COMBOIOS DE PORTUGAL

Auditoria Interna

Relatório de Execução Anual 2022 do Plano de Gestão de Riscos 2022-2023

2022/000682
DMS 784902

Dezembro 2022

EMPRESA CERTIFICADA eiC ISO 9001

Mod_10-001

GLOSSÁRIO

AI	AUDITORIA INTERNA
CA	CONSELHO DE ADMNISTRAÇÃO
CP	COMBOIOS DE PORTUGAL, EPE
CSP	CONTRATO DE SERVIÇO PÚBLICO
PGR	PLANO DE GESTÃO DE RISCOS
PPR	PLANO DE PREVENÇÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS
SGQ	SISTEMA DE GESTÃO DA QUALIDADE

ÍNDICE

1- Introdução

A gestão do risco empresarial abrange um conjunto de práticas para identificar, medir, tratar e reportar os principais riscos a que cada unidade orgânica está exposta, de acordo com as boas práticas internacionais de governação e em conformidade com os requisitos legais e regulamentares. Esta prática integra a postura de gestão que a CP espera de todos, no sentido de corresponder às necessidades e expetativas dos diversos interessados na empresa, de forma a permitir o seu crescimento e a proteção dos seus trabalhadores e outros *stakeholders*, bens, resultados e reputação.

Princípios orientadores da gestão do risco empresarial da CP:

- A gestão do risco empresarial é um processo abrangente e sistematizado, no qual os riscos são continuamente identificados, analisados e conscientemente aceites, aumentados ou mitigados dentro das tolerâncias ao risco aprovadas. Deve tomar em consideração os riscos estratégicos, operacionais, de segurança, financeiros, de conformidade, bem como todos os outros riscos que, em face da situação concreta da CP, se possam materializar. O esforço na sua prevenção deve ser proporcional à dimensão, natureza e complexidade da atividade tomando em consideração a natureza e magnitude dos riscos assumidos;
- A gestão do risco deve fazer parte das atividades correntes diárias da CP e ser partilhado pelos trabalhadores e outros *stakeholders*, os quais devem conhecer os riscos na sua área de atuação e geri-los de acordo com as políticas, regulamentos e tolerâncias ao risco aprovadas;
- A gestão do risco está intimamente ligada à estratégia, missão e visão da CP, incidindo particularmente sobre os riscos que as possam pôr em causa. Os riscos significativos devem ser geridos numa perspetiva de portfólio integrado, transversalmente a todos os seus negócios, de forma a maximizar os benefícios desse conhecimento e permitir que a exposição a riscos locais esteja suportada pelos objetivos globais da empresa;
- A gestão do risco suporta os sistemas de gestão da empresa, nomeadamente o referencial da NP EN ISO 9001, devendo estar integrada nos processos de negócio da CP, abrangendo atividades, sistemas e equipamentos de suporte, estando presente na tomada de decisão e investimentos;
- A gestão do risco deve ser planeada, revista e documentada. A comunicação interna e externa dos riscos constitui, por si só, um fator de sucesso da gestão do risco global da empresa. As políticas e procedimentos locais de gestão do risco deverão ser consistentes

com estes princípios, devendo facilitar a agregação, consolidação e revisão a nível corporativo de todos os riscos significativos.

O presente documento visa, entre outros normativos, dar resposta às disposições do Código das Sociedades Comerciais, ao Estatuto do Gestor Público, aos Princípios do Bom Governo das Empresas do Sector Empresarial do Estado, ao Decreto-Lei n.º 133/2013, de 3 de outubro e aos sistemas de gestão da Empresa suportados pela Gestão do Risco.

2- Objeto

O presente relatório tem por objeto descrever não só a execução do Plano de Ações do Plano de Gestão de Riscos 2022-2023 da CP (PGR), referente ao ano de 2022, bem como a identificação de outras recomendações de melhoria.

3- Controlo interno e estrutura orgânica da CP

Conforme estabelecido nos princípios de bom governo das empresas do Setor Empresarial do Estado, em Resolução do Conselho de Ministros nº 49/2007, a CP mantém estruturas de administração e fiscalização ajustadas à sua dimensão e realidade, possibilitando a segregação efetiva de funções de administração.

Cabe ao Conselho de Administração (CA) criar e manter um sistema de controlo interno abrangendo todas as atividades geradoras de riscos relevantes. Cabe ao Revisor Oficial de Contas, como órgão de fiscalização, o papel de verificação da eficácia da estrutura de gestão do risco. Cabe às entidades e órgãos com responsabilidade de auditoria, com destaque para a Auditoria Interna (AI), verificar a eficácia dos mecanismos de controlo interno exercendo essa atividade com independência e objetividade. O plano anual de auditoria da CP é elaborado tendo em consideração os riscos identificados no PGR, as preocupações do CA, dos responsáveis dos órgãos da CP, das empresas participadas e das entidades de fiscalização.

A independência e objetividade da AI é garantida pela dependência direta do CA, sem qualquer relação de dependência hierárquica ou funcional relativamente aos serviços auditados. A estrutura organizativa da empresa (figura 1) estabelece de forma clara um conjunto de funções de suporte e de funções de negócio, atribuindo-lhes a respetiva missão e responsabilidades.

Para além das normas legais aplicáveis, as relações que se estabelecem entre as Unidades Orgânicas da Empresa e entre estas e os seus trabalhadores, bem como o contacto com

clientes e fornecedores assentam nomeadamente, num conjunto de princípios e valores, que estão vertidos no Código de Ética da CP. O código de ética aborda, para além destes valores fundamentais, especificamente os aspetos de conflitos de interesse.

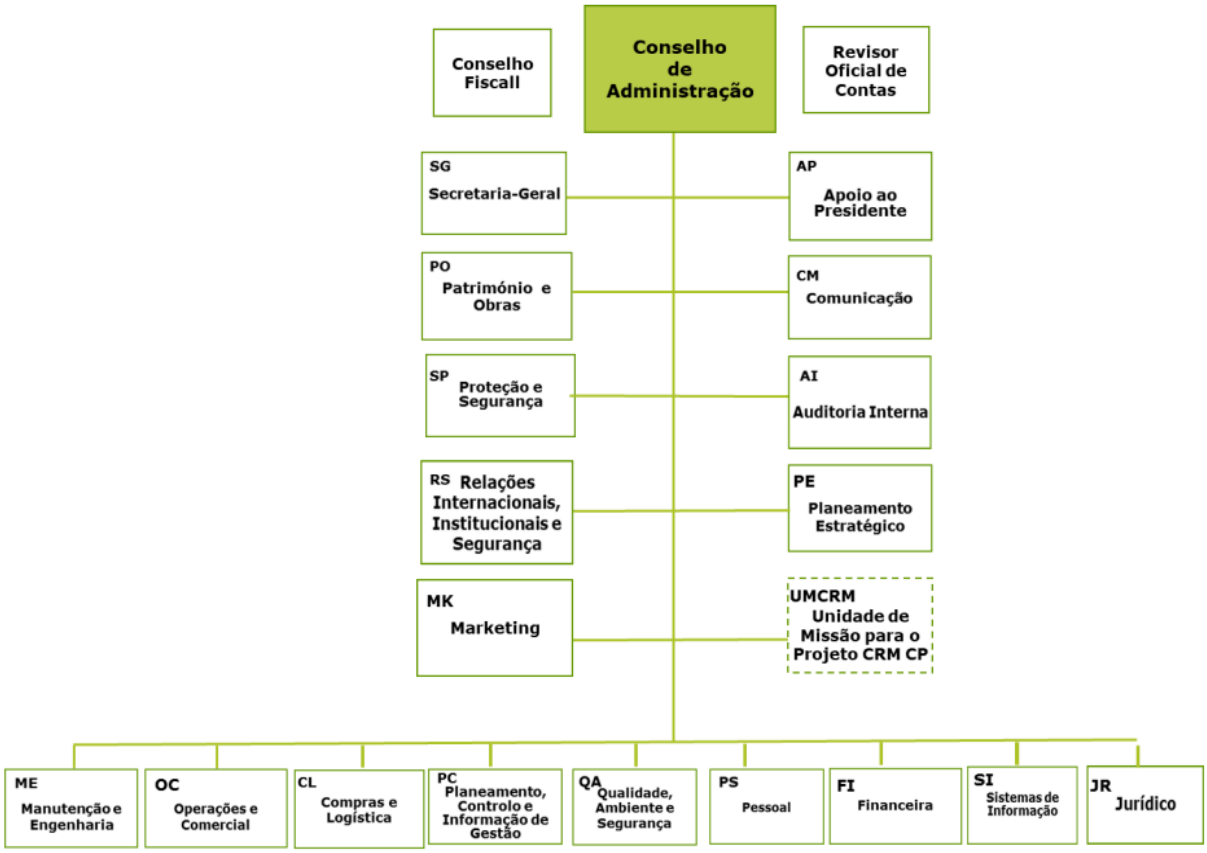

Figura 1 – Organograma Geral da CP (2022).

4- Responsabilidades

A política de gestão do risco empresarial da CP refere que o esforço de gestão do risco deve fazer parte das atividades correntes diárias da CP e ser partilhado pelos trabalhadores, os quais devem conhecer os riscos na sua área de atuação e geri-los de acordo com as políticas, regulamentos e tolerâncias ao risco aprovadas.

O PGR requer que seja explicitamente atribuída a responsabilidade pela gestão dos riscos. Essa designação pode ser nominal, referindo explicitamente um elemento ou um conjunto de elementos nomeados em grupo de trabalho sendo, no entanto, usual a designação de uma sigla de Unidade Orgânica. Ao designar uma Unidade Orgânica na coluna Responsáveis de cada tabela, sem outra menção, assume-se que o "gestor de risco" é o responsável máximo dessa mesma Unidade Orgânica.

Numa lógica mais abrangente, considera-se que os responsáveis designados na coluna Responsáveis de cada tabela devem ser os gestores dos processos/subprocessos de negócio onde os riscos foram identificados. Cabe aos gestores de cada processo ou subprocesso analisar as causas dos respetivos riscos e elaborar planos de ação com o nível de formalismo adequado ao nível do risco, abrangendo as medidas que tencionam implementar para a sua mitigação.

No sentido de apoiar a realização das ações de gestão do risco, cada órgão indica um ou mais representantes que colaboram na realização do PGR e noutras ações neste âmbito. Esta prática está instituída pelo Sistema de Gestão da Qualidade (SGQ) da CP, enquadrando o requisito de gestão do risco.

5- Metodologia de Identificação de riscos

O desenvolvimento do processo de gestão do risco do PGR da CP tem como principal orientação a metodologia definida na norma de referência NP ISO 31000:2018 - Gestão do Risco - Linhas de orientação. Segundo este referencial o processo de gestão do risco deve contemplar um conjunto de atividades, que incluem a comunicação e consulta, estabelecimento do contexto e a apreciação, tratamento, monitorização e revisão, registo e reporte do risco.

Em 2022 foram identificados no PGR 457 riscos dos quais 291 são de nível de risco baixo, 112 são de nível de risco médio e 54 são de nível elevado, constituindo um perfil de risco desafiante para a gestão, nomeadamente porque uma parte significativa dos riscos elevados é atribuível direta ou indiretamente a fatores de risco do contexto externo da CP de mitigação complexa. O tratamento específico destes riscos está associado às medidas de mitigação constantes do Plano.

Este perfil de risco contrasta com o do Plano de Prevenção de Riscos, mais centrado em fatores de risco interno onde, na primeira versão, não foram identificados riscos elevados.

6- Execução do Plano de Ação

O PGR da CP estabelece, no capítulo IX, um conjunto de ações de desenvolvimento metodológico da gestão de risco, para o período 2022-2023. Apresenta-se, em seguida, o estado de execução dessas ações, para o ano de 2022:

A1 - Desenvolvimento de recursos organizacionais que dão suporte à conformidade com a Resolução do Conselho de Ministros n.º 37/2021, de 6 de abril, que aprova a Estratégia Nacional Anticorrupção 2020-2024, com o Decreto-Lei n.º 109-E/2021, de 9 de dezembro, que cria o Mecanismo Nacional Anticorrupção e estabelece o regime geral de prevenção da corrupção, e com a Lei n.º 93/2021, de 20 de dezembro, que estabelece o regime geral de proteção de denunciantes de infrações.

Execução

Esta medida foi realizada através das seguintes ações:

- Implementação de medidas de conformidade, na sequência de Relatório de diagnóstico de "Compliance", por Entidade Externa, relativo às práticas adotadas na CP no que diz respeito às áreas:

  (a) Governo societário e responsabilidade social e desenvolvimento sustentável;

  (b) Sistema de gestão de riscos, em particular de anticorrupção e infrações conexas;

  (c) "Compliance" laboral.
- Nomeação do Responsável pelo Cumprimento Normativo;
- Implementação do Plano de Prevenção de Riscos de corrupção e infrações conexas (PPR);
- Disponibilização de canal para Whistleblowing
- Certificação segundo a Norma Portuguesa 4427: 2018 – Sistemas de Gestão das Pessoas, envolvendo nomeadamente:

  (a) Estabelecimento da Política de Gestão das Pessoas, implementação dos requisitos e definição de objetivos suportados por planos de atividade específicos, que permitam avaliar a aplicação e desenvolvimento da NP 4427;

  (b) Formação e sensibilização dos trabalhadores.

A2 - Desenvolvimento de recursos organizacionais que dão suporte à conformidade com o Decreto-Lei 65/2021, de 30 julho, que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019, incluindo ações de formação e sensibilização para reforço da compreensão de medidas de proteção e boas práticas.

Execução

Esta medida foi realizada através das seguintes ações:

- Cooperação institucional com parceiros da CP no âmbito da proteção de dados e da cibersegurança, nomeadamente o Centro Nacional de Cibersegurança (CNCS), o Gabinete Nacional de Segurança (GNS) e o Instituto da Defesa Nacional (IDN);
- Alertar para a utilização de esquemas fraudulentos efetuados com recursos a práticas de engenharia social, através de documento interno (Cibersegurança e Ciberhigiene – Práticas de engenharia social) divulgado a todos os trabalhadores da Empresa, com um conjunto de regras de proteção visando a utilização em segurança das diferentes funcionalidades do mundo digital e mantendo a privacidade dos seus dados;
- Publicação do Regulamento do Teletrabalho, em abril de 2022, que inclui orientações sobre proteção de dados pessoais e segurança da informação;
- Ações específicas de eLearning sobre fatores de risco relevantes em Cibersegurança e Ciberhigiene disponíveis para todos os trabalhadores.

A3 - Desenvolvimento de ações de recursos organizacionais com vista à melhoria do acompanhamento do portfólio de projetos da CP.

Execução

Esta medida foi realizada através de formação e sensibilização sobre Gestão de Projetos nomeadamente com as ações:

- Formação em Workshop Project Management – Top Management – destinada às chefias de primeiro nível e ao CA, tendo sido ministrada a 30 responsáveis da CP;
- Formação em Project Management – Gestores de Projeto | Equipas, tendo sido ministrada a 58 quadros técnicos da CP.

A4 - Desenvolvimento do PGR em áreas que requerem maior detalhe ao nível dos riscos.

Execução

O desenvolvimento do PGR foi realizado aprofundando o nível de detalhe da informação recolhida diretamente junto dos responsáveis e em sede de auditorias, nomeadamente nas áreas de segurança da informação e de gestão de armazéns associados ao material circulante, permitindo um conhecimento mais apurado do perfil de risco.

Na sequência da elaboração do Plano de Prevenção de Riscos de corrupção e infrações conexas da CP, documento complementar ao PGR, procedeu-se à autonomização desta tipologia de riscos, cujo desenvolvimento fica a cargo do Responsável pelo Cumprimento Normativo da CP. Este novo Plano tem, na sua primeira versão, uma metodologia compatível com o PGR.

A5 - Reformulação metodológica do PGR com as recomendações das auditorias externa e interna da qualidade.

O PGR sofreu uma significativa evolução metodológica com a inclusão de novos elementos de informação:

- **Categoria** do risco (Reputação, Económico, Jurídico, Operacional, Financeiro), permitindo compreender a natureza do seu impacto e facilitar o enquadramento na lista de principais riscos da CP;
- **Impacto qualitativo**, permitindo estabelecer de forma mais objetiva as consequências da não mitigação do risco;
- **Risco residual**, permitindo separar a perceção entre o risco não mitigado e o risco após mitigação.

A6 - Realização de plano de auditoria baseada no risco, com maior orientação das ações para riscos relevantes da organização.

Esta medida foi realizada através de:

- associação dos riscos significativos identificados no PGR, a cada uma das auditorias previstas no Programa de Auditoria anual;
- auditorias de avaliação de controlos, destacando-se os controlos de receita e de execução contratual.

A7 - Publicação e divulgação do PGR e do Relatório Anual de Execução do PGR, nomeadamente através de comunicação interna, publicação na Intranet e na Internet, publicação na Unidade Técnica (PC) e informação a interessados.

O PGR e o Relatório são disponibilizados na Intranet da CP e no site institucional da CP (Internet). É ainda disponibilizada informação ao Tribunal de Contas, à Comissão do Mercado de Valores Mobiliários (CMVM), ao Conselho Fiscal, ao Revisor Oficial de Contas (ROC), ao Auditor Externo, à Direção-Geral do Orçamento (DGO) no Sistema de Informação de Gestão Orçamental (SIGO em https://sigo.gov.pt/sigoRoot/sigo/default.jsp), à Direção-Geral do Tesouro e Finanças (DGTF) no Sistema de Recolha de Informação Económica e Financeira (SIRIEF em https://www.xbrlemportugal.pt/sirief.htm), no Site do Sector Empresarial do Estado (SEE em http://www.dgtf.pt/sector-empresarial-do-estado-see/informacao-sobre-as-empresas/entity/cp--comboios-de-portugal-epe), à Secretaria de Estado das Infraestruturas (SEI) no System Operating Reporting (SOR em http://www.sor.gov.pt/) do Ministério com o pelouro dos transportes e à Unidade Técnica de Acompanhamento e Monitorização do Setor Público Empresarial (UTAM em https://www.utam.gov.pt/) do Ministério das Finanças.

Para além das ações de caráter metodológico acima descritas, a empresa executou um conjunto de ações destinadas a mitigar fatores de risco significativos, nomeadamente:

- Migração para GSM-R (sistema de comunicação interoperável europeu) de equipamentos rádio solo-comboio, visando mitigar problemas de fiabilidade na comunicação entre o material circulante e a infraestrutura, ao longo da marcha dos comboios;
- Modernização de carruagens Arco e reabilitação de locomotivas LE2600, com o intuito de atenuar as limitações na oferta de serviço;
- Substituição de faróis frontais no material circulante de forma a melhorar a visibilidade para o maquinista e para a envolvente da infraestrutura ferroviária;
- Beneficiação de oficinas endereçando limitações na capacidade de manutenção e reparação de material circulante;
- Beneficiação de parques de material circulante abordando riscos de eficiência das operações e proteção de equipamentos;

- Recrutamento de pessoal para categorias profissionais essenciais para a continuidade da prestação do serviço, contribuindo para debelar problemas de falta de efetivo e elevada média etária.

7- Conclusões

As medidas constantes do PGR de 2022-2023 foram já largamente implementadas, dando cumprimento aos requisitos legais e normativos, gerando benefícios significativos para a empresa, existindo um conjunto de medidas em curso com o objetivo de melhorar o perfil de risco da CP. Destaca-se nomeadamente a integração do PGR como elemento agregador do sistema de gestão do risco, a evolução no paradigma da auditoria baseada no risco e o suporte aos sistemas de gestão da empresa.

8- Recomendações

O PGR da CP abrange já uma tipologia significativa de riscos. O Plano poderá, no entanto, ser melhorado com o reconhecimento de novos fatores de risco. A eficácia do acompanhamento do comportamento de cada risco poderá beneficiar de um melhor conhecimento dos respetivos controlos, pelo que se propõe uma melhor tipificação desses recursos.

Pretende-se também continuar a melhorar a identificação dos riscos de forma integrada, nomeadamente os inerentes ao Contrato de Serviço Público, bem como aprofundar os dos diferentes projetos em curso na CP.

Por forma a tornar a Gestão do Risco mais eficiente é desejável a implementação de ferramentas tecnológicas de gestão de riscos, que automatizem o processo.