ética



Plano de Prevenção de Riscos de Corrupção e Infrações Conexas

Outubro 2026

Metropolitano de Lisboa

Índice

I. Introdução 6
II. Empresa 7
1. Metropolitano de Lisboa 7
2. Metrocom 9
3. Outras empresas participadas 10
III. Metodologia adotada para a identificação e classificação de riscos e medidas de mitigação 11
IV. Acompanhamento da execução do Plano 14
V. Aprovação, divulgação e comunicação 15
VI. Anexos 16
Anexo 1 – Identificação e classificação dos riscos e medidas de mitigação 16
Anexo 2 – Matriz de risco 37
Anexo 3 – Corrupção e Infrações conexas no RGPC 39

GLOSSÁRIO E SIGLAS

A	
ACFE	*Association of Certified Fraud Examiners*
AE	Acordo de Empresa
AMT	Autoridade da Mobilidade e dos Transportes
ASE	Autoridade de Segurança da Exploração
AT	Agente de Tráfego
C	
CA	Conselho de Administração
CAI	Centro de Apoio Interno
CEC	Código de Ética e de Conduta
CF	Conselho Fiscal
CNCS	Centro Nacional de Cibersegurança
CPC	Conselho de Prevenção da Corrupção
D	
DCL	Direção de Clientes, Comercial e Receita
DCM	Direção de Comunicação, Marca e *Marketing*
DE	Direção de Coordenação de Exploração
DEI	Direção de Infraestrutura
DEO	Direção de Operação
DFI	Direção Financeira
DI	Direção de Coordenação de Novos Investimentos
DIC	EM Direção da Linha Circular
DIG	Direção de Informação de Gestão e Performance
DIL	EM Direção da Linha Violeta
DISR	Direção de Inovação, Sustentabilidade e Gestão de Risco
DIV	EM Direção da Linha Vermelha
DJC	Direção Jurídica e de *Compliance*
DL	Decreto-Lei
DLCP	Direção de Logística, Compras e Património
DMC	Direção de Manutenção de Material Circulante
DPT	Direção de Pessoas e Talento
DSF	Direção de Segurança, Vigilância e Fiscalização

DTI	Direção de Tecnologias de Informação
E	
EMV	Europay, Mastercard e Visa
EOA	Estatuto da Ordem dos Advogados
EPD	Encarregado de Proteção de Dados
F	
FC	Ferconsult, S.A.
FU	Fiscal Único
G	
GAI	Gabinete de Auditoria Interna
GSG	Secretaria-Geral
I	
IGF	Inspeção Geral de Finanças
IHT	Isenção de horário de trabalho
IMT	Instituto da Mobilidade e dos Transportes
IT	Instrução de Trabalho
O	
OC	Operador Comercial
M	
MAVT	Máquina Automática de Venda de Títulos
MB	Multibanco
MC	Metrocom, S.A.
MENAC	Mecanismo Nacional Anticorrupção
ML	Metropolitano de Lisboa, E.P.E.
MSAVT	Máquina Semi-Automática de Venda de Títulos
P	
PCN	Programa de Cumprimento Normativo
POGSE	Plano de Organização e Gestão de Segurança da Empresa
PMO	Parque de Material e Oficinas do ML
PPR	Plano de Prevenção de Riscos de Corrupção e Infrações Conexas
PSI	Política de Segurança da Informação
PSP	Polícia de Segurança Pública
R	
RCN	Responsável pelo Cumprimento Normativo

RGPC	Regime Geral de Prevenção da Corrupção
RGPD	Regulamento Geral sobre a Proteção de Dados
RGPDI	Regime Geral de Proteção de Denunciantes de Infrações
RJC	Regime Jurídico da Cibersegurança
ROC	Revisores Oficiais de Contas
S	
SAP	Sistema de informação do ML
SGQA	Sistema de Gestão da Qualidade e Ambiente
SGR	Sistema de Gestão de Risco
T	
TdC	Tribunal de Contas
TI	Tecnologia de Informação
TO	Tecnologia de Operação

I. Introdução

O presente Plano identifica e avalia os riscos de corrupção e infrações conexas associados às atividades do Metropolitano de Lisboa, E.P.E. (ML) e das empresas participadas abrangidas, descreve as medidas de mitigação existentes e define as medidas adicionais a implementar. A avaliação evidencia especial exposição nos domínios da contratação, da gestão contratual e dos processos decisórios, para os quais são previstos controlos reforçados. A implementação do Plano é acompanhada através de avaliações intercalares e anuais, com reporte aos órgãos competentes e atualização das medidas em função dos resultados obtidos.

O Metropolitano de Lisboa E.P.E. (ML), enquanto Empresa Pública, elaborou e apresentou o seu primeiro Plano de Prevenção de Riscos de Corrupção e Infrações Conexas (PPR) em dezembro de 2009. Desde então, tem procedido a diversas atualizações ao longo dos anos, permitindo uma monitorização atenta dos respetivos riscos.

Em 9 de dezembro de 2021, foi publicado o DL n.º 109-E/2021, que criou o Mecanismo Nacional Anticorrupção (MENAC) e estabeleceu o Regime Geral de Prevenção da Corrupção (RGPC), que se encontra alinhado com várias disposições da Convenção das Nações Unidas contra a Corrupção.

O RGPC reforçou as obrigações aplicáveis ao ML enquanto empresa pública. A Metrocom – Exploração de Espaços Comerciais, S.A. (MC) e a Ferconsult – Consultoria, Estudos e Projetos de Engenharia de Transportes, S.A. (FC), participadas a 100% pelo ML, têm menos de 50 trabalhadores e não se encontram autonomamente abrangidas pelo RGPC. Ainda assim, adotam instrumentos de prevenção de riscos de corrupção e infrações conexas adequados à sua dimensão e natureza e beneficiam, na medida aplicável, dos mecanismos implementados pelo ML.

Por força deste regime, o ML dispõe de um Programa de Cumprimento Normativo (PCN), acompanhado pelo responsável pelo cumprimento normativo (RCN) designado pela Empresa. O PCN integra o presente Plano e os respetivos relatórios de avaliação intercalar e anual, o Código de Ética e de Conduta, o canal de comunicação de denúncias (denominado Canal de Ética) e o plano de formação e comunicação em Ética Empresarial. Estes instrumentos são extensíveis às empresas participadas com maioria de capital na medida em que lhes sejam aplicáveis.

Neste contexto, e em cumprimento do RGPC e do Guia n.º 1/2023 do MENAC, o presente documento atualiza o PPR aplicável ao ML e às empresas participadas com maioria de capital, com especial incidência na MC. A atualização revê a identificação e a classificação dos riscos, sistematiza as medidas de mitigação adotadas e define as medidas adicionais a implementar.

II. Empresa

O ML é uma Entidade Pública Empresarial com personalidade jurídica, dotada de autonomia administrativa, financeira e patrimonial, regendo-se por estatutos próprios[1] e pela lei aplicável às empresas públicas. A instalação e exploração, em regime de exclusivo, de um sistema de transporte coletivo subterrâneo na cidade de Lisboa, encontra-se prevista no contrato de concessão celebrado com o Estado Português.

Como referido, o ML detém a totalidade do capital social da MC e da FC.

A MC é uma empresa pública, com a natureza de S.A., igualmente dotada de personalidade jurídica, autonomia administrativa, financeira e patrimonial, regendo-se por estatutos próprios e a sua atividade de exploração de espaços comerciais em subsolo está prevista no contrato de concessão celebrado com o ML.

A FC tem a mesma natureza jurídica da MC, integrando o Setor Público Empresarial, não tendo, no entanto, nem recursos humanos nem instalações próprias, na sequência da integração dos seus trabalhadores no ML.

1. Metropolitano de Lisboa

Propósito

Ser o eixo central da mobilidade na Área Metropolitana de Lisboa.

Âmbito

Prestar um serviço de transporte público de passageiros no modo metropolitano ou noutros sistemas de mobilidade em canal dedicado, onde se insere a gestão global da infraestrutura nomeadamente a conceção, a promoção da construção e a exploração, incluindo a exploração de espaços comerciais, orientado para o cliente, em regime de concessão atribuída pelo Estado promovendo a mobilidade sustentável e visando a melhoria da qualidade de vida das gerações atuais e futuras.

Princípios de gestão

As decisões gestionárias tomadas pelo ML refletem os seguintes princípios de gestão:

- O superior interesse dos nossos passageiros;
- As expetativas das diferentes partes interessadas construindo relações duradouras de confiança com os nossos trabalhadores, passageiros, parceiros e comunidades;
- O desenvolvimento do negócio de forma socialmente responsável e sustentável articulando-se de forma estreita e concertada com os restantes operadores de transporte público;
- A promoção do transporte público e da mobilidade sustentável;

[1] DL n.º 148-A/2009, de 26 de junho, na sua redação atual.

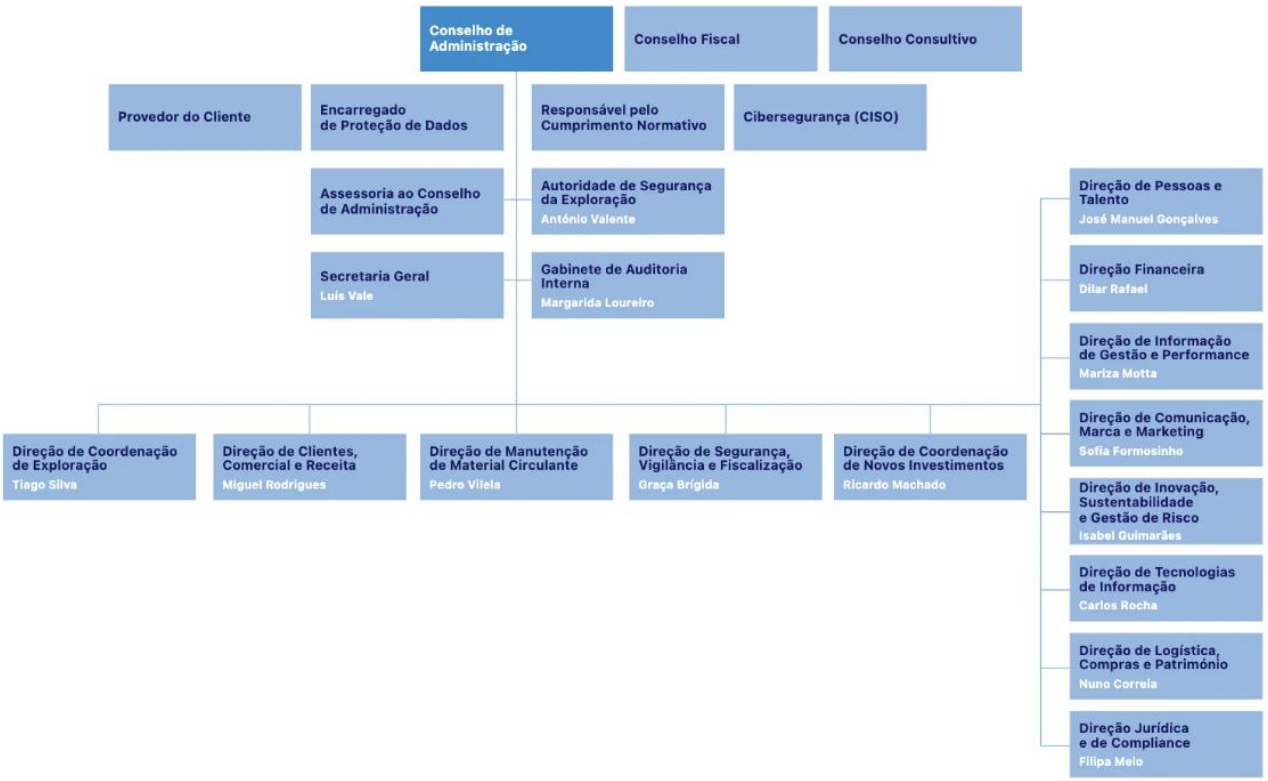
- O rigor, a transparência e o comportamento ético;
- A qualidade e segurança na prestação do serviço com recurso a soluções inovadoras, eficientes e criando valor nas áreas em que atuamos.

Estrutura orgânica

O Conselho de Administração do ML foi nomeado para o triénio 2026-2028 pela RCM n.º 213/2025, de 26 de dezembro, com a seguinte composição:

Nome	Cargo
Eng.ª Cristina Vaz Tomé	Presidente
Dr. Pedro Folgado	Vice-Presidente
Dr. Mahomed Bashir	Vogal
Eng.º Bruno Marques	Vogal
Dra. Sónia Páscoa	Vogal

A estrutura orgânica do ML encontra-se refletida no respetivo organograma, publicitado no *website* da Empresa, com a indicação das Áreas e dos seus Diretores de 1ª linha, estando as suas atribuições definidas no Manual de Organização da Empresa.



2. Metrocom

Propósito

Assegurar a adequação da oferta de produtos e serviços comerciais aos clientes do ML, no sentido de gerar um maior valor associado à utilização do meio de transporte público/metro.

Âmbito

A MC tem como função gerir com rigor e eficiência os espaços comerciais e outros equipamentos da rede do ML, assegurando a sua boa utilização, valorização e rentabilização, promovendo o aumento do grau de satisfação do cliente e a sua fidelização. Para tal, concilia o interesse comercial e a rentabilização dos seus espaços, obtendo receitas complementares como forma de gerar valor para o seu acionista, clientes e trabalhadores.

Princípios de gestão

As decisões gestionárias asseguradas pela MC refletem-se nos seguintes princípios de gestão:

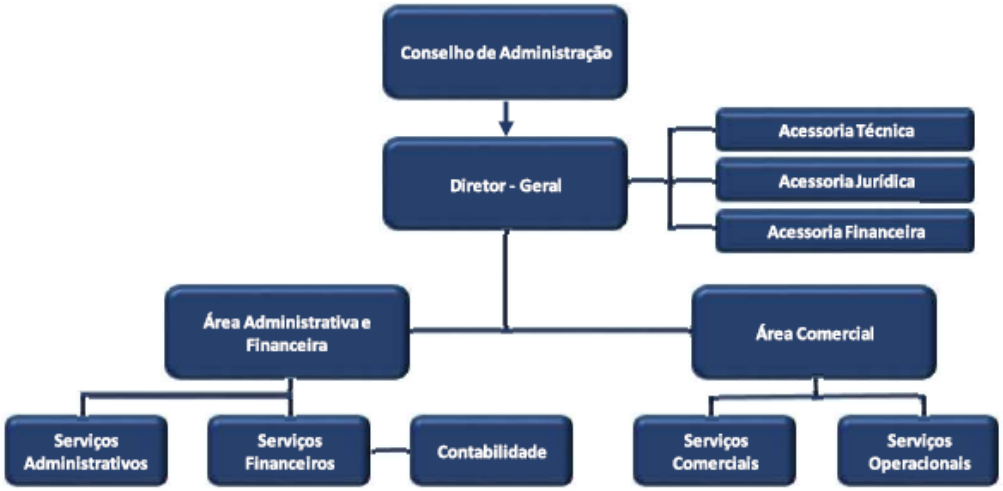
- Organização da atividade definida em função da dignidade humana, da valorização e respeito pelas pessoas, e na perspetiva da satisfação dos clientes, pautando-se pela prestação de um serviço de qualidade, e por critérios de rigor, imparcialidade, coerência e eficiência operacional, bem como pelo cumprimento dos compromissos assumidos com o cliente e com o acionista;
- Definição da estrutura organizacional assente na qualificação profissional e técnica dos seus recursos humanos, do espírito de equipa e na busca da excelência, com humildade e com respeito pelo outro;
- Responsabilidade económica, social e ambiental como empresa sustentável e geradora de valor, respeitadora das pessoas e da sua dignidade (trabalhadores, clientes e acionista) e amiga do ambiente.

Estrutura orgânica

O Conselho de Administração da MC para o triénio 2026-2028 foi eleito na Assembleia Geral de 8 de janeiro de 2026, e tem a seguinte composição:

Nome	Cargo
Eng.ª Cristina Vaz Tomé	Presidente
Dr. Pedro Folgado	Vogal
Eng.º Bruno Marques	Vogal
Dr. Mahomed Bashir	Vogal
Dra. Sónia Páscoa	Vogal

A estrutura organizativa adotada na MC compreende o recurso a direções partilhadas com o ML, sendo a gestão operacional da responsabilidade da MC, conforme organograma seguinte:



Estruturas	Responsável
Diretor Geral	Diogo Barbosa
Área Administrativa e Financeira	João Neves
Área Comercial	Diogo Barbosa

3. Outras empresas participadas

Ferconsult

Empresa especializada nas áreas de Consultoria, Estudos e Projetos de Engenharia de Transportes, que atua nos mercados nacional e internacional.

No final de 2020 deixou de ter trabalhadores, com a sua integração na empresa-mãe, mantendo a sua existência jurídica.

O ML detém direta e indiretamente, através da sua participada Ferconsult, uma participação de 100% do capital da empresa Ensitrans, A.E.I.E., cujo objeto principal consiste no desenvolvimento de estudos e projetos.

Trem e Trem II

A Trem, A.C.E. e a Trem II, A.C.E. são empresas cujo objeto principal consiste na aquisição e locação de equipamento ferroviário para o ML, sendo o seu capital detido a 100%, direta e indiretamente, através da sua participada Ferconsult.

III. Metodologia adotada para a identificação e classificação de riscos e medidas de mitigação

A metodologia desenvolve-se em quatro etapas:

1. Identificação das funções e atividades expostas;
2. Associação dos riscos às categorias e subcategorias adotadas;
3. Avaliação da probabilidade e do impacto, antes e depois da consideração dos controlos existentes;
4. Definição das medidas adicionais.

Os resultados detalhados destas etapas constam dos anexos 1 e 2.

O PPR constitui um subsistema do Sistema de Gestão de Risco (SGR) do ML e articula-se, em particular, com a gestão do risco de fraude, corrupção e comportamentos não éticos. Esta integração assegura que a identificação, a avaliação, o tratamento e a monitorização destes riscos seguem os princípios e os mecanismos de governação aplicáveis ao SGR.

Este Plano segue uma metodologia baseada na "Árvore da Fraude" da *Association of Certified Fraud Examiners* (ACFE)[2], já utilizada em versões anteriores.

A metodologia adota uma taxonomia de fraude com um âmbito mais amplo do que o conceito estrito de corrupção e infrações conexas. Para efeitos de identificação e análise, os riscos foram agrupados em três categorias principais, posteriormente desdobradas em subcategorias e, quando necessário, em níveis adicionais de detalhe:

C. CORRUPÇÃO E CONFLITOS DE INTERESSE
C1. Corrupção ativa / suborno, exercida sobre:
- C1.1. Exterior (empresas e indivíduos)
- C1.2. Trabalhadores (incluindo através de compensações internas não justificadas)

C2. Corrupção passiva ou conflitos de interesse
- C2.1. Deliberações / aprovações / orientações estratégicas, operacionais, financeiras e de *compliance*
- C2.2. Elaboração de estudos/projetos e organização de processos
- C2.3. Aquisição de bens, serviços e EOP (incluindo seleção de procedimento, adjudicações diretas, definição de especificações, elaboração de contratos, avaliação de propostas e seleção de fornecedores)
- C2.4 Recrutamento/seleção, processamento salarial, avaliação de desempenho, reclassificação e despedimento/exoneração de funções
- C2.5. Processos judiciais e disciplinares / contencioso / falsos testemunhos / tratamento de denúncias / assessoria/pareceres jurídicos
- C2.6. Atribuição de patrocínios, subsídios, donativos ou outros benefícios / parcerias
- C2.7. Aplicação de penalidades (coimas / multas)
  - C2.7.1. Fornecedores e prestadores de serviço
  - C2.7.2. Passageiros
- C2.8. Subfaturação
- C2.9. Sobrefaturação / gestão contratual (de bens, serviços e EOP, incluindo serviços / trabalhos a mais)
- C2.10. Atribuição de indemnizações / acordos

[2] Publicada originalmente em 1996 no relatório "*Report to the Nation on Occupational Fraud and Abuse*" e atualizada a cada versão do relatório, sendo a última de 2026: "*Occupational Fraud 2026: A Report to the Nations*".

C2.11. Recebimentos ilegais através de dinheiro / presentes / viagens / entretenimento / outros
C2.12. Extorsão económica
C2.13. Facilitação de acesso indevido (para ato criminoso, incluindo terrorista ou vantagem)
C2.13.1. Instalações
C2.13.2. Sistemas e tecnologias da informação e da operação
C2.14. Facilitação de branqueamento de capitais, financiamento do terrorismo, auxílio à imigração ilegal e tráfico humano (em espaços comerciais)
C2.15. Auditoria / inspeção / fiscalização

M. MANIPULAÇÃO DE INFORMAÇÃO

M1. Financeira
M1.1 Rendimentos e gastos impropriamente contabilizados e declarados / Ativos e passivos incorretamente avaliados e refletidos no balanço
M1.2. Divulgação de informação económica e financeira deturpada
M1.3. Ocultação / encobrimento de rendimentos e gastos
M2. Não financeira (incluindo indicadores e outros reportes/comunicações)
M2.1. Divulgação de informação não financeira deturpada
M2.2. Ocultação / encobrimento de informação não financeira relevante

A. APROPRIAÇÃO INDEVIDA DE ATIVOS

A1. Furto de dinheiro
A1.1. Manipulação do registo de vendas
A1.1.1. Produtos e subprodutos
A1.1.2 Títulos de transporte
A1.2. Coleta / recolha de receitas
A1.3. Trocos e diferimento de depósitos
A1.4. Fundos de maneio, fixos de caixa e de devolução
A2. Despesas indevidas, incluindo através do fundo de maneio
A3. Uso indevido de bens da empresa (*fringe benefits*)
A3.1. Automóvel
A3.2. Telemóvel
A3.3 Computador pessoal
A4. Transferências bancárias / pagamentos *homebanking*
A4.1. Uso indevido de *password* do sistema
A4.2. Autorizações forjadas
A4.3 Conta de destino não autorizada
A5. Cheques (incluindo cheques contrafeitos, furto de cheques e falsificação do seu preenchimento)
A6. Fraude na folha salarial
A6.1. Empregados fantasma
A6.2. Falsificação de horas, salários e subsídios
A6.3 Irregularidade no fornecimento de refeições
A6.4 Baixa fraudulenta
A7. Fraude em seguros
A7.1. Recebimento de indemnizações
A7.2. Reembolso de despesas
A7.3. Beneficiário fictício
A7.4. Alegação fictícia de acidente de trabalho / empolamento de danos pessoais
A7.5 Alegação fictícia de acidentes automóveis / empolamento de danos
A8. Furto / utilização indevida de existências
A9. Furto / utilização indevida de ativos fixos tangíveis
A10. Furto de propriedade intelectual
A11. Furto / utilização indevida de informação confidencial
A12. Avaliação fraudulenta de ativos

A12.1 Ativos fixos tangíveis
A12.2 Propriedades de investimento
A12.3. Aplicações / produtos financeiros

Com o envolvimento das Unidades Orgânicas, os riscos foram classificados em função de dois critérios de avaliação, a probabilidade de ocorrência (PO) e o impacto previsível da ocorrência do risco (IP), tendo sido considerados os seguintes indicadores de aferição, baseados no Guia n.º 1/2023 do MENAC:

Probabilidade de ocorrência do risco (PO)	
Baixa (1)	A prevenção do risco decorre adequadamente das medidas de mitigação adotadas anteriormente.
Média (2)	A prevenção adequada do risco pode requerer e justificar medidas de mitigação adicionais relativamente às que já existam.
Alta (3)	A prevenção adequada do risco requer medidas de mitigação adicionais relativamente às que já existam.

Impacto previsível da ocorrência do risco (IP)	
Baixo (1)	A ocorrência do risco pode traduzir-se numa redução da eficiência do procedimento ou da função a que está associado, requerendo a revisão do próprio procedimento. Trata-se de um impacto interno, com implicações no plano processual da entidade ou organização.
Médio (2)	A ocorrência do risco pode traduzir-se numa redução da eficiência e eficácia do procedimento ou da função a que está associado, requerendo a revisão do procedimento e dos correspondentes objetivos que lhe estão associados. Trata-se de um impacto interno, com implicações no plano processual e produtivo da entidade ou organização.
Alto (3)	A ocorrência do risco pode traduzir-se numa redução da eficiência e eficácia do procedimento ou da função a que está associado e pode ser objeto de mediatização. Trata-se de um impacto com implicações internas no plano processual e produtivo da entidade ou organização, e com implicações externas, de mediatização da ocorrência, com impactos reputacionais sobre a sua credibilidade.

A determinação do nível de risco decorreu da combinação da probabilidade e impacto, referidas anteriormente, de acordo com a seguinte matriz de avaliação de riscos:

		Probabilidade de Ocorrência (PO)		
		Baixa (1)	**Média (2)**	**Alta (3)**
Impacto Previsível (IP)	**Baixo (1)**	Mínimo	Fraco	Moderado
	Médio (2)	Fraco	Moderado	Elevado
	Alto (3)	Moderado	Elevado	Máximo

Para cada risco são avaliados o nível inerente (ou bruto), antes da consideração dos controlos e das medidas de mitigação existentes, e o nível residual (ou líquido), após a consideração desses mecanismos. A diferença entre os dois níveis evidencia o efeito esperado dos controlos. Por prudência metodológica, o

risco inerente é, em regra, classificado como elevado ou máximo, sem prejuízo da fundamentação aplicável a cada situação.

A identificação dos riscos, as funções ou atividades associadas, o nível de risco residual e as medidas de mitigação adotadas e a adotar constam de uma tabela no anexo 1, de acordo com o modelo apresentado em seguida:

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar

O anexo 2 apresenta a matriz consolidada dos riscos e destaca aqueles cujo nível residual é mais elevado, permitindo priorizar o acompanhamento e a implementação de medidas adicionais.

No anexo 3 apresentam-se as definições de corrupção e infrações conexas previstas no RGPC e refletidas no Código de Ética e de Conduta do ML.

IV. Acompanhamento da execução do Plano

A execução do PPR é avaliada através de dois instrumentos complementares:

- O Relatório de Avaliação Anual, que abrange a totalidade dos riscos e é apresentado até abril do ano seguinte àquele a que respeita,
- E o Relatório de Avaliação Intercalar, que incide sobre os riscos de nível elevado ou máximo e é apresentado até outubro de cada ano.

Na elaboração dos relatórios de avaliação, as Áreas responsáveis validam a informação relativa aos riscos sob a sua responsabilidade, atualizam o estado de implementação das medidas, avaliam a respetiva eficácia e fundamentam eventuais atrasos ou necessidades de reformulação. Os contributos são consolidados para efeitos de acompanhamento global da execução do PPR.

Medidas de mitigação	A medida está adotada? *(Sim / Não)*	Eficácia da medida *(se adotada)* / Razões para a sua não adoção *(quando não adotada)*	Outras medidas a adotar *(sobretudo para as situações de não adoção ou de ineficácia da medida)*

V. Aprovação, divulgação e comunicação

Nos termos dos n.ºs 6 e 7 do artigo 6.º do RGPC, o PPR é divulgado no prazo de 10 dias após a sua aprovação pelo CA:

a) Aos seus trabalhadores, através da publicação do documento no separador da prevenção de corrupção na *intranet* do ML e no *website* do ML, FC e MC;

b) Às entidades competentes, por *e-mail* à Tutela Setorial e Financeira do ML e serviços de inspeção (AMT) e fiscalização (IGF), e ao MENAC, através do carregamento em plataforma específica para o efeito.

VI. Anexos

Anexo 1 – Identificação e classificação dos riscos e medidas de mitigação

No que respeita às medidas de mitigação adotadas, merecem particular destaque os instrumentos que resultam do RGPC e outros complementares, que são transversais a todos ou a grande parte dos riscos identificados (cf. capítulo III), contribuindo para uma política de prevenção e de combate à corrupção e infrações conexas:

Riscos	Função ou Atividade	Medidas de mitigação adotadas	Medidas de mitigação a adotar
GERAL	Todas as funções e atividades em geral	Plano de Prevenção de Riscos de Corrupção e Infrações Conexas (**PPR**)[3] e respetivos Relatórios de avaliação (intercalar e anual).	
		Código de Ética e de Conduta (**CEC**)[4], prevendo, entre outras, questões relacionadas com conflito de interesses, relacionamento entre trabalhadores e com passageiros e entidades externas e confidencialidade da informação.	Reformulação do CEC para incluir a gestão da representação legítima de interesses (*lobby*).
		Canal de comunicação de denúncias (denominado **Canal de Ética**)[5] disponível na *intranet do ML*[6], com Regulamento de tratamento das denúncias.	Alargamento do Portal ML e do Canal de Ética aos trabalhadores da Metrocom. Mecanismos de denúncia associados à representação legítima de interesses (*lobby*).
		Plano de **formação** e **comunicação** de Ética Empresarial[7]	
		Subscrição de Declarações de Conflito de Interesses, incluindo de inexistência (**DICI**) ou de existência, e sua monitorização.[8]	Criação de procedimentos de conflito de interesses, que prevê a subscrição de Declarações de Conflito de Interesses.
		Procedimentos de comunicação e registo de **ofertas** e sua monitorização.	
		Sistema de controlo interno assente no modelo das 3 linhas.[9]	

[3] Cfr. art. 5.º e 6.º do RGPC.
[4] Cfr. art. 5.º e 7.º do RGPC.
[5] Cfr. art. 5.º e 8.º do RGPC.
[6] Cfr. Lei n.º 93/2021, de 20 de dezembro, que estabelece o regime geral de proteção dos denunciantes de infrações.
[7] Cfr. art. 5.º e 9.º do RGPC. Formação, de carácter obrigatório, para os trabalhadores do ML, de todos os níveis hierárquicos, e divulgação regular, através da *intranet*, de notícias sobre a temática.
[8] Coexistem na Empresa várias minutas de DICI: 1. as exigidas pelo art. 13.º/2 do RGPC (Portaria n.º 185/2024/1, alterada pela Portaria n.º 287-A/2025/1) e que inclui as genéricas do CEC (para membros do Conselho de Administração, diretores e demais chefias, participantes em procedimentos de recrutamento e formação e trabalhadores afetos à área de logística responsáveis por procedimentos de aquisição não abrangidos pelo CCP) e as específicas relativas à contratação pública, à concessão de subsídios, subvenções ou benefícios e aos processos disciplinares – Para os processos de autorização da despesa relacionados com a contratação pública e a concessão de subsídios, subvenções ou benefícios, o ML desenvolveu internamente uma solução em SAP, que consiste na automatização do preenchimento das DICI nestes processos, permitindo, de forma simples, dar cumprimento ao previsto na lei; 2. as exigidas pelo CCP (para júri e afins e gestores de contrato); 3. para os auditores internos e os intervenientes na análise e gestão de denúncias apresentadas no Canal de Ética. Existe ainda minuta para declarar a existência de conflito de interesses.
[9] Na 1ª linha de defesa, insere-se a atividade das Áreas e os respetivos procedimentos, sendo de destacar o Manual de Organização da Empresa, os manuais de processo do Sistema de Gestão de Qualidade e Ambiente e restante normativo interno (inclui regulamentos e instruções de trabalho), e os sistemas de informação e de operação (onde se inclui a ferramenta SAP de monitorização do cumprimento das deliberações do CA). Estes asseguram a observância dos princípios da independência, segregação de funções, bem como a adequada supervisão das tarefas realizadas. Na 2ª linha de defesa encontram-se as funções de gestão de risco (inclui o Manual de Risco, o Comité de Risco e seu Regulamento, bem como uma ferramenta informática de suporte) e de *compliance* (inclui o Manual de *Compliance* e uma ferramenta informática de suporte que permite a monitorizar o estado de cumprimento das obrigações macro) e na 3ª linha está função da auditoria interna (inclui o Manual de Auditoria Interna). *Vd*. maior detalhe em documento próprio do PCN.

Riscos	Função ou Atividade	Medidas de mitigação adotadas	Medidas de mitigação a adotar
		Canal de Denúncia de Assédio.	

Os quatro primeiros instrumentos materializam o Programa de Cumprimento Normativo (PCN)[10], tendo o ML um responsável pelo cumprimento normativo e encontrando-se observado o dever de publicitação no seu *website*, de acordo com o previsto no RGPC. No PCN encontram-se as medidas de prevenção e combate à corrupção no ML e empresas participadas com maioria de capital, descrevendo ainda o sistema de controlo interno existente, com o respetivo modelo de governo.

No quadro seguinte indicam-se, para cada risco identificado, a função ou atividade a que respeita, o nível de risco residual[11] e as medidas de mitigação adotadas e a adotar:

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
C. CORRUPÇÃO E CONFLITOS DE INTERESSE						
C1. Corrupção ativa / suborno, exercida sobre:						
C1.1. Exterior (empresas e indivíduos)	Relacionamento com entidades externas	1	2	Fraco	- Cumprimento do Regimento do CA, que estabelece as regras aplicáveis ao seu funcionamento (incluindo a composição do CA e competências dos seus membros, a periodicidade das reuniões, o agendamento de assuntos, os critérios de apresentação de propostas das Áreas e o processo de deliberação).	
C1.2. Trabalhadores (incluindo através de compensações internas não justificadas)	Todas as funções e atividades em geral	1	1	Mínimo	- Regime de acesso a cargos dirigentes do ML. - Aplicação do Regulamento de Carreiras anexo ao AE e demais legislação aplicável no ML. - Remunerações / compensações previstas nos AE e em normativos devidamente aprovados pelo CA e processadas pela DPT com base na informação que resulta do registo e controlo de assiduidade. - Rastreio dos pressupostos da realização de IHT, de trabalho suplementar e de outras compensações. - Delegação e subdelegação de competências para autorização da realização de trabalho suplementar e de trabalho noturno. - Processo de avaliação de desempenho com possibilidade de recurso pelos trabalhadores, em caso de discordância. - Levantamento das necessidades de formação dos trabalhadores/Áreas. - Regulamento de deslocações e estadas ao serviço do ML.	

[10] Cfr. art. 5.º/1 do RGPC. *Vd.* maior detalhe de cada instrumento em documento próprio do PCN.
[11] As siglas "PO" e "IP" correspondem à probabilidade de ocorrência e ao impacto previsível (cf. metodologia no capítulo III).

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
C2. Corrupção passiva ou conflitos de interesse						
C2.1. Deliberações / aprovações / orientações estratégicas, operacionais, financeiras e de *compliance*	Todas as funções e atividades em geral	1	3	Moderado	– Cumprimento do Regimento do CA, que estabelece as regras aplicáveis ao seu funcionamento (incluindo as competências dos membros do CA, a periodicidade das reuniões, o agendamento de assuntos, os critérios de apresentação de propostas das Áreas e o processo de deliberação). – Definição das dependências hierárquicas e funcionais entre o CA e as Áreas. – Delegação e subdelegação de poderes para agilização progressiva do processo decisório nos diversos níveis hierárquicos de responsabilidade, estabelecidos no seu atual modelo organizacional. Permite a otimização da eficácia e da eficiência do funcionamento da empresa. – Cumprimento de Resoluções do Conselho de Ministros. – Cumprimento das obrigações previstas no Contrato de Concessão. – Execução do Plano de Atividades e Orçamento aprovado pela Tutela.	– Alargamento do modelo de delegação e subdelegação de poderes a outras matérias (maior autonomia e maior responsabilidade).
C2.2. Elaboração de estudos/projetos e organização de processos	Expansão e modernização da rede	1	3	Moderado	– Promover e manter atualizados estudos que permitam tomadas de decisão informadas sobre novos investimentos de expansão da rede. – Desenvolvimento de estudos de viabilidade de novos traçados, estudos prévios, anteprojeto e projeto de execução. – Obtenção de aprovações ou decisões favoráveis pelas diversas autoridades competentes (ex: Tutelas, Câmaras Municipais, APA, ANEPC). – Revisão de projetos contratada externamente, garantindo a respetiva autonomia face ao autor do projeto. Acresce que é dado cumprimento ao n.º 2 do artigo 43.º do CCP, sempre que aplicável. – Participação, em geral, de vários técnicos de diferentes áreas na organização dos processos.	

C2.3. Aquisição de bens, serviços e EOP (incluindo seleção de procedimento, adjudicações diretas, definição de especificações, elaboração de contratos, avaliação de propostas e seleção de fornecedores)	Contratação	2	3	Elevado	– Formação sobre o CCP e práticas de conluio na contratação pública. – Definição da competência para autorizar a despesa em função do valor, para aprovar a decisão de contratar e para a prática dos demais atos necessários à formação, celebração e execução dos contratos (CA/ADM/Diretores e outras chefias – delegação e subdelegação de competências), com parametrização do SAP em conformidade (para aprovação de requisições de compra). – Subscrição de DICI por todos os envolvidos nos processos de contratação pública e sua monitorização. – Parametrização em SAP das DICI de contratação pública para a autorização de despesa (exigidas pelo art. 13.º/2 do RGPC – Portaria n.º 185/2024/1, alterada pela Portaria n.º 287-A/2025/1), seguindo uma lógica de simplificação, através da criação automática e desmaterializada de tais declarações via SAP/DMS. – A aquisição de bens ou serviços respeita os procedimentos exigíveis pelo CCP e os termos do Manual de Compras e é promovida não só pela DLCP mas também pela DJC, que também efetua procedimentos adjudicatórios e participa como júri na avaliação de propostas nos mesmos. – Definição exaustiva e objetiva das especificações técnicas / projeto de execução que devem constar em cada caderno de encargos, bem como do modelo de avaliação das propostas no programa de procedimento, quando aplicável (cumprindo o CCP). – Confirmação se as especificações técnicas afastam a dependência em fornecedores únicos e não condicionam a adjudicação a um determinado fornecedor, sempre que possível. – Peças do procedimento de concurso de EOP validadas pela assessoria jurídica respetiva. – Os avisos de abertura de concursos para a apresentação de candidaturas/propostas são adequadamente publicitados. – Utilização de ferramentas informáticas para a contratação pública (plataformas externa[12] e interna[13] e aplicação *web*[14]), com garantia da confidencialidade das propostas até ao termo do prazo para a sua apresentação. – Sempre que possível, opção por um procedimento mais concorrencial (consulta a pelo menos 3 fornecedores e rotatividade destes, em contratação excluída da parte II do CCP – baixo valor ou sector especial dos transportes) e utilização da plataforma externa de contratação pública mesmo não sendo legalmente obrigatório. Quando não é utilizada a plataforma externa é feito o recurso à aplicação *web*. – Adjudicações diretas apenas realizadas nas situações em que o CCP o permite, sendo promovida a concorrência (art. 16.º do RGPC). – Procedimentos por ajuste direto com convite a um só fornecedor são alvo de uma adequada fundamentação. – Controlo do limite trienal previsto no CCP. – Monitorização automática das obrigações decorrentes do CCP, através de integração da plataforma interna de contratação pública com a de *Compliance*.	– Implementação de uma plataforma de compras para procedimentos sem tramitação associada (que substituirá a aplicação *web*). – Desenvolvimento da plataforma de gestão de contratos, com alertas integrados. – Criação de uma bolsa de fornecedores para garantir maior diversidade e rotatividades dos mesmos. – Estudo da definição de um KPI de desempenho da área de compras alicerçado na promoção da concorrência. – Criação de um Código de Conduta dos fornecedores, que possa reforçar as questões relacionadas com a existência de conflitos de interesse e de participação na elaboração das peças de procedimento. – Atualização dos Manuais de Compras e do Processo "Recursos Materiais" (SGQA). – Elaboração de Manual do Gestor do Contrato e formação sobre as suas competências e responsabilidades. – Elaboração de uma *checklist* com as responsabilidades do gestor do contrato (a entregar aquando da subscrição das DICI pelos mesmos). – Em contratos de maior complexidade, passar a prever a existência de indicadores de execução e a nomeação de 2 gestores. – Atualização do procedimento de utilização da ferramenta ARACHNE

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
					– Utilização de uma *checklist* de conformidade nos procedimentos de concurso limitado por prévia qualificação com publicidade internacional, elaborada tendo por base o CCP e a Resoluções do TdC. – As candidaturas/propostas apresentadas são registadas e sujeitas a um processo de avaliação e seleção em conformidade com os procedimentos definidos e aprovados. – Júris de concursos composto por elementos de pelo menos duas Áreas (e, sempre que possível com rotatividade de técnicos). – Procedimento interno para a utilização da ferramenta ARACHNE[15] no âmbito dos projetos financiados por fundos comunitários para verificações *ex ante* relativas a conflitos de interesses (com a respetiva alusão nas peças de procedimentos pré-contratuais). – Registo em SAP de todas as necessidades de aquisição mediante a criação de requisição de compra em momento prévio à aprovação da despesa e através do registo do contrato em sistema (efetuado de acordo com o manual "Registo de Contratos em sistema SAP"), permitindo o inerente controlo de toda a contratação da empresa e consequentes pagamentos realizados. – Todas as decisões de aceitação/rejeição de candidaturas/propostas são comunicadas aos respetivos candidatos. – Pressupostos que sustentam a aprovação de uma alteração contratual, formalizada em adicional são alvo de uma adequada fundamentação que justifique a não adoção de um novo procedimento de concurso. – Formalização de adicionais aos contratos e publicitação dos mesmos no Portal Base e JOUE, sempre que aplicável. – Introdução de cláusula a assegurar o direito a auditar a execução do contrato pelo ML nas peças dos procedimentos pré-contratuais.	de forma a abranger todas as fontes de financiamento comunitário.

[12] Parametrizada (integrada com o Portal Base) para permitir a publicação automática neste Portal das contratações ocorridas no setor especial dos transportes (excluídas da parte II do CCP), dando cumprimento ao art. 465.º do CCP. A DLCP efetua a desencriptação dos ficheiros extraídos da plataforma, devendo ser feita em simultâneo para todos os concorrentes e apenas no fim do prazo de entrega das propostas. Após esta desencriptação, o controlo de acessos à pasta de trabalho é mantido restrito aos interessados (nomeadamente o Júri).

[13] Acompanha toda a fase pré-contratual e respetivas autorizações, permitindo a uniformização de procedimentos internos e o registo e acompanhamento (também pelas áreas requisitantes) dos procedimentos de contratação, aumentando a eficiência e a transparências dos mesmos. Desenvolvida em SAP.

[14] Utilizada para contratação em que a plataforma externa não é legalmente obrigatória. Tem uma caixa de correio dedicada e não permite a abertura de propostas em momento prévio à data definida para o efeito, garantindo os princípios previstos no art. 1.º-A do CCP.

[15] Ferramenta desenvolvida no âmbito da Comissão Europeia, enquanto mecanismo de mitigação de riscos de ocorrência de situações de conflitos de interesses, fraude, corrupção e duplo financiamento, visando proteger os interesses financeiros da União Europeia.

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
C2.4. Recrutamento/seleção, processamento salarial, avaliação de desempenho, reclassificação e despedimento/exoneração de funções	Gestão de recursos humanos	1	2	Fraco	– Regime de acesso a cargos dirigentes do ML. – Subscrição de DICI pelos trabalhadores envolvidos nos processos de recrutamento e formação e sua monitorização. – Aplicação do Regulamento de Carreiras anexo ao AE e demais legislação aplicável no ML. – Remunerações / compensações previstas nos AE e em normativos devidamente aprovados pelo CA e processadas pela DPT com base na informação que resulta do registo e controlo de assiduidade. – Rastreio dos pressupostos da realização de IHT, de trabalho suplementar e de outras compensações. – Delegação e subdelegação de competências para autorização da realização de trabalho suplementar e de trabalho noturno. – Sistema informático de processamento do vencimento. – Processo de avaliação de desempenho com possibilidade de recurso pelos trabalhadores, em caso de discordância. – Levantamento das necessidades de formação dos trabalhadores/Áreas. – Realização de entrevista de saída da Empresa, com análise de motivos.	
C2.5. Processos judiciais e disciplinares / contencioso / falsos testemunhos / tratamento de denúncias / assessoria/pareceres jurídicos	Gestão de processos judiciais	1	3	Moderado	– Proibição de conflitos de interesse e de instruir testemunhas, de acordo com o previsto nos artigos 99.º e 109.º do EOA, aprovado pela Lei n.º 145/2015, na atual redação, e sancionamento das infrações detetadas. – Sujeição dos termos dos acordos judiciais ou extrajudiciais a prévia aprovação do CA. – Subscrição de DICI pelos intervenientes nos processos disciplinares (instrutor, membros do órgão decisor e membros do CA) e na análise e gestão de denúncias apresentadas no Canal de Ética e sua monitorização. – Processo de tratamento de denúncias no Canal de Ética e no Canal de Denúncia de Assédio de acordo com os respetivos regulamentos e legislação aplicável.	

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
C2.6. Atribuição de patrocínios, subsídios, donativos ou outros benefícios / parcerias	Relacionamento com entidades externas	1	2	Fraco	– Subscrição de DICI aquando da atribuição de subsídios ou equivalente e sua monitorização. – Aprovação prévia do CA e cumprimento da legislação no que respeita à publicitação e reporte das subvenções públicas junto da IGF (Lei n.º 64/2013, de 27 de agosto). – Cumprimento da transparência administrativa, incluindo a publicitação no *website* e *intranet* da relação de todos os benefícios e subvenções concedidos, independentemente do valor (art. 12.º do RGPC). – Formalização de acordos e parcerias no âmbito da política comercial da empresa com entidades terceiras, pessoas coletivas ou singulares, no que se refere à concessão de benefícios e de acesso à rede de transporte e demais condições contratuais, respeitando a política de descontos comerciais aprovado pelo CA, em vigor em cada momento. – Estabelecimento de acordos com entidades terceiras, referentes a atividades sem relação direta com o serviço de transporte, que revistam interesse para a projeção da marca ML e para angariação de receitas adicionais, incluindo a definição das condições contratuais para o efeito.	– Definição de Regulamento de registo e atribuição aos trabalhadores de bilhetes ou outros benefícios recebidos pela Empresa na sequência de parcerias, patrocínios ou outros benefícios atribuídos.
C2.7. Aplicação de penalidades (coimas / multas)						
C2.7.1. Fornecedores e prestadores de serviços	Gestão de contratos / projetos	1	3	Moderado	– O gestor do contrato / projeto propõe, se for o caso, a aplicação de penalidades. – Aplicação de penalidades nos termos previstos contratualmente, salvo decisão fundamentada e aprovada pelo CA. – Definição da delegação de competências nos membros do CA para a prática dos atos necessários à execução dos contratos, designadamente a aplicação de sanções por incumprimento de obrigações contratuais ou legais.	– Desenvolvimento da plataforma de gestão de contratos, com alertas integrados. – Elaboração de Manual do Gestor do Contrato e formação sobre as suas competências e responsabilidades. – Elaboração de uma *checklist* com as responsabilidades do gestor do contrato (a entregar aquando da subscrição das DICI pelos mesmos). – Em contratos de maior complexidade, passar a prever a existência de indicadores de execução e a nomeação de 2 gestores.

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
C2.7.2. Passageiros	Fiscalização de passageiros	1	1	Mínimo	- Canais de acesso da rede ML fechados, apenas permitindo entradas/saídas de pessoas com validação de título de transporte. - A composição das equipas de fiscalização inclui uma chefia atenta ao risco, minimizando-o. - Acompanhamento das equipas de fiscalização por vigilantes - Terminais Portáteis de Fiscalização (TPF) utilizados pelos fiscais em modo ambulante (cais/átrio e comboio) para controlo dos títulos de transporte e para registo das infrações incluindo os respetivos autos de notícia. Um título não válido deve ter sempre associado auto de notícia. - Rotina de envio diário de autos emitidos ao IMT/AT - Campanha de informação/sensibilização ao passageiro para a validação do título de transporte.	- Instalação de aplicação nos terminais de fiscalização com novas funcionalidades.
C2.8. Subfaturação	Venda de bens e serviços / Outras cobranças	1	2	Fraco	- Verificação da conformidade da faturação face ao contratado mediante o registo no SAP. - Utilização de leilões eletrónicos em processos de venda de sucata e de imóveis, sem intervenção direta da Empresa na licitação.	

C2.9. Sobrefaturação / gestão contratual (de bens, serviços e EOP, incluindo serviços / trabalhos a mais)	Gestão de contratos / projetos	1	3	Moderado	– Formação sobre o CCP e práticas de conluio na contratação pública. – Definição da competência para autorizar a despesa em função do valor, para aprovar a decisão de contratar e para a prática dos demais atos necessários à formação, celebração e execução dos contratos (CA/ADM/Diretores e outras chefias – delegação e subdelegação de competências), com parametrização do SAP em conformidade (para aprovação de requisições de compra). – Subscrição de DICI por todos os envolvidos nos processos de contratação pública e sua monitorização. – Subscrição de DICI pelos gestores de contrato e sua monitorização. – Rastreabilidade no SAP da autorização da despesa e da realização do pagamento. – Registo em SAP de todas as necessidades de aquisição mediante a criação de requisição de compra em momento prévio à aprovação da despesa e através do registo do contrato em sistema (efetuado de acordo com o manual "Registo de Contratos em sistema SAP"), permitindo o inerente controlo de toda a contratação da empresa e consequentes pagamentos realizados. – Procedimentos de registo e acompanhamento da execução de nota de encomenda e de contratos em SAP com e sem hierarquia de serviços. – Gestor do contrato / projeto, que acompanha a sua execução, com atribuições em matéria de validação de serviços prestados / bens fornecidos e execução de empreitadas e sua faturação. – Pagamentos aos empreiteiros/fornecedores apenas efetuados depois de verificada a conformidade da faturação face ao contratado (e consequentemente face ao orçamentado) através de documentos de controlo, registados no SAP (Registo do contrato em SAP, Anexo a Pedidos de Autorização de Pagamento, Auto de Medição, Autos de receção e declarações de aceitação – previstos nos cadernos de encargos para garantir a conformidade dos materiais e serviços –,Mapa de Controlo de Faturação, Relatório de controlo de execução de contratos). – Fiscalização de obras contratada externamente e independente do Empreiteiro. – Monitorização da execução do Plano de Trabalhos de empreitadas – Processo eficiente e eficaz gestão de alterações em empreitadas, com avaliação dos pedidos de alteração por equipa multidisciplinar e respeito pelos prazos legal ou contratualmente previstos. – Confirmação dos recursos humanos envolvidos na implementação de um contrato, nomeadamente dos elementos chave, comparativamente aos aprovados na proposta e previstos no contrato, solicitando evidência da adequabilidade caso se verifiquem substituições significativas. A substituição de elementos chave deve ter autorização prévia do ML. – Mecanismo de verificação/deteção de registo no sistema de faturas em duplicado (ex: com o mesmo montante ou com a mesma referência) ou falsas. – Processo de registo no SAP da entrada de faturas por *e-mail* que minimiza os erros decorrentes da inserção manual dos dados. – Formalização de adicionais aos contratos e publicitação dos mesmos no Portal Base e JOUE, sempre que aplicável.	– Atualização dos Manuais de Compras e do Processo "Recursos Materiais" (SGQA). – Elaboração de Manual do Gestor do Contrato e formação sobre as suas competências e responsabilidades. – Elaboração de uma *checklist* com as responsabilidades do gestor do contrato (a entregar aquando da subscrição das DICI pelos mesmos). – Em contratos de maior complexidade, passar a prever a existência de indicadores de execução e a nomeação de 2 gestores. – Monitorização/revisão do subsistema de gestão de risco para os projetos de prolongamento da linha Vermelha e linha Violeta (associados ao risco de "Gestão da expansão da rede" do SGR), que inclui os riscos relacionados com a corrupção e as infrações conexas. Início da fase de gestão de riscos após a consignação da obra. – Auditoria à execução do contrato de aquisição de serviços de manutenção e conservação dos espaços comerciais do ML e respetivo *follow-up* de implementação das recomendações. – Auditoria ao processo de reporte de execução física e financeira dos projetos co-financiados às entidades e respetivo *follow-up* de implementação das recomendações.

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
					– Monitorização/revisão do subsistema de gestão de risco para o projeto da linha Circular[16] (associado ao risco de "Gestão da expansão da rede" do SGR), que inclui os riscos relacionados com a corrupção e as infrações conexas. – Introdução de cláusula a assegurar o direito a auditar a execução do contrato pelo ML nas peças dos procedimentos pré-contratuais.	
C2.10. Atribuição de indemnizações / acordos	Gestão de contratos / projetos	1	3	Moderado	– Indemnizações ou acordos com fornecedores e prestadores de serviço submetidos à aprovação do CA. – Indemnizações por ocupações ou expropriações a todos os interessados, designadamente proprietários, arrendatários e empresas, de acordo com o que está previsto na lei e mediante o valor apurado por peritos avaliadores independentes designados pelo Tribunal da Relação de Lisboa. – Indemnizações por prejuízos a todos os interessados, designadamente proprietários, arrendatários e empresas, de acordo com o que está previsto na lei. – Processos de indemnização por expropriação acompanhados pela DJC, por consultor externo e submetidos à aprovação do CA. – Monitorização/revisão do subsistema de gestão de risco para o projeto da linha Circular[17] (associado ao risco de "Gestão da expansão da rede" do SGR), que inclui os riscos relacionados com a corrupção e as infrações conexas.	– Monitorização/revisão do subsistema de gestão de risco para os projetos de prolongamento da linha Vermelha e linha Violeta (associados ao risco de "Gestão da expansão da rede" do SGR), que inclui os riscos relacionados com a corrupção e as infrações conexas. Início da fase de gestão de riscos após a consignação da obra.
C2.11. Recebimentos ilegais através de dinheiro / presentes / viagens / entretenimento / outros	Relacionamento com entidades externas	1	2	Fraco	– Procedimentos de comunicação e registo de ofertas, com elaboração de relatório anual. – Reforço periódico da comunicação do referido Procedimento aos trabalhadores, bem como uma informação aos parceiros sobre as políticas anticorrupção e respetivos controlos implementados na Empresa, visando desincentivar ofertas. – Cumprimento da transparência administrativa, incluindo a publicitação no *website* e *intranet* da relação de doações, heranças, ofertas ou donativos recebidos (art. 12.º do RGPC).	– Definição de Regulamento de registo e atribuição aos trabalhadores de bilhetes ou outros benefícios recebidos pela Empresa na sequência de parcerias, patrocínios ou outros benefícios atribuídos.
C2.12. Extorsão económica	Relacionamento com entidades externas	1	3	Moderado		
C2.13. Facilitação de acesso indevido (para ato criminoso, incluindo terrorista ou vantagem)						

[16] Prolongamento entre a estação Rato (linha amarela) e a estação Cais do Sodré (linha verde), incluindo as novas ligações nos viadutos do Campo Grande.
[17] Idem.

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
C2.13.1. Instalações	Segurança de acesso físico	1	3	Moderado	– Plano de Organização e Gestão de Segurança da Empresa (POGSE), enquanto subsistema do risco de "*Security*" do SGR. – Planos Anuais de Segurança da Exploração e respetivos Relatórios de acompanhamento semestral (remetidos ao IMT), enquanto subsistema do risco de "*Security*" do SGR. – Relatórios de segurança trimestrais com a análise da atividade. – Canais de acesso da rede ML fechados, apenas permitindo entradas/saídas de pessoas através de validação de título de transporte. – Regulamento de acesso, proteção e vigilância das instalações administrativas e oficinais no ML objeto de ações de formação. – Sistemas / ações de vigilância e gestão de contratos de serviços, guardaria e portaria, com produção de relatório trimestral de acompanhamento e verificação. – Ações de formação a Vigilantes. – Contributo da Divisão de Segurança aos Transportes Públicos da PSP (DSTP) para a segurança na rede ML. – Controlo de acessos às instalações do ML, físicos e à distância. – Auditorias cliente mistério periódicas aos procedimentos de segurança e vigilância nas instalações e implementação das respetivas recomendações.	– Alargamento da instalação de sistema de deteção de descida à via. – Atualização do sistema de vigilância. – Alargamento do sistema de mestragem. – Participação no projeto *Shield* PCP. – Plano de ação com medidas a implementar resultantes de GT sobre o vandalismo em operadores de transporte. – Levantamento de arquivo físico – Implementação do Relatório de Avaliação da Documentação Acumulada (RADA). – Processo de *follow-up* de implementação das recomendações da auditoria aos procedimentos de controlo da execução dos serviços de vigilância, guardaria e portaria.

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
C2.13.2. Sistemas e tecnologias da informação e da operação	Segurança de acesso digital	1	3	Moderado	– GT interdisciplinar no âmbito da cibersegurança para endereçar os desafios desta temática. – Existência do Responsável de Cibersegurança. – Existência de Encarregado de Proteção de Dados. – Política de Segurança de Informação do ML e formação em *e-learning* obrigatória (com conteúdos definidos internamente e disponibilizada na *intranet*). – Procedimento de resposta a ciberataques. – Plano de comunicação de crise – ciberataque. – Procedimento de gestão de *passwords*. – Introdução de requisitos de cibersegurança em cláusulas contratuais nos procedimentos de contratação. – Relatório de Cibersegurança (remetido anualmente ao CNCS). – O sistema SAP identifica os utilizadores que estão autorizados para o efeito, detendo cada um deles uma chave individual de acesso. – Mecanismos de controlo que permitem identificar o utilizador, o equipamento que foi utilizado, que programas informáticos foram executados, data e horas de utilização. – Outras medidas de segurança da informação (ex.: mudança periódica de *password*, composição da *password*, testes de *phishing* e realização de simulacros de intrusão). – Utilização de protocolos seguros (encriptados). – Configuração de segurança de portas nos *switches* – Modernização da autenticação e gestão de acessos, – Comunicação interna e formação para incutir a ciberconsciência. – Auditorias periódicas de segurança à infraestrutura de sistemas e tecnologias de informação (intrusão interna e externa).	– *Follow-up* das melhorias identificadas pelo GT da cibersegurança.

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
C2.14. Facilitação de branqueamento de capitais, financiamento do terrorismo, auxílio à imigração ilegal e tráfico humano (em espaços comerciais)	Gestão de espaços comerciais	1	2	Fraco	– Controlo e monitorização da atividade real dos lojistas com visitas de inspeção regulares aos espaços comerciais. – Não aceitação do pagamento da renda de lojistas em numerário.	– *Due diligence* e seleção de lojistas (avaliação prévia rigorosa dos atuais e potenciais lojistas, com realização de *background check* / questionário). – Introdução de cláusulas contratuais expressas, nos novos contratos de lojistas ou na respetiva renovação, sobre branqueamento de capitais, financiamento do terrorismo, auxílio à imigração ilegal e tráfico humano, cujo incumprimento conduza à imediata rescisão do contrato. – Formação e sensibilização de trabalhadores da Metrocom sobre fraude em espaços comerciais.
C2.15. Auditoria / inspeção / fiscalização	Gestão	1	2	Fraco	– Manual de Auditoria Interna. – Realização de auditorias internas e de ações de acompanhamento (*follow-up*) à implementação de recomendações dos relatórios de auditoria aprovados com relatórios trimestrais de reporte ao CA. – Promoção da salvaguarda da independência da função de auditoria interna e a objetividade dos auditores internos do GAI, sendo as auditorias efetuadas com rigor, isenção e imparcialidade, de acordo com o preconizado nas Normas Globais de Auditoria Interna (GIAS – *Global Internal Audit Standards*) do *The Institute of Internal Auditors*. – Subscrição de DICI pelo responsável do GAI e pelos auditores internos, que fazem parte integrante do processo da auditoria, e sua monitorização. – Colaboração do GAI com os órgãos de fiscalização da empresa. – Independência e autonomia de entidades externas responsáveis pelas atividades de Inspeção, Fiscalização e Auditoria.	

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
M. MANIPULAÇÃO DE INFORMAÇÃO						
M1. Financeira						
M1.1. Rendimentos e gastos impropriamente contabilizados e declarados / Ativos e passivos incorretamente avaliados e refletidos no balanço	Contabilidade	1	2	Fraco	– Respeito pelos princípios contabilísticos geralmente aceites. – Contas auditadas por uma empresa externa de Auditoria. – Declarações financeiras anualmente certificadas por uma sociedade de ROC e objeto de parecer por parte do CF/FU. – Independência e autonomia de entidades externas responsáveis pelas atividades de Inspeção, Fiscalização e Auditoria.	– Processo de *follow-up* de implementação das recomendações da auditoria aos adiantamentos em situação de doença e de acidente de trabalho.
M1.2. Divulgação de informação económica e financeira deturpada	Informação de gestão	1	2	Fraco	– Contas auditadas por uma empresa externa de Auditoria. – Declarações financeiras anualmente certificadas por uma sociedade de ROC e objeto de parecer por parte do CF/FU. – Independência e autonomia de entidades externas responsáveis pelas atividades de Inspeção, Fiscalização e Auditoria.	
M1.3. Ocultação / encobrimento de rendimentos e gastos	Informação de gestão	1	2	Fraco	– Pagamento de gastos/despesas apenas efetuado depois de validado/aprovado pelo responsável ou hierarquia competente, carecendo de justificação, comprovativo e registo obrigatório em SAP. – Declarações financeiras anualmente certificadas por uma sociedade de ROC e objeto de parecer por parte do CF/FU.	
M2. Não financeira (incluindo indicadores e outros reportes/comunicações)						
M2.1. Divulgação de informação não financeira deturpada	Informação de gestão	1	2	Fraco	– Cálculo rigoroso de indicadores, incluindo os referentes aos Contratos de Concessão e de Gestão. – Prevenção de situações de reporte fraudulento ou comunicação indevida de boas práticas de sustentabilidade (ex: *ESG washing*) e encobrimento de más práticas, incluindo da parte de fornecedores / prestadores / parceiros.	
M2.2. Ocultação / encobrimento de informação não financeira relevante	Informação de gestão	1	2	Fraco	– Cálculo rigoroso de indicadores, incluindo os referentes aos Contratos de Concessão e de Gestão.	

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
A. APROPRIAÇÃO INDEVIDA DE ATIVOS						
A1. Furto de dinheiro						
A1.1. Manipulação do registo de vendas						
A1.1.1. Produtos e subprodutos	Vendas	1	1	Mínimo	– Segregação de funções entre as Áreas responsáveis pelo processo de venda e pela cobrança de receita.	
A1.1.2. Títulos de transporte	Comercial	1	2	Fraco	– Controlo do cumprimento de procedimentos de registo e depósito de receita/valores da venda assistida. As vendas efetuadas por cada agente são registadas em sistema informático e controladas diariamente, comparando com a receita realizada. Em caso de falha significativa ou sistemática, o responsável é alvo de inquérito e eventual processo disciplinar. – Instruções de Trabalho relacionadas com a devolução de títulos de transporte em cartão Navegante ocasional e personalizado. – Instrução de Trabalho relacionada com a venda de títulos de transporte em posto de venda. – Controlo de receita analisa todos os turnos, mesmo os que vierem a zeros (designadamente verifica se foram realizadas trocas gratuitas e, em caso afirmativo, se foram enviados os respetivos cartões de origem). – Relatório com evidência de todos os eventos de troca e transferência de títulos em posto de venda. – Não permitidas operações de trocas de títulos sem leitura do cartão original para um novo cartão quando o número de série do cartão já foi objeto de alguma troca. Caso contrário, o Operador Comercial (OC) / Agente de Tráfego (AT) efetua um pré-registo no sistema MSAVT sujeito a validação e aprovação pelo Centro de Apoio Interno (CAI), sendo esta entidade responsável por definir a quantidade e/ou o valor a carregar no novo suporte, não tendo o OC/AT qualquer possibilidade de manipular esta informação. – Aquando da realização de transferências de títulos ou trocas por avaria, o sistema MSAVT não permite a inserção de números de cartão de forma manual. – Nas operações de transferência de títulos, os carregados no cartão de destino são eliminados do cartão de origem, de modo a que não seja possível executar várias transferências do mesmo título para vários cartões. – Nas operações de transferência de contrato (passe) das guias de substituição cartões Navegante personalizados, o mesmo é definitivamente eliminado da respetiva guia.	– Auditoria ao sistema de bilhética (processo de venda assistida – MSAVT) e respetivo *follow-up* de implementação das recomendações. – Devolução do valor pago pelos títulos de transporte para o mesmo de meio de pagamento (numerário ou cartão de débito/crédito).

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
A1.2. Coleta / recolha de receitas	Controlo de receita	1	2	Fraco	– Recolha e contagem de valores das MAVT e das MSAVT por entidade independente. – Análise da informação do sistema de bilhética e apuramento de falhas/sobras das MAVT e MSAVT. – Receita EMV exclusiva do ML, sem numerário envolvido e validada por entidade independente. – Diminuição do numerário em circulação face aos pagamentos eletrónicos (EMV e MB) e gratuitidades.	– Aquisição de MAVT para substituição do parque total existente na rede. – Auditoria ao sistema de bilhética (processo de venda assistida – MSAVT) e respetivo *follow-up* de implementação das recomendações.
A1.3. Trocos e diferimento de depósitos	Comercial	1	2	Fraco	– Controlo e registo em impresso próprio das entregas de unidades de trocos aos agentes. – Verificação periódica das existências de trocos nas malas personalizadas. Em caso de falha significativa ou sistemática, é feito um inquérito para averiguação das causas e determinação de responsabilidades. – Análise da informação do sistema de bilhética e apuramento de falhas/sobras das MAVT e MSAVT.	
A1.4. Fundos de maneio, fixos de caixa e de devolução	Gestão de fundos	1	1	Mínimo	– Cumprimento de normas e procedimentos definidos no Regulamento de Utilização de Fundos de Tesouraria. – Controlo e registo em impresso próprio e no SAP de todos os movimentos efetuados.	
A2. Despesas indevidas, incluindo através de fundos de maneio	Gestão de fundos	1	1	Mínimo	– Cumprimento de normas e procedimentos definidos no Regulamento de Utilização de Fundos de Tesouraria. – Pagamento de gastos/despesas apenas efetuado depois de validado/aprovado pelo responsável ou hierarquia competente, carecendo de justificação, comprovativo e registo obrigatório em SAP. – Mecanismo de verificação/deteção de registo no sistema de faturas em duplicado (ex: com o mesmo montante ou com a mesma referência) ou falsas. – Processo de registo no SAP da entrada de faturas por *e-mail* que minimiza os erros decorrentes da inserção manual dos dados.	
A3. Uso indevido de bens da empresa (*fringe benefits*)						
A3.1. Automóvel	Utilização de viaturas de serviço personalizadas e operacionais	1	1	Mínimo	– Normas de atribuição e utilização de veículos automóveis, definidas em Regulamento específico. – Existência de um gestor de frota. – Controlo mensal dos consumos de combustíveis e respetivos *plafonds* das viaturas de serviço personalizadas (mediante aplicação informática desenvolvida para o efeito), sendo suportado pelo utilizador o montante que exceda o fixado. – Controlo e registo diário em impresso próprio de todas as viagens efetuadas nas viaturas de serviço operacional, fins a que se destinam, quilómetros realizados e motoristas.	

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
A3.2. Telemóvel	Utilização de telemóveis de serviço	1	1	Mínimo	– Controlo mensal dos consumos de telemóvel e respetivos *plafonds*, sendo suportado pelo utilizador o montante que exceda o fixado.	
A3.3. Computador pessoal	Utilização de computadores de serviço	1	1	Mínimo	– Normas e procedimentos de afetação e utilização de computadores pessoais. – Utilização sujeita a monitorização e auditoria para efeitos de administração, segurança e garantia de *compliance* relativamente à Política de Segurança de Informação do ML.	
A4. Transferência bancárias / pagamentos *homebaking*						
A4.1. Uso indevido de *password* do sistema	Utilização de sistemas	1	2	Fraco	– GT interdisciplinar no âmbito da cibersegurança para endereçar os desafios desta temática . – Política de Segurança de Informação do ML e formação em *e-learning* obrigatória (com conteúdos definidos internamente e disponibilizada na *intranet*). – O sistema SAP identifica os utilizadores que estão autorizados para o efeito, detendo cada um deles uma chave individual de acesso. – Mecanismos de controlo que permitem identificar o utilizador, o equipamento que foi utilizado, que programas informáticos foram executados, data e horas de utilização. – Outras medidas de segurança da informação (ex.: mudança periódica de *password*, composição da *password*, testes de *phishing* e realização de simulacros de intrusão). – Comunicação interna e formação para incutir a ciberconsciência. – Auditorias periódicas de segurança à infraestrutura de sistemas e tecnologias de informação (intrusão interna e externa).	
A4.2. Autorizações forjadas	Utilização de sistemas	1	2	Fraco	– O sistema SAP identifica os utilizadores que estão autorizados para o efeito, detendo cada um deles uma chave individual de acesso. – Mecanismos de controlo que permitem identificar o utilizador, o equipamento que foi utilizado, que programas informáticos foram executados, data e horas de utilização. – Verificação sistemática de contas.	
A4.3. Conta de destino não autorizada	Utilização de sistemas	1	1	Mínimo	– Cada trabalhador tem associada uma conta bancária, no SAP, onde são creditados mensalmente os seus vencimentos, por transferência bancária, cuja ordem é dada ao banco exclusivamente pela DFI.	
A5. Cheques (incluindo cheques contrafeitos, furto de cheques e falsificação do seu preenchimento)	Utilização de meios de pagamento	1	1	Mínimo	– Controlo pela DPT de valores de indemnizações da Companhia de Seguros pagos por cheque, havendo contas específicas para sua contabilização. – Verificação sistemática de contas.	

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
A6. Fraude na folha salarial						
A6.1. Empregados fantasma	Gestão de recursos humanos	1	1	Mínimo	– Existência de automatismo de controlo e de validação na aplicação informática do SAP. – Acesso restrito aos módulos de inserção/modificação pelos responsáveis pelo processamento salarial. – Execução de análises por amostragem aos recibos de vencimento processados. – Toda a informação que é introduzida nos sistemas de informação necessita de aprovação, pelo menos, por dois níveis de autorização.	
A6.2. Falsificação de horas, salários e subsídios	Controlo de horas e ausências / Processamento de remunerações	1	2	Fraco	– Desmaterialização do sistema de controlo de assiduidade *online* (aplicação *Myteleponto)* – permite a agilização do processo de inserção/alteração de férias e dos respetivos subsídios de férias e a visualização/regularização/aprovação/controlo de irregularidades, com identificação dos aprovadores. – Controlo da assiduidade nas instalações através da picagem de cartão físico e/ou reconhecimento facial/dados biométricos (implementado no PMO III e estações). – Controlo da assiduidade através de picagem no computador para trabalhadores em teletrabalho ou localizados fora das instalações. – Regularização de registo de horas na aplicação *Myteleponto*, resultante de ausências ou outras irregularidades, sujeita a validação da chefia e controlo da DPT. – Aprovação e registo de horas de trabalho suplementar de acordo com o normativo em vigor. – Aplicação SAP de processamento salarial com automatismo que controla eventuais incorreções, com identificação dos responsáveis pelas inserções/modificações no sistema.	– Processo de *follow-up* de implementação das recomendações da auditoria aos adiantamentos em situação de doença e de acidente de trabalho. – Processo de *follow-up* de implementação das recomendações da auditoria aos procedimentos de atribuição de trabalho suplementar. – Alargamento do controlo da assiduidade através do reconhecimento facial/dados biométricos nas restantes instalações do ML. – Implementação de mecanismos de controlo interno pela DPT para confirmação das situações de esquecimento de marcação ou de cartão por parte dos trabalhadores da DEO.
A6.3. Irregularidade no fornecimento de refeições	Gestão dos refeitórios	1	1	Mínimo	– Registo do fornecimento de refeições subsidiadas aos trabalhadores que delas podem beneficiar, através de validação de cartão de trabalhador ou preenchimento de impresso próprio. – Disponibilização da informação das refeições consumidas pelos trabalhadores na aplicação *Myteleponto*. – Procedimento de reserva de refeições e ceias. – Existência na *intranet* de um local reservado a reclamações dos trabalhadores relativos ao funcionamento do refeitório e dos serviços de *vending*.	

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
A6.4. Baixa ou reforma por invalidez fraudulentas	Gestão de recursos humanos	1	2	Fraco	– Programa de visitas domiciliárias para certificação da situação de doença. – Monitorização dos níveis de absentismo na Empresa, em particular nas áreas operacionais/por categoria profissional (com KPI definidos), análise das situações críticas e implementação de medidas de combate ao absentismo.	
A7. Fraude em seguros						
A7.1. Recebimento de indemnizações	Gestão de seguros	1	1	Mínimo	– Controlo interno dos valores das indemnizações por acidente de trabalho pagos pela Companhia de Seguros.	
A7.2. Reembolso de despesas	Gestão de seguros	1	1	Mínimo	– Verificação dos documentos exigidos no âmbito das despesas afetas ao seguro de saúde pela Companhia de Seguros, mediante a utilização de portal ou *app* disponibilizados para o efeito.	
A7.3. Beneficiário fictício	Gestão de seguros	1	1	Mínimo	– Verificação dos documentos exigidos no âmbito das despesas afetas ao seguro de saúde pela Companhia de Seguros, mediante a utilização de portal ou *app* disponibilizados para o efeito. – Verificação e validação do processo de acidente de trabalho.	
A7.4. Alegação fictícia de acidente de trabalho / empolamento de danos pessoais	Gestão de seguros	1	2	Fraco	– Rastreio dos acidentes de trabalho e encaminhamento dos trabalhadores para a Companhia de Seguros. – Exigência da apresentação do relatório médico passado pelos serviços médicos do ML. – Manual de Segurança no Trabalho. – Análise de riscos ocupacionais, enquanto subsistema do risco de "Segurança e saúde no trabalho" do SGR. – Procedimento a adotar em caso de acidente de trabalho. – Procedimentos/metodologia de análise de acidentes de trabalho. Existe uma investigação e análise de acidentes de trabalho graves ou que seja importante implementar medidas. – Campanhas de sensibilização sobre o tema da sinistralidade laboral, através de publicações periódicas na *intranet* e promoção de ações. – Registo em *Compliance* de obrigações decorrentes da segurança e saúde no trabalho.	– Processo de *follow-up* de implementação das recomendações da auditoria aos adiantamentos em situação de doença e de acidente de trabalho. – Revisão da Política de Segurança e Saúde no Trabalho. – Atualização de plano de prevenção de acidentes de trabalho.
A7.5. Alegação fictícia de acidentes automóveis / empolamento de danos	Gestão de seguros	1	1	Mínimo	– Regulamento sobre a utilização de veículos automóveis da frota.	

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
A8. Furto / utilização indevida de existências	Gestão de materiais e armazéns	1	2	Fraco	– Registo e controlo no SAP das entradas e saídas de materiais dos armazéns da Empresa. – Manual de gestão de stock e de reservas no armazém, da DLCP. – Instrução de Trabalho sobre a movimentação de materiais em armazém, da DMC e DEI. – Inventários periódicos aos armazéns. – Videovigilância das instalações. – Controlo periódico das existências mais relevantes para o funcionamento das estações.	– Atualização do sistema de vigilância.
A9. Furto / utilização indevida de ativos fixos tangíveis	Todas as funções e atividades em geral	1	2	Fraco	– Todos os bens são registados e periodicamente inventariados. – Verificação periódica do seu estado de conservação. – Controlos de segurança nas instalações.	
A10. Furto de propriedade intelectual	Todas as funções e atividades em geral	1	2	Fraco	– GT interdisciplinar no âmbito da cibersegurança para endereçar os desafios desta temática. – Existência de Encarregado de Proteção de Dados. – Política de Segurança de Informação do ML e formação em *e-learning* obrigatória (com conteúdos definidos internamente e disponibilizada na *intranet*). – O sistema SAP identifica os utilizadores que estão autorizados para o efeito, detendo cada um deles uma chave individual de acesso. – Mecanismos de controlo que permitem identificar o utilizador, o equipamento que foi utilizado, que programas informáticos foram executados, data e horas de utilização. – Outras medidas de segurança da informação (ex.: mudança periódica de *password*, composição da *password*, testes de *phishing* e realização de simulacros de intrusão). – Comunicação interna e formação para incutir a ciberconsciência. – Auditorias periódicas de segurança à infraestrutura de sistemas e tecnologias de informação (intrusão interna e externa).	– Formalização das Políticas de Segurança de Informação.

Riscos	Função ou Atividade	PO	IP	Nível de risco residual	Medidas de mitigação adotadas	Medidas de mitigação a adotar
A11. Furto / utilização indevida de informação confidencial	Todas as funções e atividades em geral	1	2	Fraco	– Informação confidencial em suporte de papel guardada em local seguro. – GT interdisciplinar no âmbito da cibersegurança para endereçar os desafios desta temática. – Existência de Encarregado de Proteção de Dados. – Política de Segurança de Informação do ML e formação em *e-learning* obrigatória (com conteúdos definidos internamente e disponibilizada na *intranet*). – O sistema SAP identifica os utilizadores que estão autorizados para o efeito, detendo cada um deles uma chave individual de acesso. – Mecanismos de controlo que permitem identificar o utilizador, o equipamento que foi utilizado, que programas informáticos foram executados, data e horas de utilização. – Outras medidas de segurança da informação (ex.: mudança periódica de *password*, composição da *password*, testes de *phishing* e realização de simulacros de intrusão). – Comunicação interna e formação para incutir a ciberconsciência. – Auditorias periódicas de segurança à infraestrutura de sistemas e tecnologias de informação (intrusão interna e externa).	– Formalização de Políticas de Segurança de Informação. – Levantamento de arquivo físico – Implementação do Relatório de Avaliação da Documentação Acumulada (RADA).
A12. Avaliação fraudulenta de ativos						
A12.1 Ativos fixos tangíveis	Compra e venda de ativos fixos tangíveis	1	3	Moderado	– Declarações financeiras anualmente certificadas por uma sociedade de ROC e objeto de parecer por parte do CF/FU.	
A12.2 Propriedades de investimento	Compra e venda de propriedades de investimento	1	3	Moderado	– Realização de avaliações externas de alguns ativos e passivos. – Cumprimento da legislação relativa à compra e venda de imóveis do Setor Público Empresarial. – Declarações financeiras anualmente certificadas por uma sociedade de ROC e objeto de parecer por parte do CF/FU.	– Inventariação e controlo de bens de investimento.
A12.3 Aplicações / Produtos financeiros	Compra e venda de produtos financeiros	1	1	Mínimo	– O ML não tem autonomia para adquirir ou vender produtos financeiros, sendo efetuado via IGCP.	

Anexo 2 – Matriz de risco

Estão, assim, identificados e avaliados 53 riscos de corrupção e infrações conexas no contexto do ML e empresas participadas com maioria de capital, que estão distribuídos da seguinte forma na matriz de risco.

		Probabilidade de Ocorrência (PO)		
		Baixa	**Média**	**Alta**
Impacto Previsível (IP)	**Baixo**	Mínimo – 17 riscos C1.2, C2.7.2 A1.1.1, A1.4, A2, A3.1 A3.2, A3.3, A4.3, A5, A6.1, A.6.3, A7.1, A7.2, A7.3, A7.5, A12.3	Fraco	Moderado
	Médio	Fraco – 24 riscos C1.1, C2.4, C2.6, C2.8, C2.11, C2.14, C2.15 M1.1, M1.2, M1.3, M2.1, M2.2 A1.1.2, A1.2, A1.3, A4.1, A4.2, A6.2, A6.4, A7.4, A8, A9, A10, A11	Moderado	Elevado
	Alto	Moderado – 11 riscos: C2.1, C2.2, C2.5, C2.7.1, C2.9, C2.10, C2.12, C2.13.1, C2.13.2 A12.1, A12.2	Elevado – 1 risco C2.3	Máximo

Destacam-se 11 riscos com nível residual moderado:

- C2.1. Corrupção passiva ou conflitos de interesse – Deliberações / aprovações / orientações estratégicas, operacionais, financeiras e de *compliance;*
- C2.2. Corrupção passiva ou conflitos de interesse – Elaboração de estudos/projetos e organização de processos;
- C2.5. Corrupção passiva ou conflitos de interesse – Processos judiciais e disciplinares / contencioso / falsos testemunhos / tratamento de denúncias / assessoria/pareceres jurídicos;
- C2.7.1. Corrupção passiva ou conflitos de interesse – Aplicação de penalidades (coimas / multas) a fornecedores e prestadores de serviço;
- C2.9. Corrupção passiva ou conflitos de interesse – Sobrefaturação / gestão contratual (de bens, serviços e EOP, incluindo serviços / trabalhos a mais);
- C2.10. Corrupção passiva ou conflitos de interesse – Atribuição de indemnizações / acordos;
- C2.12. Corrupção passiva ou conflitos de interesse – Extorsão económica;
- C2.13.1. Corrupção passiva ou conflitos de interesse – Facilitação de acesso indevido (para ato criminoso, incluindo terrorista ou vantagem): Instalações;

- C2.13.2. Corrupção passiva ou conflitos de interesse – Facilitação de acesso indevido (para ato criminoso, incluindo terrorista ou vantagem): Sistemas e tecnologias da informação e da operação;
- A12.1. Corrupção passiva ou conflitos de interesse – Avaliação fraudulenta de ativos: Ativos fixos tangíveis;
- A12.2. Apropriação indevida de ativos – Avaliação fraudulenta de ativos: Propriedades de investimento.

Existe apenas 1 risco com nível residual elevado:

- C2.3. Corrupção passiva ou conflitos de interesse – Aquisição de bens, serviços e EOP (incluindo seleção de procedimento, adjudicações diretas, definição de especificações, elaboração de contratos, avaliação de propostas e seleção de fornecedores).

Anexo 3 – Corrupção e Infrações conexas no RGPC

O quadro seguinte apresenta as definições de corrupção e infrações conexas previstas no RGPC[18]:

Crimes previstos pelo Decreto-Lei n.º 48/95, de 15 de março (Código Penal) com as subsequentes alterações Aplicável a funcionários e trabalhadores de entidades e organizações do setor público, de natureza pública ou que, de algum modo, exerçam atividades, no todo ou em parte, que sirvam o interesse público ou que beneficiem de apoios públicos.		
Crime	**Definição legal e quadro punitivo**	**Exemplos ilustrativos de situações práticas**
Da corrupção	**Recebimento ou oferta indevidos de vantagem (art.º 372º)** *1 – O funcionário que, no exercício das suas funções ou por causa delas, por si, ou por interposta pessoa, com o seu consentimento ou ratificação, solicitar ou aceitar, para si ou para terceiro, vantagem patrimonial ou não patrimonial, que não lhe seja devida, é punido com pena de prisão até cinco anos ou com pena de multa até 600 dias.* *2 – Quem, por si ou por interposta pessoa, com o seu consentimento ou ratificação, der ou prometer a funcionário, ou a terceiro por indicação ou conhecimento daquele, vantagem patrimonial ou não patrimonial, que não lhe seja devida, no exercício das suas funções ou por causa delas, é punido com pena de prisão até três anos ou com pena de multa até 360 dias.* *3 – Excluem-se dos números anteriores as condutas socialmente adequadas e conformes aos usos e costumes.*	Quando um dirigente ou outro trabalhador de uma organização, no exercício das suas funções, solicita ou recebe de outra pessoa, direta ou indiretamente, um bem patrimonial ou financeiro que não lhe é devido e que é suscetível de condicionar os seus deveres de integridade e isenção.
	Corrupção Passiva (art.º 373º) *1 – O funcionário que por si, ou por interposta pessoa, com o seu consentimento ou ratificação, solicitar ou aceitar, para si ou para terceiro, vantagem patrimonial ou não patrimonial, ou a sua promessa, para a prática de um qualquer acto ou omissão contrários aos deveres do cargo, ainda que anteriores àquela solicitação ou aceitação, é punido com pena de prisão de um a oito anos.* *2 – Se o acto ou omissão não forem contrários aos deveres do cargo e a vantagem não lhe for devida, o agente é punido com pena de prisão de um a cinco anos.*	Quando um dirigente ou outro trabalhador de uma organização solicita ou recebe um suborno, ou a sua promessa, em troca de tomar uma decisão, no âmbito das suas funções, que beneficie indevidamente quem o subornou.
	Corrupção Ativa (art.º 374º) *1 – Quem, por si ou por interposta pessoa, com o seu consentimento ou ratificação, der ou prometer a funcionário, ou a terceiro por indicação ou com conhecimento daquele, vantagem patrimonial ou não patrimonial com o fim indicado no n.º 1 do artigo 373.º, é punido com pena de prisão de um a cinco anos.* *2 – Se o fim for o indicado no n.º 2 do artigo 373.º, o agente é punido com pena de prisão até três anos ou com pena de multa até 360 dias.* *3 – A tentativa é punível.*	Quando um dirigente ou outro trabalhador dá ou promete determinada vantagem, em troca de serem tomadas certas decisões a seu favor.
Do peculato	**Peculato (art.º 375º)** *1 – O funcionário que ilegitimamente se apropriar, em proveito próprio ou de outra pessoa, de dinheiro ou qualquer coisa móvel ou imóvel ou animal, públicos ou particulares, que lhe tenha sido entregue, esteja na sua posse ou lhe seja acessível em razão das suas funções, é punido com pena de prisão de 1 a 8 anos, se pena mais grave lhe não couber por força de outra disposição legal.*	Quando um dirigente ou outro trabalhador de uma organização se apropria de bens ou valores patrimoniais pertencentes à organização onde exerce funções.

[18] Cfr. art. 3.º.

	2 – Se os valores ou objectos referidos no número anterior forem de diminuto valor, nos termos da alínea c) do artigo 202.º, o agente é punido com pena de prisão até 3 anos ou com pena de multa. *3 – Se o funcionário der de empréstimo, empenhar ou, de qualquer forma, onerar valores ou objectos referidos no n.º 1, é punido com pena de prisão até 3 anos ou com pena de multa, se pena mais grave lhe não couber por força de outra disposição legal.*	
	Peculato de uso (art.º 376º) *1 – O funcionário que fizer uso ou permitir que outra pessoa faça uso, para fins alheios àqueles a que se destinem, de coisa imóvel, de veículos, de outras coisas móveis ou de animais de valor apreciável, públicos ou particulares, que lhe forem entregues, estiverem na sua posse ou lhe forem acessíveis em razão das suas funções, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.* *2 – Se o funcionário, sem que especiais razões de interesse público o justifiquem, der a dinheiro público destino para uso público diferente daquele a que está legalmente afectado, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.*	Quando um dirigente ou outro trabalhador de uma organização utiliza em seu favor, ou autoriza a que terceiros o façam, bens patrimoniais, equipamentos ou valores, materiais ou financeiros, pertencentes à organização onde exercem funções ou que se encontram à sua guarda.
	Participação económica em negócio (art.º 377º) *1 – O funcionário que, com intenção de obter, para si ou para terceiro, participação económica ilícita, lesar em negócio jurídico os interesses patrimoniais que, no todo ou em parte, lhe cumpre, em razão da sua função, administrar, fiscalizar, defender ou realizar, é punido com pena de prisão até 5 anos.* *2 – O funcionário que, por qualquer forma, receber, para si ou para terceiro, vantagem patrimonial por efeito de acto jurídico-civil relativo a interesses de que tinha, por força das suas funções, no momento do acto, total ou parcialmente, a disposição, administração ou fiscalização, ainda que sem os lesar, é punido com pena de prisão até 6 meses ou com pena de multa até 60 dias.* *3 – A pena prevista no número anterior é também aplicável ao funcionário que receber, para si ou para terceiro, por qualquer forma, vantagem patrimonial por efeito de cobrança, arrecadação, liquidação ou pagamento que, por força das suas funções, total ou parcialmente, esteja encarregado de ordenar ou fazer, posto que não se verifique prejuízo para a Fazenda Pública ou para os interesses que lhe estão confiados.*	Quando um dirigente ou outro trabalhador de uma organização, no exercício das suas funções, toma decisões que beneficiem um determinado interesse particular, do próprio ou de terceiro, lesando o interesse ou provocando prejuízos para a organização ou entidade.
Do abuso de autoridade	**Concussão (art.º 379º)** *1 – O funcionário que, no exercício das suas funções ou de poderes de facto delas decorrentes, por si ou por interposta pessoa com o seu consentimento ou ratificação, receber, para si, para o Estado ou para terceiro, mediante indução em erro ou aproveitamento de erro da vítima, vantagem patrimonial que lhe não seja devida, ou seja superior à devida, nomeadamente contribuição, taxa, emolumento, multa ou coima, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias, se pena mais grave lhe não couber por força de outra disposição legal.* *2 – Se o facto for praticado por meio de violência ou ameaça com mal importante, o agente é punido com pena de prisão de 1 a 8 anos, se pena mais grave lhe não couber por força de outra disposição legal.*	Quando um dirigente ou outro trabalhador de uma organização, no exercício das suas funções, se apropria de um valor ou bem patrimonial que não seja devido, e cuja existência decorra de um erro circunstancial ou que tenha sido por si deliberadamente induzido.

	Abuso de poder (art.º 382º) *O funcionário que, fora dos casos previstos nos artigos anteriores, abusar de poderes ou violar deveres inerentes às suas funções, com intenção de obter, para si ou para terceiro, benefício ilegítimo ou causar prejuízo a outra pessoa, é punido com pena de prisão até 3 anos ou com pena de multa, se pena mais grave lhe não couber por força de outra disposição legal.*	Quando um dirigente ou outro trabalhador de uma organização se prevalece do poder funcional de que dispõe para satisfação indevida de interesses próprios ou de terceiros.
Crimes Conexos	**Tráfico de influência (art.º 335º)** *1 - Quem, por si ou por interposta pessoa, com o seu consentimento ou ratificação, solicitar ou aceitar, para si ou para terceiro, vantagem patrimonial ou não patrimonial, ou a sua promessa, para abusar da sua influência, real ou suposta, junto de qualquer entidade pública, nacional ou estrangeira, é punido: a) Com pena de prisão de 1 a 5 anos, se pena mais grave lhe não couber por força de outra disposição legal, se o fim for o de obter uma qualquer decisão ilícita favorável; b) Com pena de prisão até 3 anos ou com pena de multa, se pena mais grave lhe não couber por força de outra disposição legal, se o fim for o de obter uma qualquer decisão lícita favorável.* *2 - Quem, por si ou por interposta pessoa, com o seu consentimento ou ratificação, der ou prometer vantagem patrimonial ou não patrimonial às pessoas referidas no número anterior: a) Para os fins previstos na alínea a), é punido com pena de prisão até 3 anos ou com pena de multa; b) Para os fins previstos na alínea b), é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.* *3 - A tentativa é punível.* *4 - É correspondentemente aplicável o disposto no artigo 373.º-B.*	Quando alguém solicitar ou receber um bem ou valor material ou financeiro em troca de mover as suas influências junto de uma entidade ou serviço publico tendo em vista um determinado propósito ilícito dessa entidade ou serviço.
	Branqueamento (art.º 368º-A) *1 - ...* *2 - ...* *3 - Quem converter, transferir, auxiliar ou facilitar alguma operação de conversão ou transferência de vantagens, obtidas por si ou por terceiro, direta ou indiretamente, com o fim de dissimular a sua origem ilícita, ou de evitar que o autor ou participante dessas infrações seja criminalmente perseguido ou submetido a uma reação criminal, é punido com pena de prisão até 12 anos.* *4 - Na mesma pena incorre quem ocultar ou dissimular a verdadeira natureza, origem, localização, disposição, movimentação ou titularidade das vantagens, ou os direitos a ela relativos.* *5 - Incorre ainda na mesma pena quem, não sendo autor do facto ilícito típico de onde provêm as vantagens, as adquirir, detiver ou utilizar, com conhecimento, no momento da aquisição ou no momento inicial da detenção ou utilização, dessa qualidade.* *6 - ...*	Quando alguém procede de modo intencional para ocultar a origem ilícita de bens e valores patrimoniais, financeiros ou materiais.