gestão de bens materiais designadamente de equipamentos informáticos	Rara	Insignificante	*Baixo*
109	Sistemas de Informação	Manutenção de Soluções Tecnológicas Internas	Integração de Dados Fictícios;	Rara	Marginal	*Baixo*
110	Sistemas de Informação	Acesso à informação dos Sistemas	Omissão/manipulação/adulteração de informação com o objetivo de condicionar as decisões	Rara	Considerável	*Baixo*
111	Sistemas de Informação	Cumprimento de normativos	Privacy by Design	Ocasional	Marginal	*Médio*
112	Sistemas de Informação	Angariação de Investigadores	Privilegiação de certo candidato devido a conflito de interesses	Rara	Marginal	*Baixo*
113	Sistemas de Informação	Acesso à informação dos Sistemas	Tráfico de Dados	Ocasional	Significativa	*Médio*
114	Sistemas de Informação	Manutenção de Soluções Tecnológicas Internas	Vulnerabilidades e intrusões que ponham em causa a disponibilidade da informação ou a confidencialidade/ integridade da informação	Rara	Significativa	*Médio*
115	Unidades Complementares	Seleção de Fornecedores	Aceitação de benefícios para atribuição a formadores	Rara	Insignificante	*Baixo*
116	Unidades Complementares	Seleção de Fornecedores	Aceitação de benefícios para atribuição a fornecedores	Rara	Marginal	*Baixo*
117	Unidades Complementares	Vigilância de Exames da Pearson Vue	Facilitação nos Exames (vigilância menos atenta)	Rara	Marginal	*Baixo*
118	Unidades Complementares	Ofertas de formações	Formando - Falta de isenção e/ou imparcialidade técnica ou benefício em detrimento de interesses alheios	Rara	Insignificante	*Baixo*
119	Unidades Complementares	Acesso à informação dos Sistemas	Omissão/manipulação/adulteração de informação com o objetivo de condicionar as decisões	Rara	Insignificante	*Baixo*