COMBOIOS DE PORTUGAL

Auditoria Interna

Relatório de Execução Anual do Plano de Gestão de Riscos 2024-2025

Ano 2024

2023/000395
DMS 821834

Portaria 39/2019: 150.20.302

janeiro 2025

EMPRESA CERTIFICADA eiC ISO 9001

Mod_10-001

GLOSSÁRIO

AI	AUDITORIA INTERNA
CA	CONSELHO DE ADMNISTRAÇÃO
CP	COMBOIOS DE PORTUGAL, EPE
PGR	PLANO DE GESTÃO DE RISCOS

ÍNDICE

1- Introdução

A gestão do risco empresarial abrange um conjunto de práticas para identificar, medir, tratar e reportar os principais riscos a que a CP 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, por cada unidade orgânica, 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.

2- Objeto

O presente documento visa dar resposta, entre outros normativos, 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.

Este relatório tem por objeto descrever não só a execução do Plano de Ações do Plano de Gestão de Riscos 2024-2025 da CP (PGR), referente ao ano de 2024, 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.

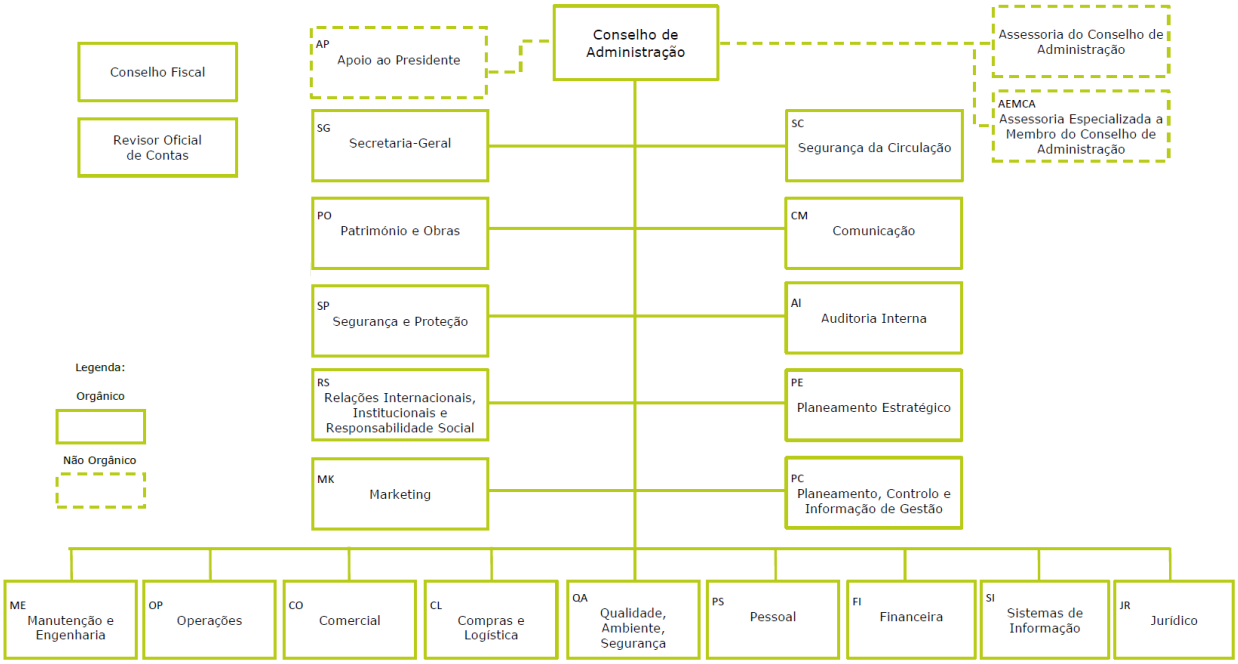

Figura 1 – Organograma Geral da CP (fev.2024).

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 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.

A responsabilidade pela gestão dos riscos está atribuída ao responsável máximo de cada unidade orgânica, identificada na coluna "Responsável" pela respetiva sigla.

No sentido de apoiar a realização das ações de gestão do risco, cada órgão indica um ou mais representantes que colaboram na realização deste documento e noutras ações neste âmbito. Esta prática está instituída nomeadamente pelo sistema de gestão da qualidade, enquadrando o requisito de gestão do risco, pelo sistema de gestão do ambiente, pelo sistema de gestão de segurança, pela equipa de proteção de dados pessoais, identificando elementos que prestam apoio aos responsáveis de cada órgão na compilação, atualização e divulgação de informação junto dos seus colegas.

Cabe aos responsáveis dos respetivos órgãos, em interlocução com os representantes nomeados, analisar as causas dos respetivos riscos e elaborar planos de ação com o formalismo adequado ao nível do risco, abrangendo as medidas que tencionam implementar para a sua mitigação.

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.

Relativamente a 2024, foram identificados no PGR 455 riscos, dos quais 283 são de nível baixo, 149 de nível médio e 23 de nível elevado, a que corresponde a distribuição 62%, 33% e 5% respetivamente, 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.

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 2024-2025. Apresenta-se, em seguida, o estado de execução dessas ações, para o ano de 2024:

A1 - Realização de ações de formação sobre a aplicação da metodologia de gestão de riscos empresariais na CP, para sensibilização de trabalhadores em particular os envolvidos na elaboração do Plano de Gestão de Riscos (PGR) e elementos de equipas de projeto.

Execução

Esta medida foi concretizada através da realização, em 26, 29 e 31 janeiro, de uma ação de formação específica para os Representantes de Gestão do Risco, aberta a todos os responsáveis, sob os temas Gestão do Risco Empresarial – Conceito e Prática e Plano de Prevenção de Riscos de Corrupção e Infrações Conexas (PPR), atualizando os formandos relativamente aos referenciais normativos e à metodologia de elaboração do PGR e PPR.

A2 - Implementação de comunicações periódicas internas para sensibilização sobre aspetos e práticas de gestão do risco, nomeadamente sobre os riscos globais de natureza externa com peso crescente na atividade empresarial.

Execução

Esta medida foi realizada através da publicação mensal, iniciada em abril de 2024, de uma newsletter centrada nos riscos globais que influenciam a empresa e o seu contexto, num total de nove edições.

A4 - 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, para reforço de medidas de proteção e boas práticas.

Execução

O desenvolvimento desta ação foi realizado, nomeadamente através de:

- Continuidade dos trabalhos de revisão das políticas e normas de segurança da CP, com o recurso a equipa multidisciplinar, no seguimento da aprovação pelo CA, em outubro de 2023, da Política Geral de Segurança da Informação, alinhada com a norma NP ISO27001, a fim de melhor preparar a CP para os novos requisitos da Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 (Diretiva SRI 2NIS2) (NIS2), ainda em processo de transposição para a legislação nacional;
- Melhoria dos meios de segurança do datacenter, na sequência da sua relocalização;

- Ações de sensibilização presencial em cibersegurança, cibercrime e ciberhigiene para 48 formandos.

A5 - Desenvolvimento e implementação de recursos organizacionais com vista à melhoria do acompanhamento do portfólio de projetos da CP.

Execução

O desenvolvimento desta ação foi efetuado nomeadamente através de:

- Apresentação institucional dos projetos estratégicos, por parte das respetivas equipas de projeto;
- Consolidação da aplicação da metodologia de gestão de projetos por parte das equipas de projeto, nomeadamente com envio sistemático de Relatórios de Status para melhor acompanhamento por parte do CA e do Planeamento Estratégico da CP;
- Maior formalização do risco associado aos projetos estratégicos.

A6 - Desenvolvimento do âmbito do PGR para dar resposta a novos requisitos.

Execução

O âmbito do PGR foi incrementado através do desenvolvimento da área de sustentabilidade, compliance e projetos estratégicos, aprofundando-se o nível de detalhe da informação recolhida junto dos responsáveis e em sede de auditorias, permitindo um conhecimento mais apurado do perfil de risco.

A7 - Reformulação metodológica do PGR com as recomendações das equipas externa e interna de auditoria.

Execução

O PGR sofreu uma significativa evolução metodológica com:

- A inclusão de novos elementos de informação, incluindo o ajuste na estrutura e nos textos relativos aos conceitos de metodologia, a melhoria das tabelas no que concerne à diferenciação entre riscos, impactos e causas do risco e a sistematização da identificação dos riscos d dos projetos estratégicos. Foram tendencialmente retirados deste Plano os riscos relativos à corrupção e infrações conexas, os quais constam do Plano de Prevenção de Riscos de Corrupção e Infrações Conexas, cuja responsabilidade de conformidade pertence legalmente ao Responsável de Cumprimento Normativo;

- O desenvolvimento de metodologia de monitorização para realização periódica dessa atividade.

A8 - 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;
- Envolvimento de técnicos da gestão do risco em auditorias específicas, para colaboração no detalhe do perfil de risco dessas atividades.

A9 - Publicação e divulgação do PGR e do Relatório Anual de Execução do PGR, através de publicação na Intranet e na Internet, para informação a interessados.

O PGR e o Relatório são disponibilizados no NossoEspaço (intranet da CP) e no site institucional da CP, sendo que os riscos-chave da empresa são também divulgados a outros interessados em relatórios de gestão.

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

- Continuação da preparação das Novas Obrigações de Relato de Sustentabilidade inerentes aos requisitos da Diretiva de Reporte Corporativo de Sustentabilidade (Corporate Sustainability Disclosure Directive – CSRD), nomeadamente as Normas Europeias de Relato de Sustentabilidade (ESRS);
- Continuação da recuperação de material circulante (UQEs, carruagens e locomotivas);
- Melhoria dos canais de venda, com relevo para o investimento nas novas Máquinas de Venda Automática (MVA) e validadores;
- Melhoria dos mecanismos de armazenagem (stocks de manutenção e reparação), com relevo para o investimento em armazéns automáticos;

- Continuação da melhoria da imagem da CP, nomeadamente com a remodelação de bilheteiras e gabinetes de apoio e a manutenção da limpeza e desgrafitagem do material circulante;
- Adoção de metodologias de gestão de projetos, no âmbito do Plano Estratégico da CP, com a adequação de recursos organizacionais;
- Desenvolvimento de competências na área de Cibersegurança e Ciberhigiene, através de formação e sensibilização;
- Formalização de normativos e políticas;
- Beneficiação de equipamentos oficinais para obviar limitações na capacidade de manutenção e reparação de material circulante;
- 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;
- Consolidação da internalização de operações de manutenção (GSM-R - sistema de comunicação interoperável europeu, Convel - sistema de suporte à segurança da circulação);

7- Conclusões

As medidas constantes do PGR de 2024-2025 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 inclusão de novos fatores de risco, a melhoria da aplicação da metodologia por parte dos Representantes, a evolução no paradigma da auditoria baseada no risco e o suporte aos sistemas de gestão da empresa e o desenvolvimento de uma metodologia de monitorização de risco.

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, decorrentes de boas práticas e de novas obrigações legais, das quais se destaca a Diretiva de Reporte Corporativo de Sustentabilidade e a Diretiva 2022/2555 (NIS2), e com o desenvolvimento

de tabela de riscos gerais transversais à organização. A eficácia do acompanhamento do comportamento de cada risco poderá beneficiar de um melhor conhecimento dos respetivos controlos, pelo que se propõe continuar a melhoria na tipificação dos mesmos.